THE BECOMING OF CYBER FINANCIAL CRIME: ASSEMBLAGES AND (MIS)USER-DRIVEN INNOVATION

WAN FEI KATELYN MA

A DISSERTATION SUBMITTED TO

THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

GRADUATE PROGRAM IN SCIENCE & TECHNOLOGY STUDIES

YORK UNIVERSITY

TORONTO, ONTARIO

July 2026

© Wan Fei Katelyn Ma, 2026

Abstract

As digital financial technologies expand, consumers increasingly integrate digital products and services into everyday routines. Through ongoing use and adaptation, these practices may exceed their intended configurations. Within specific social and institutional contexts, some of these (mis)uses are enacted as cyber financial crime. At the same time, (mis)users actively drive innovation by reworking digital access, interfaces, and functionalities in response to situated needs, constraints, and opportunities. These continual reconfigurations position cyber financial crime not as a fixed phenomenon, but as a process of becoming—assembled and reassembled through shifting sociotechnical relations.

This dissertation addresses three interrelated challenges in contemporary cyber financial crime governance. First, it critiques the tendency to treat cyber financial crime as a stable and clearly bounded object despite its continual reconstitution in practice. Second, it identifies the limitations of existing analytical frameworks in accounting for the contingency and processual nature of cyber financial crime. Third, it examines the growing misalignment between governance mechanisms and an evolving financial ecosystem increasingly shaped by (mis)user-driven innovation.

Drawing on assemblage thinking as its primary theoretical framework, this dissertation reconceptualizes cyber financial crime as a dynamic assemblage composed of heterogeneous human and non-human elements. Empirically, the study adopts a multi-phase qualitative research design, including document analysis and semi-structured interviews. The analysis is organized around four analytically generative characteristics—heterogeneity, multiplicity, affectivity, and fluidity—which together provide a systematic approach to examining how cyber financial crime is produced, interpreted, and managed in practice.

The findings demonstrate that cyber financial crime emerges through the co-constitution of technological infrastructures and organizational routines. Multiple and sometimes competing realities of criminality, authorization, and victimization are enacted through investigative and adjudicative practices, while boundaries of crime, responsibility, and liability remain fluid and continually reconfigured through institutional decision-making and (mis)user-driven innovation.

The dissertation concludes by arguing that assemblage thinking offers a productive analytical tool for enhancing cyber financial crime governance and policy. Situated at the intersection of Science and Technology Studies and criminology, this research provides conceptual and practical insights for scholars, policymakers, and industry practitioners seeking to govern cyber financial crime as an evolving sociotechnical phenomenon in Canada and beyond.

Dedication

To my mother and my father

To my partner Thomas and my daughter Emma

To those who fight cyber financial crime relentlessly

Acknowledgements

I extend my overwhelming gratitude to my supervisor and dissertation committee—Professor Kean Birch, Professor Denielle A. Elliott, and Professor James Sheptycki—for their continuous support and invaluable guidance throughout this academic journey. Kean, your recognition of my talent and potential has been instrumental to my growth as a scholar; Denielle, your academic support and intellectual inspiration sustained me through moments of uncertainty and helped me gain—and regain—confidence in this project; James, thank you for encouraging me to become an expert and a leader from day one. I am also deeply grateful to Professor Natasha Tusikov, an important mentor whose careful and rigorous feedback consistently pushed my thinking to a deeper analytical level.

The numerous revisions of the proposal and manuscripts over the past several years were greatly strengthened by the committee's constructive critiques and thoughtful engagement. These intellectual exchanges energized my research and ultimately shaped its theoretical and empirical contributions. I am also deeply grateful to the STS Graduate Program and the broader STS community at York University for fostering a vibrant intellectual environment and for nurturing the networks and relationships that have been central to my development as a scholar.

I am thankful to the STS program at Harvard Kennedy School for providing me with the opportunity to join them in 2021 as a summer student. Additionally, I am grateful for the opportunity to participate as a roundtable discussant at the Graduate Research in STS Conference in October 2022 and as a presenter and panelist at the Science and Democracy Network Conference in August 2023. The experiences gained at Harvard Kennedy School have significantly enriched the STS foundation of my dissertation.

My genuine appreciation goes to the Criminology program at Wilfrid Laurier University for providing me the opportunity to teach cyber criminology-related courses. Thank you, Prof. James Popham, for inspiring me to become a great teacher and a courageous researcher. I appreciate the opportunity to teach the learning modules designed in collaboration with the United Nations Office on Drugs and Crime (UNODC), which also substantially informed my research.

I am filled with endless gratitude for the colleagues, mentors, and friends I have met in the industry. Daureen Younan, my fearless leader, deserves special thanks for shaping me into a strong and resilient industry professional. Thank you for letting me set sail to a beautiful life journey. Linda Elbagoury, I appreciate your guidance in transforming me into a “five whys” curious learner. Adrienne Vickery, thank you for consistently having confidence in me. My gratitude also goes to Tarundeep Dhot for contributing to the development of my analytical skills and to Mohsen Raza, my creative engine and source of boundless imagination. Lastly, Tammy McKinnon, thank you for being a guiding light in all my professional, academic, and personal endeavors.

To my close friends, a special thank you to RL for always tossing the life-saving rope when I feel like I’m drowning. Belle, I appreciate your sisterhood support. WJ and LXD in China, thank you for consistently being there for me day after day as I wake up at 4:45 am to write and create. HW, you remind me that we are pushing humanity forward. JL, for always supporting the introverted side of me. And thank you to people who have supported my passion and pursuits, my personal trainer Hamed, my writing instructor Nicole, and my mentors, Dr. Wael Saghir and Dr. Alexander Stingl. To all my friends from the PhD Dissertation Café, I am deeply grateful for the support and companionship during our virtual writing sessions. To my

SnakeBaby mom support group, thank you for giving me the strength to move forward at the intersection of motherhood and research, and for reminding me that these identities can coexist with care, resilience, and purpose.

I owe the biggest debt to my family. I wouldn't have navigated through my PhD studies, my professional career, my teaching responsibilities, my health conditions, and my personal life commitments without the unwavering support of my mother. Mom, you empowered me to believe in myself and guided me to see the world with kindness, ambition, and love. Dad, thank you for your unconditional love and for encouraging me to think bigger and to always be brave. I am deeply grateful to my partner, Thomas, for his constant understanding, patience, and boundless love. To my daughter, Emma—you taught me the true meaning of resilience. And finally, thank you to my dog, Sunny, for faithfully accompanying me through countless days and nights of writing, year after year.

Done is Better Than Perfect.

人生无需跨越千里，只需不断向前。

一步有一步的答案，一程有一程的风景。

只要不停止出发。

Table of Contents

Abstract ii
Dedication iv
Acknowledgements v
Table of Contents viii
List of Tables xi
List of Figures xii
Funding Statement xiii
Abbreviations xiv
Preface xv

Chapter 1 - Introduction 1
1.1 Introduction 1
1.2 The Becoming of Cyber Financial Crime within the Financial Ecosystem 4
1.3 Research Objectives and Methodological Approach 8
1.4 Practitioner Positionality 13
1.5 Dissertation Structure 17
1.6 Conclusion 19
Chapter 2 - Literature Review 20
2.1 Introduction 20
2.2 The Emergence of Cybercrime as a Governance Object 21
2.3 Definitional Instability: Conceptual Ambiguity and Classification Challenges in Cybercrime 24
2.4 Use, Misuse, and the Shifting Boundary Between Deviance and Crime 34
2.5 Financial Ecosystems, Institutions, and the Production of Risk 41
2.6 Limits of Existing Governance and Control Approaches 45
2.7 Conclusion 50
Chapter 3 - Theoretical Framework 52
3.1 Introduction 52
3.2 Assemblage Thinking: Cyber Financial Crime as Relational Becoming and Enacted Realities 55
3.3 (Mis)User-Driven Innovation as a Productive Force in the Cyber Financial Crime Assemblage 59
3.4 Core Analytical Characteristics of the Cyber Financial Crime Assemblage 64
3.5 Theoretical Framework Justification: The Conjunction of Criminal Opportunity (CCO) Framework and Related Approaches 70
3.6 Conclusion 77

Chapter 4 - Research Design and Methods 78
4.1 Introduction 78
4.2 Phase I: Document Analysis 80
4.3 Phase II: Semi-Structured Interviews: The Technology Experts 85
4.4 Phase III: Semi-Structured Interviews: The Policy Experts 89
4.5 Interview Recruitment 91
4.6 Data Analysis 95
4.7 Research Ethics 98
4.8 Considerations and Limitations: Positionalities 102
4.9 Conclusion 107
Chapter 5 - Heterogeneity: Assembling Elements and Differences 109
5.1 Introduction 109
5.2 The Documented Words: Defining Legal and Regulatory Documents 112
5.3 Technological Infrastructure: Malware, Files, and Codes 126
5.4 The Human Actors: (Mis)users, Insiders, and Institutional Actors 136
5.5 Financial Instruments, Authentication, and Knowledge Practices 158
5.6 Conclusion 166
Chapter 6 - Multiplicity: Enacting the Many Realities 170
6.1 Introduction 170
6.2 Authorized or Not: The Multiplicity of Access Controls 173
6.3 One Incident, Many Realities: Enacting Victimization 180
6.4 The Work of Blame: Mobilizing Faults and Multiplying Accountabilities 199
6.5 Conclusion 219
Chapter 7 - Affectivity: Intensities, Forces, and Desires 220
7.1 Introduction 220
7.2 The Urge to Exploit: Compromises, Tools, and Intrusions 222
7.3 The Desire to Capture: Platforms, Logics, and Decisions 237
7.4 The Drive to Settle: Automated Processes for Investigation and Reimbursement 254
7.5 Conclusion 273
Chapter 8 - Fluidity: Reconfigurations and Relations of Exteriority 275
8.1 Introduction 275
8.2 Fraud or Disputes: The Contested Liabilities 277
8.3 The Fluid Boundaries of Criminalities 292
8.4 Mobilizing Operations: The Fluidity of Labour Resources 312
8.5 Conclusion 325

Chapter 9 - Conclusion 326
9.1 Summary 326
9.2 Key Theoretical Contribution and Empirical Findings 328
9.3 Industry Implications: Governing Cyber Financial Crime as an Evolving Assemblage 332
9.4 Policy Implications: Claims, Crimes, and Knowledge 335
9.5 Future Research Directions 340

References 343

Appendices 375
Appendix A: Codebook 375

List of Tables

Table 1. Categorization and Examples of Cybercrime by the United Nations Office on Drugs and Crime.....25

Table 2. Interviews by Position Categorization: Technology Experts 87

Table 3. Interviews by Position Categorization: Policy Experts 89

Table 4. Overview of Coding Themes 96

Table 5. Canadian Anti-Fraud Centre Frauds by Medium 123

Table 6. Psychological Vulnerabilities and Classic Cases.....139

Table 7. Common Authentication Methods.....288

List of Figures

Figure 1. Relating Abuse, Attacks, Breaches, and Cybercrime 26

Figure 2. Conceptualizing Cybercrime: Definitions, Typologies, and Taxonomies 29

Figure 3. The Matrix of Cybercrimes by Wall (2007) 30

Figure 4. Cybercrime Typology Consolidation 31

Figure 5. Incident Email to Capital One's Responsible Disclosure Program 146

Figure 6. Illustration of Money Mule Cases 183

Figure 7. An Example of Goodwill Fraud Claim Reimbursement 210

Figure 8. Sample Cyber Financial Crime Investigation Platform: SAS Fraud Management 238

Figure 9. Determining Transaction Legitimacy through Fraud Analytics 242

Figure 10. Maintaining Behavioural Profiles for Accurate Fraud Detection 246

Figure 11. Convergence of Fraud Detection Algorithms 248

Figure 12. Lock Card Function on Mobile Application 257

Figure 13. An Example of the Technology Adjudication Process 263

Figure 14. Differences Between Fraud and Dispute 284

Figure 15. Example of a Cyber Financial Crime Investigation Platform 287

Figure 16. Human-Machine Collaboration Investigation: Customer Context 295

Figure 17. Top 5 Dollar Loss by Year and Fraud Type 315

Funding Statement

This dissertation, submitted to the Graduate Program in Science & Technology Studies at York University, was accomplished without any external funding. All research, analysis, and writing were undertaken independently without any financial assistance from external entities. The author recognizes the self-funded nature of this research endeavor and expresses gratitude for the financial support provided by family, as well as the personal investment dedicated to the successful completion of this dissertation.

Abbreviations

ANT	Actor-Network Theory
AT	Assemblage Thinking
CAFC	Canadian Anti-Fraud Centre
CCO	Conjunction of Crime Opportunity model
FCAC	Financial Consumer Agency of Canada
OTP	One-Time Passcode
PAT	Predictive Analytics Technologies
RCMP	Royal Canadian Mounted Police
SCOT	Social Construction of Technology
STS	Science and Technology Studies
SWIFT	Society for Worldwide Interbank Financial Telecommunication

Preface

This dissertation is organized as a set of interconnected chapters that examine cyber financial crime from different empirical and analytical positions. The chapters are not intended to function as independent studies; each focuses on a different aspect of the overall process being investigated. The purpose of this preface is to explain how these components fit together as a single project.

Instead of treating cyber financial crime as a fixed category of offence, the dissertation approaches it as something that takes shape through practice. The object appears differently across consumer interactions, investigative work, technological systems, and organizational decision-making. The argument therefore develops through comparison across these perspectives rather than through a single linear case.

The introductory chapters establish the context, existing scholarship, theoretical framework, and methodological approach guiding the study. The empirical chapters then examine how cyber financial crime becomes actionable across institutional practices. Chapter 5 analyzes the heterogeneous elements involved, including legal and regulatory texts, technological infrastructures, human actors, and financial instruments. Chapter 6 examines multiplicity, showing how authorization, victimization, and accountability are enacted differently across actors and situations. Chapter 7 explores affectivity, focusing on the forces and motivations shaping intrusion, platform decision-making, and automated investigation and reimbursement processes. Chapter 8 addresses fluidity, examining contested liabilities, shifting boundaries of criminality, and the reconfiguration of labour resources. The final chapter synthesizes the findings and outlines theoretical, industry, and policy implications.

All chapters draw on overlapping interviews, documents, and operational materials and should therefore be read as coordinated examinations of a shared analytical object rather than as separate studies. Differences across chapters are intentional, demonstrating how cyber financial crime is variously enacted through practices of detection, verification, adjudication, and organizational response. Taken together, the dissertation traces the ongoing becoming of cyber financial crime as it emerges across institutional settings. The chapters therefore invite the reader to follow how the object comes into being across sites rather than from a single perspective.

The formatting and organization of this dissertation follow the Technical Requirements for Doctoral Dissertations established by the York University Faculty of Graduate Studies. Citations and references conform to the American Psychological Association (APA) 7th edition style. While APA 7 permits the use of narrative citations within sentences, this dissertation follows supervisory guidance to use parenthetical citations placed at the end of sentences for consistency and readability.

Chapter 1 - Introduction

1.1 Introduction

On April 11, 2024, CBC News reported on a series of cybercrime incidents involving over 140 Bank of Montreal (BMO) customers across Canada, who collectively lost more than $1.5 million through unauthorized money transfers. These cybercrime victims were unaware of the unauthorized logins to their accounts, leading to the depletion of their funds via e-transfers, global wire transfers, or bill payments. As a result, many victims faced disrupted financial plans and lost funds meant for children's university tuition, family vacations, or home renovations, with some even forced to rent out rooms in their homes or delay sending their children to universities. The group of victims is now planning to file a class-action lawsuit against BMO, believing the bank's security system failed to protect them against sophisticated cybercrime.

BMO refused to reimburse the fraud claims, stating there were no signs of security compromises such as failed login attempts or irregularities in malware scans. BMO spokesperson Jeff Roman acknowledged the evolving nature of cyber scams, suggesting customers might have unknowingly shared their credentials with scammers. The Ombudsman for Banking and Investment Services (OBSI), a Canadian external compliance body that mediates disputes between member banks and clients, highlighted the challenges of online money transfer cases, primarily due to the difficulty in locating the perpetrators. Cybercrime investigator Kenrick Bagnall suggested malware might have evaded detection, while Duff Conacher from the non-profit advocacy organization *Democracy Watch* criticized the current system as a "blame the victim" approach, arguing that banks should automate security measures and take greater responsibility for ensuring digital banking safety (King, 2024).

When a series of cybercrime incidents occurs, these diverse perspectives lead to a range of different perceptions and responses. Banks like BMO often focus on developing technical security measures and updating their financial service agreements, but they may not fully account for sophisticated cyber threats or scams that evade their internal detection and control mechanisms. Customers, on the other hand, expect their financial institutions to provide robust security and quick resolutions when unauthorized activities occur. Cybersecurity experts highlight the evolving nature of cyber threats, emphasizing the need for developing advanced malware detection and proactive policy measures. Advocacy groups stress the importance of holding financial institutions accountable to better protect consumers within the financial ecosystem instead of having a “blame the victim” system.

In our digitally enabled world, digital financial services, such as advanced digital payment systems, automated financial services, and online banking platforms, offer consumers the convenience of transactions at their fingertips. However, these services also introduce various technology-enabled risks, including the compromise of sensitive online data through cyber attacks, data breaches, or insider threats, which can consequently lead to the facilitation of cyber financial crime.

As illustrated by the cyber incidents reported by CBC News, different actors interpret the same event through divergent lenses. Banks emphasize their efforts to safeguard customers; victims argue that existing protections are insufficient; cybersecurity experts point to weaknesses in malware scanning mechanisms; mediators maintain that banks have met their obligations; and advocacy groups contend that greater responsibility should be assumed by financial institutions. These fragmented assessments and beliefs reveal the absence of a holistic approach to cyber

financial crime governance, with judgments produced in silos rather than through systematic engagement with the phenomenon as a whole.

This multiplicity of perspectives underscores that cyber financial crime is neither singular nor coherent. Similar to the BMO incident, the empirical narratives examined in this dissertation reveal contested understandings, visions, and problem definitions of cyber financial crime. Such perceptions do not arise in isolation but emerge through intricate interactions among heterogeneous actors within the financial ecosystem. As cyber financial crime evolves, so too do institutional responses. This ongoing process is shaped by multi-directional and multi-dimensional interactions through which technologies, strategies, and policies are continuously reconfigured. Seemingly disparate actors, practices, and processes become increasingly entangled as they develop complex relations and dependencies (Anderson et al., 2012).

My argument throughout this dissertation is that cyber financial crime is a process of becoming that is continually assembled through heterogeneous relations among users, digital financial technologies, institutional practices, and regulatory interpretations. It takes form through the situated interactions of users and misusers, (mis)user-driven innovation, digital infrastructures, institutional practices, regulatory frameworks, and affective judgments about responsibility, risk, and harm enacted by both human and non-human actors. What counts as cyber financial crime is therefore not pre-given; it is enacted through everyday decisions, interpretations, and negotiations across multiple sites. By tracing how these enactments unfold within Canadian financial institutions, this dissertation argues that cyber financial crime is continuously produced, contested, and stabilized—often temporarily—through assemblage dynamics rather than resolved through linear detection or control mechanisms.

1.2 The Becoming of Cyber Financial Crime within the Financial Ecosystem

Cybercrime can be broadly defined as "action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct" (Council of Europe, 2001, p. 1). There are many different types of cybercrime, such as offences against computer data and systems, computer-related offences, content-related offences, offences related to infringements of copyright, and acts of racism and xenophobia committed through computer systems (Council of Europe, 2001).

This dissertation focuses specifically on cyber financial crime, rather than examining the broader phenomenon of cybercrime. As the field grows, many authors have attempted to provide cybercrime typologies and define cyber financial crime as a subset of cybercrime (Chandra & Snowe, 2020; Donalds & Osei-Bryson, 2014; Kigerl, 2016; Lee & Wang, 2022). Scholars address cyber financial crime in different terms, such as cyber economic crime, economic cybercrime, financial fraud, attacks against property or theft, cyber fraud, computer-related fraud or forgery, and computer-related identity offences (Fletcher, 2007; Gottschalk, 2010; Phillips et al., 2022; Rajput, 2020; United Nations Office on Drugs and Crime [UNODC], 2022).

The project does not examine cybercrimes that are unrelated to financial or economic interests, such as cyber pornography, cyber stalking, cyber vandalism, cyber espionage, cyber bullying, and so on (Tabassum et al., 2018; Payne, 2020). Nor does it cover social studies of finance. Where social studies of finance strategically unpack financial statistics, financial modelling, and financial technologies in sociotechnical and sociopolitical contexts, this project focuses on the technological developments and policy decisions related to cyber financial crime (MacKenzie, 2001; MacKenzie & Millo, 2003; Muniesa, 2007, 2021).

Cyber financial crime typically occurs within a financial ecosystem. A financial ecosystem refers to a complex and dynamic network of interconnected relationships and processes involving a diverse collection of human and non-human actors. This includes individual and organizational consumers, financial service providers, deposit-taking intermediaries, money transfer platforms, marketplaces and exchanges, regulatory bodies, and other governmental agencies and entities that support systems such as legal services, accounting, auditing, and consulting firms (Bose et al., 2019). Human and non-human actors, along with their interactions, collectively shape the functioning, stability, and evolution of the financial landscape. Within a financial ecosystem, actors can collectively enable capital allocation, facilitate payment and settlement, foster financial innovation, enhance financial stability, and, unfortunately, sometimes also facilitate cyber financial crime.

In this dissertation, cyber financial crime is provisionally defined as the unauthorized use of digital technologies to obtain financial benefit. Such unauthorized use commonly involves the unlawful acquisition or control of property belonging to others through technological means (Gottschalk, 2010; McGuire & Holt, 2017; Rajput, 2020). Within this project, cyber financial crime encompasses a range of practices, including but not limited to cyber fraud and scams; the (mis)use of digital technologies or institutional policies for financial gain; cybersecurity breaches that result in, or seek to result in, financial harm; and the exploitation of vulnerabilities embedded in digital infrastructures or governance arrangements.

From a Science and Technology Studies (STS) perspective, however, this definition is neither stable nor self-evident. Distinctions between authorized and unauthorized uses of technology are enacted through institutional guidelines, risk frameworks, and organizational practices rather than determined by universal criteria. Similarly, what counts as unlawful is

contingent upon specific regulatory regimes, legal jurisdictions, and enforcement practices. The notion of possession of property is likewise unsettled in digital contexts, where property is not simply given but negotiated, thus raising questions about whether digital identities, credentials, data, or virtual assets are recognized and governed as property within particular sociotechnical arrangements.

Despite these conceptual instabilities, cyber financial crime is consistently associated with digital infrastructures and the potential for financial impact. Prior research shows that cyber scammers rely on digital communication platforms to exploit victims (Button & Cross, 2017); cyber attackers leverage technological means to gain unauthorized access to sensitive financial information (van der Wagen, 2018); and actors engage in insider fraud, money laundering, and terrorist financing through global, digitized financial networks (Chatain et al., 2008). In practice, incidents involving actual or potential monetary loss are most frequently classified as cyber financial crime (Rajput, 2020). Yet, as this dissertation argues, such classifications are not merely descriptive but actively produced through institutional judgment, technological mediation, and evolving interpretations of misuse and responsibility.

My research focuses on the fraud types that may have the largest financial impact on consumers. The Canadian Anti-Fraud Centre reports that investment fraud, romance fraud, spear phishing, extortion, and merchandise fraud are the top five fraud types that have the highest dollar losses (Canadian Anti-Fraud Centre, 2022). These common fraud types would all fall under the cyber financial crime categorization I have summarized as:

(a) Unauthorized transactions using personal information such as identity theft and data theft;

(b) Authorized transactions without fraudulent intent such as Authorized Push Payment (APP) scams; and

(c) Authorized transactions with fraudulent intent such as client intentional fraud or first party fraud.

The above fraud typology and terminology originate from my own empirical research. In 2021, I co-authored a peer-reviewed study with Tammy McKinnon, *COVID-19 and Cyber Fraud: Emerging Threats During the Pandemic* (Ma & McKinnon, 2021), which has been cited by over 100 scholarly publications at the time of writing. The typology has also circulated beyond academia and is used by fraud-prevention firms and reporting agencies (Ma & McKinnon, 2021). Informal professional feedback further indicates that investigators and banking risk teams employ the typology within case-classification practices, making it not only descriptive but operative in structuring how cyber financial crime events are recognized and acted upon (Check Point Research, 2019; Federal Trade Commission, 2021; RBC, 2020).

Human and non-human actors both facilitate and respond to cyber financial crime in dynamic and innovative ways. These actions are neither fixed nor random but organized through underlying sociotechnical logics that shape how cyber financial crime emerges and is governed (Baker & McGuirk, 2017). Human actors engaging in unauthorized uses of technology continuously adapt their practices to exploit vulnerabilities in digital systems and institutional policies, while non-human actors, such as malicious software and phishing infrastructures, evolve alongside these practices. In response, financial institutions deploy cybersecurity technologies, including automated fraud detection systems, while regulatory bodies establish policies and compliance frameworks to govern digital financial activities. Non-human actors, such as monitoring algorithms and cybersecurity infrastructures, play a central role in these

governance efforts, alongside collaborative arrangements, such as intelligence sharing between financial institutions and law enforcement agencies.

To account for this complexity, this dissertation conceptualizes cyber financial crime and its governance as an assemblage: a provisional achievement emerging from the co-functioning of human and non-human actors. Assemblage provides a productive unit of analysis for capturing the heterogeneous, relational, and non-linear dynamics through which multiple actors, technologies, and institutional practices are provisionally aligned to produce particular outcomes (Duff, 2014; Deleuze & Guattari, 1987). Attending to four analytically generative characteristics—heterogeneity, multiplicity, affectivity, and fluidity—the cyber financial crime assemblage is understood as a continuous process of becoming, through which actors co-constitute one another and temporarily stabilize meanings of cyber financial crime and its governance. These provisional stabilizations are repeatedly unsettled as (mis)user-driven innovation reconfigures relations within the assemblage, thereby rearranging perspectives, definitions, and strategies. In this sense, cyber financial crime is not resolved or contained but continually reassembled through shifting sociotechnical connections, affective judgments, and interpretive practices.

1.3 Research Objectives and Methodological Approach

As both an industry practitioner and an independent researcher, I have continuously refined my approach to cyber financial crime in order to keep pace with evolving technologies and innovations. The introduction of new digital financial products routinely gives rise to new fraud patterns, which in turn generate new strategies for prevention, detection, and management within the financial ecosystem. This sustained professional and academic engagement has shaped

my understanding of cyber financial crime and enabled me to identify several interrelated challenges that inform the research objectives of this dissertation.

Organizations and institutions vary widely in how they define and interpret cyber financial crime. What is considered unacceptable, deviant, or criminal in one institutional context may not be defined as such in another. These definitional differences directly shape regulatory obligations, research and development priorities for digital financial products and services, and experiences of victimization. The heterogeneous elements and shifting relations through which cyber financial crime is interpreted contribute to its provisional assembly and reassembly, making it not a stable object but an ongoing process of becoming.

Despite this complexity, both academic and industry approaches often rely on fragmented or partial frameworks, revealing a lack of an analytical tool capable of systematically accounting for these dynamics. A central aim of this doctoral project is therefore to develop an analytical approach that can address cyber financial crime across both scholarly and institutional settings. Financial ecosystems' ongoing reconfigurations generate misalignments between technologies, policies, and governance practices, often producing new vulnerabilities and sites of contestation. Thus, it is essential for any proposed framework to acknowledge the inherent instability and ongoing evolution of financial ecosystems.

The primary challenges highlighted above have shaped the main research objectives of my project:

1. To identify and deploy an assemblage-based analytical framework capable of capturing cyber financial crime as a heterogeneous, relational, and continually reconfigured phenomenon.

2. To examine how cyber financial crime is defined, interpreted, and provisionally stabilized across institutional, regulatory, and organizational contexts, and how these processes shape what becomes governable in practice.
3. To analyze how (mis)user-driven innovation continually reconfigures the cyber financial crime assemblage, reshaping vulnerabilities, investigative practices, governance strategies, and institutional responses within an evolving financial ecosystem.

To achieve these research objectives, I use document analysis and semi-structured interviews as my qualitative research methods. Below is a summary of my data collection and analysis processes, of which I provide more details in the Research Design and Methods chapter.

The first phase of this qualitative research identifies the co-functioning human and non-human elements of the cyber financial crime assemblage within the Canadian financial ecosystem through document analysis. This phase examines publicly available documents produced by both public and non-public sector actors to map the critical human and non-human elements of the cyber financial crime assemblage. Drawing on existing literature alongside contemporary policies and institutional materials, the analysis traces how cyber financial crime is conceptualized, regulated, and operationalized across the Canadian financial ecosystem.

The second and third phases examine how cyber financial crime professionals in Canada understand and interpret the use and misuse of digital financial products and services from distinct but interconnected perspectives. Phase Two focuses on technology experts, exploring how they conceptualize digital infrastructures, security tools, and system vulnerabilities, and how users and misusers configure these technologies in ways that generate (mis)user-driven innovation within the Canadian financial ecosystem. Phase Three centres on policy actors,

examining how regulatory frameworks, institutional policies, and governance logics interpret and respond to these technological practices. Both Phases Two and Three focus at the institutional level, drawing on interview data from practitioners within Canadian financial institutions to analyze how responsibilities are distributed across human and non-human actors and how assumptions about risk, intent, and responsibility are embedded in technological and policy responses. Together, these phases illuminate how consumer complaints are addressed and how technological innovation is simultaneously framed as a source of vulnerability and a mechanism for mitigation in cyber financial crime governance.

I then integrate findings from all three phases of the research to frame cyber financial crime as a dynamic assemblage. Drawing on assemblage thinking as the primary theoretical framework, I synthesize relevant literature to articulate four analytically generative characteristics—heterogeneity, multiplicity, affectivity, and fluidity—which structure the four empirical chapters of the dissertation. I conclude by reflecting on the analytical usefulness of the proposed assemblage model and by placing it in dialogue with more traditional criminological frameworks, such as the Conjunction of Crime Opportunity (CCO) model, to develop policy implications and operational insights for industry practice. Taken together, findings across the three phases illustrate the sociotechnical configurations that sustain the cyber financial crime assemblage, while also revealing the tensions, contradictions, and misalignments that emerge across governance levels and institutional domains.

While this dissertation uses assemblage thinking to frame cyber financial crime as a dynamic and relational phenomenon, its analysis of power remains partial and situated. Deleuze and Guattari describe assemblages as compositions of heterogeneous human and non-human components that continuously configure and reconfigure their relations (Deleuze & Guattari,

1987). However, their account does not fully explain how actors with unequal authority, resources, knowledge, technical access, and institutional capacity may exert different forms and intensities of pressure upon an assemblage (Anderson & McFarlane, 2011; Müller & Schurr, 2016). These uneven capacities may stabilize particular arrangements, restrict possible actions, privilege certain interpretations, and influence the direction through which the assemblage is disrupted or reconfigured. Although this dissertation considers these uneven relations, it does not provide a complete structural analysis of the political, economic, and institutional conditions through which power is produced and maintained.

This limitation is particularly important because the dissertation approaches cyber financial crime primarily from an industry and practitioner perspective. The analysis is informed by practical concerns related to fraud detection, investigation, technological development, risk management, control design, and institutional decision-making. This standpoint provides access to the operational processes through which financial institutions identify cyber financial crime, define financial and technological risks, allocate resources, and develop institutional responses. At the same time, it may privilege industry based definitions of risk, loss, responsibility, efficiency, and effectiveness. It may also provide greater visibility to actors, technologies, and decision-making processes located within financial institutions than to the experiences of victims, users, offenders, community organizations, and other actors positioned outside formal industry structures.

Within these limitations, the dissertation examines how uneven relations of power shape the configuration and becoming of cyber financial crime assemblages. It considers how particular human and non-human actors become differently positioned to define problems, authorize knowledge, establish measures of risk, assign responsibility, structure possible actions,

and influence institutional responses. These relations are neither unilateral nor equally distributed. Different actors possess different forms of legal authority, institutional capacity, technical control, material influence, practical knowledge, and access to information. These uneven capacities allow some actors to exert more sustained pressure upon the assemblage, while others exercise weaker, localized, temporary, or less institutionally recognized forms of influence.

Uneven relations of power therefore contribute directly to the reconfiguration of the assemblage because they generate different intensities of pressure across its components. Actors with greater institutional authority, technical control, legal capacity, material resources, or privileged access may exert stronger influence over how cyber financial crime is interpreted and how institutional responses are designed. However, these actors do not have complete or predictable control, as technologies can behave unexpectedly, offenders may adapt their tactics, users can resist or evade controls, and institutional priorities may conflict. Consequently, the assemblage is subjected to a range of influences from diverse components, each with unequal capacities to act. Thus, these findings should be viewed as a contextual practitioner account of power within industry responses to cyber financial crime, rather than a comprehensive analysis of the broader social, political, and economic structures that shape its evolution.

1.4 Practitioner Positionality

This section outlines how my professional and academic experiences shape my approach to cyber financial crime and explain my motivation for undertaking this doctoral project. While a more systematic discussion of positionality appears in the Research Design and Methods chapter, this section focuses on the practical inspirations and conceptual tensions that gave rise to the research questions and analytical framework developed in this dissertation.

I began my career in 2016 at one of Canada's largest financial institutions as a fraud detection professional, where my primary responsibility was to identify and block suspicious activity on consumer accounts. At the time of writing this dissertation in 2026, I have spent over ten years working across multiple functions within fraud management. Over this period, I held a range of roles, including fraud detection agent, business resource officer, training and learning facilitator, fraud operations supervisor and project manager, reporting analyst, horizontal fraud strategist, senior fraud strategist, and, most recently, manager of strategic initiatives in North American fraud operations. Each role involved distinct forms of training, performance metrics, and institutional priorities, shaping how cyber financial crime was understood and addressed in practice.

These experiences revealed that cyber financial crime is not treated as a unified phenomenon within financial institutions, but rather as a compartmentalized problem distributed across specialized teams:

- Fraud detection units focus on immediate incident containment and loss recovery.
- Cybersecurity teams emphasize system vulnerabilities and threat mitigation.
- Anti-money laundering units prioritize regulatory compliance and transaction monitoring.
- Customer service teams manage complaints and reimbursement claims.
- Policy and risk teams concentrate on governance frameworks, metrics, and external regulatory alignment.

Although these teams address related risks, they often operate in silos, guided by different assumptions, objectives, and evaluative standards. As a result, the interconnected nature of cyber financial crime threats is frequently obscured, limiting the financial ecosystem's capacity to respond cohesively.

Throughout my career, I was trained to interpret cyber financial crime differently depending on my institutional position. As a fraud investigator, the problem was framed as an operational issue requiring rapid intervention and financial recovery. In data analytics roles, cyber financial crime was translated into patterns, indicators, and model performance metrics, with success measured through loss reduction and detection efficiency. In governance- and policy-oriented roles, the emphasis shifted toward compliance, auditability, and risk forecasting, often privileging regulatory alignment over operational nuance. In strategic initiatives roles, cyber financial crime was further reframed through lenses of efficiency, cost containment, and customer experience, where the goal was to streamline workflows and optimize end-to-end processes. Each role brought with it a distinct institutional logic that defined what counted as relevant evidence, legitimate concern, and effective intervention.

These shifting framings made clear to me that cyber financial crime is not simply discovered or detected, but actively interpreted and produced through organizational practices. What is recognized as misuse, risk, or harm depends on where one is positioned within the institution and which mandates take precedence. Knowledge about cyber financial crime is therefore unevenly distributed and selectively validated, shaped by role-specific priorities rather than by a holistic understanding of the phenomenon.

When I began my doctoral training in STS at York University—following the completion of a Master's degree in Criminal Justice with a concentration in Cybercrime Investigation and Cybersecurity—I became increasingly aware that many academic and policy-oriented approaches to cyber financial crime did not reflect these practical realities. Existing theoretical models and policy frameworks often assume coherence, stability, or linear causality, while my industry experience suggested that cyber financial crime is far more contingent, negotiated, and

dynamic. In particular, I found little engagement with how institutional silos, automated systems, and everyday decision-making practices shape what cyber financial crime comes to be.

This gap is especially evident in how technological artifacts and social processes such as (mis)user-driven innovation are frequently treated as isolated variables rather than as co-functioning elements within a broader sociotechnical configuration. In practice, innovations introduced by users and misusers routinely reconfigure institutional responses, policy interpretations, and governance strategies, yet these dynamics remain under-theorized in both academic and industry-oriented analyses. The absence of an STS-informed analytical approach has contributed to governance gaps, practice inconsistencies, and recurring misalignments within the Canadian financial ecosystem.

My positionality as an industry practitioner also shapes how power is interpreted throughout this dissertation. My professional experience within fraud operations provides practical knowledge of how financial institutions identify cyber financial crime, assess risks, develop technological controls, allocate resources, and respond to operational challenges. This position offers valuable access to industry practices and allows the analysis to engage with the institutional and technical processes through which cyber financial crime is understood and managed. However, it may also direct greater analytical attention toward organizational priorities, operational effectiveness, financial loss, risk management, and institutional decision-making. As a result, the dissertation may provide greater visibility to actors and relations located within formal industry structures, while the experiences and forms of influence associated with victims, users, offenders, community organizations, and other external actors may be less fully represented. I therefore recognize that the analysis of power presented in this dissertation is situated rather than institutionally neutral and reflects the opportunities and limitations produced

by my practitioner perspective. Although many of these actors appear in the documentary material and in practitioners' accounts, their perspectives are not necessarily represented through direct empirical engagement. The resulting analysis is therefore better understood as a situated examination of how power operates through and around financial institutions, including their differential capacities to define problems, mobilize resources, implement technologies, establish controls, and influence responses to cyber financial crime. A more detailed reflexive account of my positionality and methodological choices follows in the Research Design and Methods chapter.

1.5 Dissertation Structure

This dissertation is organized into nine chapters that collectively explore cyber financial crime as a dynamic sociotechnical assemblage within the Canadian financial ecosystem.

Chapter 1 introduces the study by framing cyber financial crime as an evolving phenomenon within contemporary financial ecosystems. It delineates the research objectives, methodological approach, and the positionality of the practitioner that underpins the analysis. Chapter 2 reviews the interdisciplinary literature on cybercrime, governance, and financial risk, emphasizing the instability of definitions, the shifting boundary between legitimate and illegitimate use, and the shortcomings of prevailing governance and control strategies. This chapter highlights the analytical gaps that necessitate the adoption of an assemblage-based framework.

Chapter 3 develops the theoretical framework, advancing assemblage thinking as a productive lens for analyzing cyber financial crime as relational, processual, and enacted through practice. It introduces (mis)user-driven innovation as a key force shaping the evolution of the assemblage and articulates the four core analytical characteristics that structure the empirical

chapters. Additionally, the chapter situates this framework in dialogue with the CCO model and discusses other potentially relevant frameworks, clarifying points of tension, complementarity, and contribution. Chapter 4 elaborates on the multi-phase qualitative research design, which encompasses document analysis and semi-structured interviews with technology and policy experts, as well as the strategies for data analysis, ethical considerations, and reflections on positionality.

Chapters 5 through 8 present the empirical analysis, each organized around one analytical characteristic of the cyber financial crime assemblage. Chapter 5 examines heterogeneity by tracing how legal texts, technological infrastructures, human actors, financial instruments, and knowledge practices are assembled and differentiated in practice. Chapter 6 focuses on multiplicity, demonstrating how cyber financial crime is enacted through multiple, sometimes conflicting realities of access, victimization, blame, and accountability. Chapter 7 analyzes affectivity, attending to the intensities, desires, and forces that animate exploitation, detection, investigation, and settlement processes, including automated decision-making systems. Chapter 8 explores fluidity by examining how boundaries between fraud and dispute, crime and non-crime, and institutional responsibilities are continually reconfigured through shifting relations of exteriority.

Chapter 9 concludes the dissertation by synthesizing the key theoretical and empirical contributions, revisiting the research aims, and reflecting on the implications for industry governance and public policy. It critically unpacks dominant claims about cyber financial crime advanced by financial institutions and outlines directions for future research. Together, the chapters inspire a deeper understanding of cyber financial crime as a dynamic assemblage

constantly shaped by sociotechnical practices, institutional insights, and the creative potential of (mis)user-driven innovation.

1.6 Conclusion

This introductory chapter began by outlining the concept of cyber financial crime and defining the scope of the project. In doing so, it establishes the empirical and conceptual boundaries of the dissertation while also highlighting the practical ambiguities that emerge when intent, authorization, and responsibility are interpreted unevenly across contexts.

The chapter then introduced the project's three core research aims and the analytical focus on four key assemblage characteristics: heterogeneity, multiplicity, affectivity, and fluidity. Together, these characteristics provide a structured yet flexible lens for analyzing how cyber financial crime is enacted and governed within the Canadian financial ecosystem.

By mobilizing an STS analytical framework grounded in heterogeneity, multiplicity, affectivity, and fluidity, the dissertation reconceptualizes cyber financial crime as a dynamic assemblage and advances a comprehensive analytical tool for understanding and governing cyber financial crime in practice.

Chapter 2 - Literature Review

2.1 Introduction

This chapter reviews key literature from STS and criminology to situate the dissertation within existing scholarly debates on cyber financial crime. The review is organized around three interrelated areas: the emergence of cybercrime, the dynamics of use and misuse in digital environments, and the conceptualization of cyber financial crime. Together, these bodies of work provide the theoretical and empirical foundations necessary for understanding how cyber financial crime has been defined, studied, and governed.

This chapter reviews interdisciplinary scholarship on cybercrime and cyber financial crime to establish the conceptual foundations for the dissertation. Drawing primarily from criminology, cybersecurity, socio-legal studies, and STS, the chapter examines how cybercrime has emerged as an object of governance, how it has been defined and classified, and how these definitions have been shaped by shifting technological practices, institutional judgments, and regulatory contexts.

The chapter begins by tracing the emergence of cybercrime as a governance object (Section 2.2). It then examines the persistent definitional instability surrounding cybercrime (Section 2.3), debates around use and misuse and interpretations of digital practices (Section 2.4) and how risk is produced, assessed, and managed through institutional arrangements and technological infrastructures (Section 2.5). The chapter concludes by critically examining the limits of existing governance and control approaches (Section 2.6), showing how disciplinary and organizational silos generate fragmented understandings of cyber financial crime. To summarize, the chapter establishes the need for an alternative analytical approach capable of

capturing the relational, dynamic, and evolving nature of cyber financial crime—an approach developed in the following theoretical framework chapter.

2.2 The Emergence of Cybercrime as a Governance Object

In July 1961, Leonard Kleinrock, working through the Massachusetts Institute of Technology (MIT), published his first paper on packet switching theory, which was later considered to be the foundation of the internet (Kleinrock, 1961). Kleinrock convinced the U.S. Department of Defense's Advanced Research Projects Agency (DARPA) of the theoretical feasibility of using packet switching rather than circuits for communications (Leiner et al., 2009). DARPA soon turned this computer network concept into a project called "ARPANET," which "allows individuals at different sites to share hardware, software, and data" (as cited in Abbate, 2000, p. 96). As the project developed, Vinton Cerf and Robert Kahn began testing the first ARPANET node at the University of California, Los Angeles (UCLA); the ARPANET project became the starting point of the internet we know today (Abbate, 2000).

The modern history of cybercrime began soon after the initial development of the internet. In 1962, MIT set up computer passwords to protect students' privacy and to limit students' usage of the system. An MIT student named Allan Scherr allegedly manipulated the system by tricking the computer into printing all passwords using a punch card. He also shared the passwords with his friends so they could use other students' credentials after their designated time ran out (Cyber Security Intelligence, 2022). Allan Scherr's case is considered the first documented instance of cybercrime, although at the time there was still no consensus on how to define and address such behaviour.

In 1982, William Gibson first coined the word *cyberspace* in his famous science fiction short story, “Burning Chrome,” where he discusses the hacker group “Cyberspace Seven” (Gibson, 1982, as cited in Wall, 2008). Cyberspace was originally used to illustrate the “mass consensual hallucination” of computer networks, and the term was later adopted by other technology users (Gibson, 1982, as cited in Wall, 2008, p. 51).

During the 1990s, as networked computing expanded beyond specialist communities, the term cyberspace migrated from science fiction into technological, commercial, and policy discourses (Branch, 2021). Technology companies, policymakers, and media outlets increasingly adopted the term to describe emerging online environments, digital infrastructures, and networked forms of interaction. This shift marked an important transition: cyberspace was no longer framed solely as a fictional or metaphorical domain but as a socially and economically significant space requiring management, regulation, and governance.

As the concept gained traction, the terms cybercrime and cyber crime also began to circulate within academic, policy, and public discourse. Cybercrime was increasingly used to describe crimes and harms committed through networked technologies and often functioned as a shorthand for emerging online risks and insecurities (Wall, 2008). Early criminological engagement with cybercrime emerged in the 1990s, encompassing studies of such topics as: child sexual exploitation in online environments (Furnell, 2020); cybercrime targeting individuals, businesses, and governments (Stephens, 1995); and malicious software and credit card fraud (Meyer, 1995).

As cybercrime developed as a conceptual object, a rise of related terms followed, including computer crime, digital crime, electronic crime, internet crime, network crime, technocrime, and virtual crime (Payne, 2020). This terminological expansion reflects ongoing

uncertainty over how to delineate the boundaries of crime in digitally mediated environments. Despite this diversity, cybercrime has remained the most widely adopted term, as it provides a flexible and encompassing label for a broad range of technologically mediated harms (Payne, 2020). At the same time, this conceptual elasticity contributes to the persistent ambiguity and instability that characterize cybercrime as a category of governance and analysis.

Interestingly, despite the wide acceptance of the term, scholars in the field seem unable to agree on the spelling of cybercrime. It can be one word (cybercrime), two words (cyber crime), hyphenated (cyber-crime), or plural (cyber crimes or cybercrimes) (Payne, 2020). This dissertation uses the term *cybercrime* as a deliberately broad analytical category to capture criminal practices that emerge through digitally mediated relations rather than through any single technology, offence type, or legal classification.

The different conceptualizations of cybercrime can lead to different prioritizations in the understanding and handling of the phenomenon. Emphasizing the cyber element can imply focusing on the technology component and the task of finding technical solutions; highlighting the plural nature can suggest varieties in cybercrime typologies and the ability to quantify the issue; and hyphenating the word signifies the compounding effects of technology and humans in a sociotechnical context (Wall, 2008; Payne, 2020). Some may even argue that highlighting the element of *cyber* is no longer as important or relevant, since technology is required to commit virtually all types of crime, and offline activities are now closely connected with online behaviours (Holt, 2012; Junger et al., 2020; McCuddy, 2022).

Cybercrime emerged as a problematic object for law, policing, and governance not by simply coming into existence but through a series of sociotechnical processes. Tracing the development of the internet and cyberspace alongside the coining of the term cybercrime

demonstrates that the category was assembled through technological change, infrastructural expansion, scholarly and policy discourse, legal interpretation, and institutional response. From its inception, cybercrime has been marked by conceptual instability, shaped by shifting definitions, regulatory priorities, and governance practices rather than by a fixed object.

2.3 Definitional Instability: Conceptual Ambiguity and Classification Challenges in Cybercrime

Cybercrime encompasses a wide range of activities, including cyber theft, cyber pornography, cyberbullying, cyber terrorism, cyberstalking, cyber vandalism, cyber espionage, cyber piracy, cyber trespassing, cyber-enabled white-collar crime, and cyber fraud (Payne, 2020). These activities manifest through diverse forms of cyberattack, such as destructive digital intrusions targeting specific organizations, acts of governmental or corporate vandalism and espionage, and the theft of personal credentials through social engineering techniques or crimeware.

The development of technology has drastically increased the possibilities, seriousness, and scope of cybercrime on impacted countries worldwide, including in the Global South. In December 2010, the United Nations Office on Drugs and Crime (UNODC) established the Global Programme on Cybercrime to provide technical assistance, capacity building, international cooperation, and awareness training on cybercrime (UNODC, 2022). While there is no universally agreed definition of cybercrime, the Global Programme on Cybercrime broadly captures cybercrime based on the categories in Table 1 (UNODC, 2022).

Table 1. Categorization and Examples of Cybercrime by the United Nations Office on Drugs and Crime

Categories	Examples
Offences against the confidentiality, integrity and availability of computer data and systems	Hacking; malware creation, possession, and distribution; denial of service (DoS) attacks; distributed denial of service (DDoS) attacks; and website defacement
Computer-related offences	Computer-related fraud or forgery; computer-related identity offences; sending or controlling sending of spam; computer-related copyright or trademark offences; computer-related acts causing personal harm; and computer-related solicitation or "grooming" of children
Content-related offences	Child sexual abuse material; publication of false information (applicable to various countries); and incitement to terrorism

Note. Adapted from *Global Programme on Cybercrime* by the United Nations Office on Drugs and Crime, 2022.

While the examples provided by the UNODC offer a useful entry point for understanding cybercrime, the resulting categorizations are often unstable and overlapping. For instance, computer-related offences frequently intersect with content-related offences, while offences against the confidentiality, integrity, and availability of computer data and systems often encompass both categories. Rather than forming discrete or mutually exclusive classifications, these examples reflect interconnected practices and techniques that cut across multiple domains of cyber activity.

Many of the practices identified by UNODC, such as hacking, malware deployment, distributed denial-of-service attacks, spam, and identity theft, are also integral to what is commonly described as cyber financial crime. As such, cyber financial crime does not sit neatly within a single category but emerges through the interaction of technical methods, institutional responses, and regulatory interpretations. The definitional boundaries of cyber financial crime within UNODC's framework therefore remain ambiguous, pointing to the need for an analytical

approach capable of engaging these overlaps and interdependencies rather than treating them as isolated or independent phenomena.

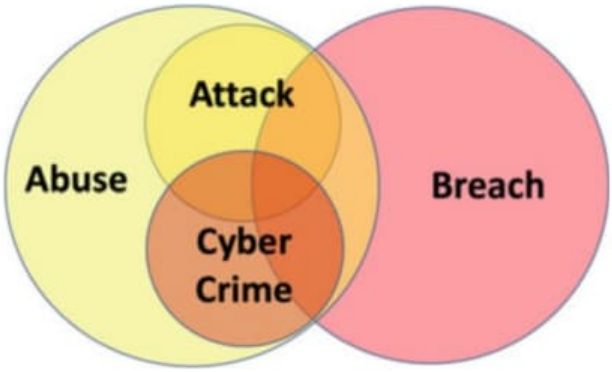
Differentiating Cybercrime and Cyber Deviance

What constitutes a cybercrime may be defined differently across cultures, jurisdictions, fields of study, and political agendas. Not all cyber deviant behaviours are defined as cybercrime; some may be labelled as abuse, attacks, or breaches.

According to Sumner, deviance is a "violation of established contextual, cultural, or social norms, whether folkways, mores, or codified law" (Sumner, 1906, as cited in Robertson, 2020, p. 615). Only codified laws are explicitly enforced by governmental bodies, while folkways and mores are not enforced or regulated in this way (Robertson, 2020). Therefore, not all cyber deviances are considered cybercrimes, but all cybercrimes are cyber deviances.

Steven Furnell offers a Venn diagram, represented in Figure 1, to illustrate the overlapping relationships and the complexity of cybercrime definitions (Furnell, 2020, p. 66).

Figure 1. Relating Abuse, Attacks, Breaches, and Cybercrime



Note. Adapted from "Technology Use, Abuse, and Public Perceptions of Cybercrime," by S. Furnell, 2020, in T. Holt & A. Bossler (Eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (p. 66), Palgrave Macmillan.

This diagram effectively illustrates the relationship between abuse, attacks, and cybercrime. Abuse, attacks, and breaches are all forms of cyber deviance. As shown in the diagram, however, not all abuses, attacks, or breaches result in cybercrimes. For instance, possessing pornography may represent abuse or cybercrime depending on the jurisdiction and cultural context. Some countries fully prohibit pornography while others fully liberalize it (Person et al., 2016).

Denial of Service illustrates the combination of abuse and attack, as the technology infrastructure and service are abused through the form of cyber attacks. However, it could also be considered a breach if the source information of the Denial of Service was harvested from a data breach incident (Furnell, 2020). The data breach may eventually lead to a cybercrime if sensitive information is compromised and abused by malicious actors (Bush, 2016; Lagazio et al., 2014).

In practice, cybercrime and cyber deviance are frequently used interchangeably, reflecting the instability of the boundary between them. Distinguishing cybercrime from cyber deviance is often convoluted, particularly given the variation in legal definitions and enforcement regimes across jurisdictions. What counts as misuse of digital technology—and who has the authority to make that determination—is not fixed, but socially produced through legal frameworks, institutional practices, and normative judgments. As a result, definitions of use and misuse in cyber contexts are continually reworked, emerging as a dynamic and contested issue shaped by interacting technological, regulatory, and social arrangements.

Cyber Financial Crime as a Subset of Cybercrime

The primary focus of this dissertation is cyber financial crime, which is technological crime involving the unlawful possession of property belonging to others (Gottschalk, 2010;

McGuire & Holt, 2017; Rajput, 2020). As mentioned, this definition can be problematic, and interpretation is strongly dependent on the specific context of the case. What is also worth noting is that as technology develops, there can be various types and definitions of property, including virtual assets such as cryptocurrencies and other forms of digital money (Adrian & Mancini-Griffoli, 2019). As well, when it results in financial profit, stealing virtual property items such as weapons and vanity items in an online game setting can be considered a form of cyber financial crime (Cleghorn & Griffiths, 2015).

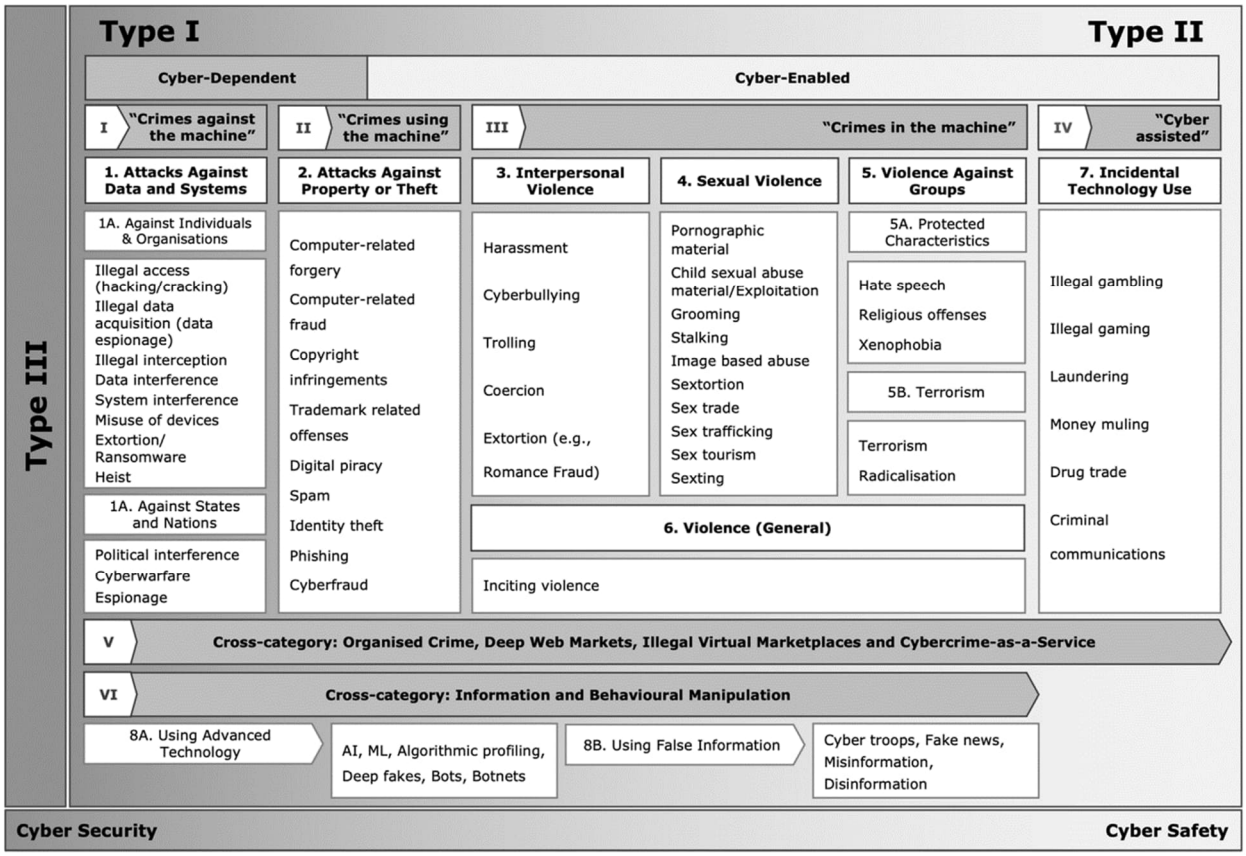
Most cyber financial crime cases include monetary loss, as unauthorized users aim to financially benefit through cyber exploitation (Rajput, 2020). Cyber financial crime cases involving attempted monetary loss are also prevalent, while prevention technologies may be capable of blocking the suspicious transactions or suspending the compromised bank accounts. Some cyber financial crimes do not necessarily result in monetary damages, for instance, fraudulent credit applications, fraudulent mortgage applications using stolen identification, or failed online banking login attempts.

It is important to note that there is no one widely accepted cyber financial crime definition or categorization. Cyber financial crime is often included as a subset of cybercrime, and the typology of cyber financial crime is often embedded within the typology of cybercrime.

To better illustrate, I have included some cybercrime conceptualizations, typologies, and definitions below. Most contain some cyber financial crime components, but the categorizations often overlap or are incomplete (Chandra & Snowe, 2020; Donalds & Osei-Bryson, 2014; Kigerl, 2016; Lee & Wang, 2022).

One recent attempt is by Phillips et al., who lay out the cybercrime and cyber financial crime taxonomies in Figure 2 (Phillips et al., 2022, p.379).

Figure 2. Conceptualizing Cybercrime: Definitions, Typologies, and Taxonomies



Note. From *Conceptualizing cybercrime: Definitions, typologies and taxonomies* (p. 390), by M. Phillips et al., 2022, *Forensic Sciences, 2*(2). https://doi.org/10.3390/forensicsci2020028. Copyright 2022 by the authors.

The typology offered by Phillips et al. is useful because it differentiates types of cybercrime and cyber financial crime using typology indicators, such as cyber dependent, cyber-enabled, crime against the machine, crime using the machine, crimes in the machine, cyber assisted, and so on. It effectively categorizes different cybercrimes and cyber financial crimes based on the crime's relationship with the machine and considers the possibilities of cross-categorization. Here, the *machine* denotes the broader computational infrastructure—networked systems, platforms, databases, and payment architectures—through which digital activity is enacted. However, this framework does not analytically define cyber financial crime as an

independent domain. Because it organizes offences according to their technical relationship to digital systems rather than their financial logics, institutional arrangements, or regulatory conditions, cyber financial crime appears merely as a subset of cybercrime rather than as a distinct category with its own organizing dynamics.

Wall provides a matrix of cybercrime exemplifying how integrity-related, computer-related, and content-related cybercrimes all differ (Wall, 2007, p.4). Wall's work is considered one of the most instrumental contributions to the field of cybercrime. In this matrix, cyber financial crime can be linked to both integrity-related and computer-related crimes. Hacking and identity theft can both lead to financial losses. Again, Wall's typology includes cyber financial crime components in the matrix, but it is also embedded within the larger categorization of cybercrime as a subset (see Figure 3).

Figure 3. The Matrix of Cybercrimes by Wall (2007)

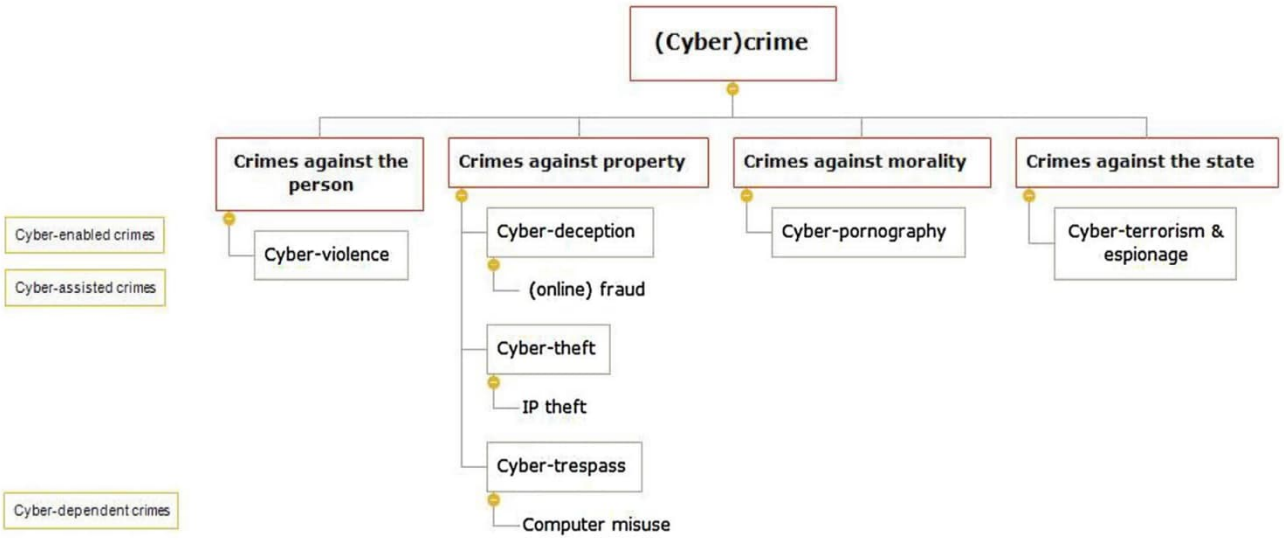
Table 4.1 The Matrix of Cybercrimes: Level of Opportunity by Type of Crime (with selected examples)

	Integrity-related (Harmful Trespass)	*Computer-related (Acquisition theft/deception)*	*Content-related 1 (Obscenity)*	*Content-related 2 (Violence)*
More opportunities for tradional crime (eg., through communications)	Phreaking Chipping	Frauds Pyramid schemes	Trading sexual materials	Stalking Personal Harassment
New opportunities for traditional crime (e.g., organization across boundaries)	Cracking/Hacking Viruses Hactivism	Multiple large-scale frauds 419 scams Trade secret theft ID Theft	Online Sex trade Camgirl sites	General hate speech Organized paedophile rings (child abuse)
New opportunities for new types of crime	Spams (list constuction and content) Denial of Service Information Warfare Parasitic Computing	Intellectual Property Piracy Online Gambling E-auction scams Small-impact bulk fraud	Cyber-sex Cyber-pimping	Online Grooming Organised Bomb talk/Drug talk Targeted hate speech

Note. From *Cybercrime: The Transformation of Crime in the Information Age* (p. 4), by David Wall, 2007, Sage Publications. Copyright 2007 by Sage Publications.

Another attempt by Correia consolidates work from the British government, British Police, and several cybercriminology scholars (Correia, 2019). In this typology, in Figure 4, Correia captures cyber financial crime under the term crimes against property and includes cyber-deception, cyber-theft, and cyber-trespassing (Correia, 2019, p.3). The typology is effective in the sense that it differentiates crimes against property from other types of cybercrime such as crimes against the person, crimes against morality, and crimes against the state. This approach, to an extent, can better conceptualize cyber financial crime and differentiate cyber financial crime from the rest of cybercrime. However, by placing them within crimes against property, the framework frames the offence mainly as the unlawful taking of assets rather than examining the socio-technical arrangements through which the harm is produced. As a result, it improves legal clarity but does not fully theorize cyber financial crime as a distinct issue.

Figure 4. Cybercrime Typology Consolidation



Note. From “Responding to Victimisation in a Digital World: A Case Study of Fraud and Computer Misuse Reported in Wales” (p. 3), by Correia, S. G., 2019, *Crime Science*, 8(1). Copyright 2022 by Crime Science.

In summary, no single definition or typology of cyber financial crime has achieved conceptual clarity or analytical coherence, and cyber financial crime is frequently treated as a subsidiary category of cybercrime. Existing typologies often rely on overlapping and intersecting classifications. For example, phishing commonly enables identity theft by compromising user credentials, which then facilitates unauthorized financial transactions (Levi, 2017). Cyber fraud is similarly categorized as a form of computer-related fraud, while practices such as money muling are frequently entangled with romance fraud, reflecting cross-categorizations between interpersonal deception and technologically mediated activity. In Correia’s framework, cyber-theft is likewise dependent on cyber-trespassing, further illustrating how these categories rarely operate independently.

This definitional ambiguity complicates efforts to analytically separate cyber financial crime from broader cybercrime categories. Activities framed as crimes against machines or crimes using machines can both result in cyber financial crime, just as crimes against persons and crimes against property may converge within financially motivated cyber activity (Correia, 2019; Phillips et al., 2022). Moreover, the widespread adoption of particular terminologies within academic literature does not necessarily align with how cyber financial crime is understood or operationalized in industry practice.

These overlapping, incomplete, and sometimes inconsistent definitions carry significant implications for reporting, governance, and regulation. As Barn and Barn note, the absence of a coherent classification system makes accurate reporting difficult, contributing to legislative

uncertainty and regulatory inconsistency (Barn & Barn, 2016). For instance, reporting cyber theft becomes problematic when cyber-trespassing is treated as a prerequisite component rather than as part of a broader configuration of practices. These challenges suggest that cyber financial crime cannot be adequately captured through rigid typologies alone. Instead, the literature points to the need for analytical approaches that can accommodate relational overlap, contextual variation, and ongoing reconfiguration as technologies, practices, and institutional responses evolve (Chandra & Snowe, 2020; Das & Nayak, 2013).

Beyond generating reporting and regulatory inconsistencies, divergent definitions of cyber financial crime also structure the analytical horizons of existing research frameworks differently. Dominant approaches do not simply differ in how they label cyber financial crime; they advance particular explanatory logics about how such crime occurs, where responsibility lies, and which interventions appear appropriate. Typology-driven frameworks categorize cyber financial crime into specific offence types, focusing on technical aspects, offender behaviour, or individual criminal acts. While this approach helps with clear classification and comparison, it often overlooks the organizational practices, decision-making processes, and institutional discussions needed to identify, assess, and resolve these incidents in real life. Models that focus on risk and control explain cyber financial crime primarily by assessing probabilities, exposures, and potential losses. While these models emphasize measurable outcomes, they tend to overlook important relational dynamics such as coordination between institutions, shifting accountability, and the influence of user-driven innovation. Together, these frameworks may help stabilize the understanding of cyber financial crime for governance purposes, but they fail to account for how this phenomenon is continuously enacted, contested, and reconfigured across various technological, organizational, and regulatory contexts. This discrepancy highlights why existing

approaches are inadequate for capturing cyber financial crime as a dynamic and evolving system, rather than a fixed or singular entity.

2.4 Use, Misuse, and the Shifting Boundary Between Deviance and Crime

The previous sections have shown how cyber financial crime is commonly positioned as a subset of cybercrime and how existing definitions and categorizations are often partial or unstable. From an STS perspective, these instabilities are not simply conceptual shortcomings but reflect deeper sociotechnical dynamics. Söderberg, for example, argues that cybercriminals frequently operate at the forefront of technological change, with practices such as hacking signaling shifts in identity and social positioning from antagonist to protagonist through processes of "creative destruction" (Söderberg, 2010). This perspective highlights how innovation and transgression are often intertwined rather than oppositional.

The goals, meanings, and consequences of cyber activities are therefore highly context dependent. Practices initially framed as misuse or deviance may later be reinterpreted as legitimate or even valuable. For instance, techniques developed by misusers to exploit system vulnerabilities are often appropriated by cybersecurity firms to identify and remediate security flaws (Söderberg, 2010). Similarly, skilled crackers may be recruited by cybersecurity companies as *white hats* or vulnerability researchers, repositioning previously illicit expertise within institutionalized security practices (Mollick, 2005). These shifts illustrate how the same technical practices can circulate across domains of deviance, crime, and legitimacy.

Questions of who the users are, how and where technologies are deployed, what consequences follow from their use, and who holds the authority to define these activities are central to understanding digital use and misuse. The framing of use versus misuse directly shapes

how cybercrime is defined, regulated, and punished. Whether an action is deemed proper use or misuse is not inherent to the technology itself but emerges through social, cultural, economic, and legal contexts that vary across time and place.

These dynamics complicate the application of classical criminological frameworks to cyber contexts. Traditional approaches often rely on binary oppositions—such as guilt and innocence, people and things, or nature and culture—to classify behaviour and maintain clear boundaries between the normal and the deviant (Brown, 2006). While such binaries offer analytical clarity, they struggle to capture the shifting, negotiated, and relational nature of cyber activities, where meanings and classifications are continually reworked through interactions among technologies, users, institutions, and regulatory regimes.

Classical criminology conceptualized crime primarily through rational choice, legal transgression, and proportional punishment (Beirne, 1987; Clarke & Felson, 2017). Crime was understood as the outcome of individual decision-making within a normative legal order, and explanation centred on deterrence, responsibility, and moral accountability. Positivist criminology, emerging in the nineteenth century, departed from this orientation by shifting analytical attention away from legal norms and rational choice toward empirically observable regularities, social patterns, and causal explanations grounded in measurement, classification, and statistical analysis.

Within this early positivist tradition, Adolphe Quetelet occupies a foundational position. Quetelet's application of statistical reasoning to crime introduced the notion of the *"average man"* and framed criminality as a patterned social phenomenon rather than a series of isolated moral failures (Beirne, 1987, p.1141). By applying the normal distribution to crime statistics, Quetelet distinguished between statistical regularity and deviation, thereby translating social

variation into calculable distributions. While Quetelet did not advance a simple binary theory of crime, his work nonetheless relied on a sharp analytical distinction between normality and abnormality. His distinctions between “industrious” and “depraved” populations, as well as between respectable and inferior social groups, illustrate how statistical patterns were infused with normative assumptions about character, morality, and social order (Beirne, 1987, p.1141).

The practical consequences of this orientation were significant. Statistical distinctions between normality and deviation informed how criminal penalties were designed, justified, and adjusted, embedding criminological explanation within administrative and institutional practices of classification, risk assessment, and control. Subsequent critiques of Quetelet and early positivist criminology have highlighted the mechanistic tendencies of these models, particularly their inability to accommodate moral change, contextual interpretation, and the socially contingent nature of what is deemed regularity or crime (Beirne, 1987). What appears as statistical regularity is therefore not simply discovered but produced through historically specific social and political interpretations of what counts as crime.

Dominant positivist-informed frameworks in cyber financial crime research tend to operationalize crime through stabilized categories, event-based metrics, and outcome-oriented indicators. In practice, this often involves translating fluid and relational practices into fixed offence types, standardized loss categories, or calculable risk scores. While such approaches are effective for producing aggregate trends, comparative statistics, and institutional benchmarks, they struggle to capture how cyber financial crime is enacted through shifting sociotechnical arrangements, interpretive judgments, and (mis)user-driven innovation across organizational and regulatory contexts. In this sense, the challenge is not epistemological incompatibility but analytical reduction: existing frameworks explain *how much*, *how often*, or *with what impact*

cyber financial crime occurs, while leaving underexamined *how* it comes to be recognized, stabilized, and governed in practice. This analytical gap motivates the need for alternative approaches capable of tracing cyber financial crime as a process of ongoing becoming rather than as a pre-given object of measurement.

Similarly, socially constructed notions contribute to the development and the conceptualization of cybercrime. The binary labelling of "use" and "misuse" in the context of digital technology, though seemingly logical, can potentially lead to a variety of conceptual challenges and philosophical debates in a regulatory context. The establishment of notions such as proper use and misuse impacts the framings of and consensus surrounding cybercrime. The binary opposition of use and misuse can potentially be counter-productive in understanding cybercrime. For example, some misuses of digital technology can otherwise be viewed as innovative. Even if the digital technology is not being used in the intended ways, it does not necessarily mean that the act falls under the categorization of deviance or criminality.

Definitions and conceptualizations of uses and misuses do exist and can be predominantly well received by a given society and the majority of digital users. For example, those who use digital technology in a way that does not break financial institutions' cardholder agreements are generally considered proper users, and in contrast, users who interact with digital technologies innovatively may be considered misusers.

It is important to note that what is widely accepted may not necessarily mean the truth or the "should," as these socially constructed notions can be determined and shaped by different actors and configurations of power. Those who have the power to create and approve cardholder agreements determine what is use and misuse. The idea of what is widely accepted can be created by those in positions of power, and such players may shape public perceptions.

Subsequently, the constructions of proper use and misuse contribute to different economic implications and sociological notions, which consequently lead to different interpretations of policy problems and solutions.

Use and Misuse in the Context of Cybercrime

Use and misuse do not merely follow technological development; they participate in defining and redefining what comes to be understood as cybercrime as technologies are adopted, adapted, and embedded in everyday practices. Each mode of technological adoption produces distinct sociotechnical meanings, practices, and interpretations attached to digital products and processes.

From an STS perspective, users are not passive recipients of technology but actively consume, modify, domesticate, design, reconfigure, and resist technological systems, while technologies simultaneously shape users through dynamic and participatory processes of co-construction (Oudshoorn & Pinch, 2003). Within this relational dynamic, distinctions between use and misuse emerge through normative judgments rather than through inherent properties of the technology itself.

Uses are often qualified through descriptive labels that assign value and legitimacy to particular practices. For example, “proper use” typically refers to forms of engagement anticipated or encouraged by designers, platforms, and institutional actors, whereas “misuse” denotes deviations from established normative frameworks of acceptable use (Latzko-Toth et al., 2019). These distinctions become especially visible in relation to specific financial and digital technologies. In the context of online banking platforms, logging in from recognized devices, conducting routine transactions, and adhering to authentication protocols are commonly framed as proper use, while credential sharing, scripted login attempts, or repeated authentication

failures may be categorized as misuse or suspicious behaviour. Similarly, for payment cards and mobile wallets, transactions that align with expected spending patterns and geographic locations are typically treated as legitimate, whereas rapid purchases, cross-border transactions, or the use of automation tools may trigger classifications of improper use, even when no malicious intent is present. These examples illustrate how the boundary between use and misuse is not inherent to the technology itself but is produced through institutional expectations, contractual agreements, and risk management practices.

Moreover, what counts as misuse is often determined retrospectively through fraud detection systems, compliance rules, and reimbursement policies that translate situated practices into standardized signals of deviance. As a result, cybercrime becomes closely tied to how particular interactions with digital technologies are interpreted and stabilized within organizational frameworks. Socially produced notions of use and misuse therefore play a central role in shaping how cybercrime is conceptualized and governed. Misuse may be associated with a range of motivations, including malicious intent aimed at psychological or physical harm such as cyberstalking or cyber-enabled terrorism (Halder & Jaishankar, 2011; Hazelwood & Koon-Magnin, 2013); material or financial gain, most commonly in cases of cyber fraud (Button & Cross, 2017; Rajput, 2020); or personal and affective motivations such as revenge, recreation, prestige, or ideological commitment, often observed in hacktivist practices (Holt et al., 2017; Seebruck, 2015). Together, these varied motivations further underscore the instability of use/misuse distinctions and their implications for defining cybercrime. The processual and interpretive character of use and misuse further complicates attempts to define cyber financial crime through fixed categories, underscoring the need for analytical approaches capable of

tracing how technologies, users, and institutional judgments are continually reassembled in practice.

Arguably, what is labelled as misuse can function as a site of creative problem-solving, technological experimentation, or ideological resistance, particularly in domains shaped by rapid technological change. Importantly, neither misuse nor its outcomes—whether framed as productive or harmful—are self-evident; these labels are negotiated and stabilized through social, institutional, and regulatory interpretations. Practices developed by misusers often exceed the intentions of system designers, producing unanticipated effects that may later be reinterpreted as beneficial, legitimate, or innovative within particular contexts. For example, creative engagements with Global Positioning System (GPS) technologies enable gamers to construct virtual races and reimagine spatial relations, while the repurposing of digital mapping tools can operate as a form of resistance to conventional surveillance practices (Farman, 2014). Similarly, practices such as legally sanctioned “tax smoothing” or “income smoothing” in accounting, as well as innovative applications of the Remote Associates Test (RAT) to solve problems through distant analogy, illustrate how unconventional uses of systems may be stabilized as productive rather than harmful (Beda et al., 2020; Mirdala et al., 2014). These examples underscore that the distinction between innovation and harm is not inherent to the practice itself but emerges through processes of classification, valuation, and governance.

These examples complicate any straightforward equation of misuse with deviance or criminality. Instead, they suggest that misuse is relational and context-dependent, acquiring meaning through interactions among technologies, institutional norms, regulatory interpretations, and social values. Not all determinations of misuse of digital technologies should therefore be

treated as inherently problematic or criminal. Rather, misuse often operates as a generative force that reshapes how technologies are understood, governed, and repurposed.

For cyber financial crime, this insight is particularly consequential. Practices that emerge through (mis)user-driven innovation may simultaneously destabilize existing governance frameworks and prompt new forms of institutional response, reclassification, and control. What comes to count as cyber financial crime is thus not fixed in advance but continually reconfigured as technologies, policies, and user practices interact. This shifting boundary underscores cyber financial crime as a process of becoming, one that unfolds through ongoing sociotechnical negotiation rather than through static definitions or stable categories.

2.5 Financial Ecosystems, Institutions, and the Production of Risk

This section extends the preceding discussion of definitional instability by examining how cyber financial crime is addressed within financial ecosystems and institutional contexts. While cybercrime scholarship frequently recognizes financial motivations, financial dimensions are often discussed across multiple cybercrime categories and organizational settings. This dispersion can make it difficult to see how financial institutions, technological infrastructures, and governance practices shape the production, assessment, and management of risk. By shifting attention to financial ecosystems, this section considers how cyber financial crime is interpreted, organized, and managed through institutional practices, evaluative criteria, and sociotechnical arrangements. This perspective also draws attention to the ways in which existing governance and control approaches may become fragmented across institutional domains—a limitation that is examined in greater detail in the following section.

Financial Motivations and Loss-Based Risk Assessment

Existing literature frequently addresses the financial dimensions of cybercrime by focusing on mechanisms of financial extraction, such as fraudulent transactions using stolen credentials, cryptocurrency-enabled laundering, and profits generated through scams and underground markets (Ewen, 2021; Haasio et al., 2020; Hayes et al., 2018; Higbee, 2018; Rajput, 2020). This body of work underscores the centrality of financial motivation in cybercrime, yet it often treats financial harm primarily in terms of realized monetary loss. As a result, cyber financial crime is frequently conceptualized through outcome-based measures that prioritize completed transactions and quantifiable damages.

As Rider notes in his book *A Research Agenda for Financial Crime*, greed is the primary driver of fraud and financial misconduct (Rider, 2022). According to Rider, monetary loss operates as a key metric for assessing severity, prioritizing cases, and allocating institutional resources. Loss thresholds frequently shape investigative attention, regulatory response, and prosecutorial decision-making. However, many cyber activities associated with cyber financial crime, such as failed unauthorized logins, attempted fraud applications, or efforts to bypass automated controls, do not result in immediate financial loss. Despite the absence of realized damage, these activities remain oriented toward financial extraction and are routinely classified as financially significant risks within institutional frameworks.

This reliance on loss-based risk assessment complicates existing cybercrime categorizations. It blurs the boundary between crime, attempted crime, and exposure by privileging monetary outcomes over intent, method, and systemic vulnerability. As a result, institutional judgments play a decisive role in determining what counts as cyber financial crime, often through probabilistic assessments of future harm rather than retrospective evaluation of

loss. This emphasis on loss as a governing metric highlights the limitations of outcome-focused frameworks and points to the need for analytical approaches that can account for cyber financial crime as an evolving process shaped by risk, anticipation, and institutional interpretation.

Institutional Interpretation and Definitional Instability

Although cyber financial crime is frequently referenced in the literature, it is often defined implicitly rather than explicitly. In this dissertation, cyber financial crime refers to the unauthorized use of technology with the intent to unlawfully obtain assets or property belonging to others (Gottschalk, 2010; McGuire & Holt, 2017; Rajput, 2020). However, this definition remains inherently unstable. Distinctions between authorized and unauthorized use depend on institutional policies, regulatory interpretations, and situational context rather than on fixed legal or technical criteria.

What is interpreted as cyber financial crime varies across institutional settings. For example, high-risk investment behaviour may be framed as legitimate consumer choice, whereas the use of available credit to purchase volatile digital assets may be interpreted as misuse of financial products (Cleghorn & Griffiths, 2015; Korauš et al., 2017). Such distinctions demonstrate that legitimacy, deviance, and criminality are not inherent properties of financial activity but are produced through institutional evaluation and governance practices.

This instability is further reinforced through enforcement thresholds and jurisdictional variation. Financial loss often determines prosecutorial priority, with low-value incidents deprioritized or treated as non-criminal despite similarities in technical method or intent (Ashton, 2017). Comparable activities may be classified as cyber deviance or cybercrime depending on perceived financial impact, enforcement capacity, and legal context. Cross-border complexity, resource constraints, and evidentiary challenges contribute to uneven accountability, while

psychological harm and victim reparations remain largely absent from existing frameworks (Ajayi, 2016; Christou, 2018).

Taken together, these dynamics suggest that cyber financial crime cannot be understood as a stable legal or criminological category. Instead, it is variably enacted through processes of identification, investigation, adjudication, and governance that differ across institutional and regulatory contexts.

Situating Cyber Financial Crime within Financial Ecosystems

To address the limitations of outcome-focused and siloed approaches, this dissertation situates cyber financial crime within financial ecosystems, where risk is not merely detected or managed but actively produced through ongoing interactions among institutions, technologies, and users. Borrowed from ecological science, the concept of an ecosystem emphasizes interdependence among actors, environments, and relationships (García-Holgado & García-Peñalvo, 2018). In financial contexts, this perspective has been adopted to capture how interconnected institutions, infrastructures, platforms, and regulatory bodies collectively organize financial activity and shape conditions of risk (Bose et al., 2019; Strumeyer, 2017).

A financial ecosystem comprises financial intermediaries, service providers, regulators, data infrastructures, and supporting institutions whose interactions enable, evaluate, and govern financial transactions (Bose et al., 2019). This dissertation focuses on the personal financial ecosystem as it relates to cyber financial crime, explicitly including households and individual consumers alongside financial institutions, payment platforms, regulators, data providers, authentication services, and criminal financial actors. Consumers and criminal actors are not treated as external to the ecosystem but as situated participants whose actions, interpretations, and adaptations interact with institutional technologies and governance arrangements. This focus

necessarily brackets other dimensions of the financial ecosystem such as wholesale banking, capital markets, and interbank infrastructures in order to examine cyber financial crime as it is enacted within everyday personal financial practices. By centring the personal financial ecosystem, the analysis captures how authorized and unauthorized uses of technologies and policies coexist and how risk is produced through institutional assessments of intent, exposure, and potential harm rather than through technological action alone.

The focus on the personal financial ecosystem necessarily excludes domains such as wholesale finance, capital markets, and interbank infrastructures, which operate through different governance logics and risk configurations. By centring the personal financial ecosystem, this analysis adopts an STS-informed perspective that treats cyber financial crime not as a pre-existing object but as something enacted through everyday financial practices, institutional classifications, and sociotechnical decision-making. This orientation makes visible how everyday interactions, organizational judgment, and (mis)user-driven innovation participate in the ongoing assembly of cyber financial crime—dimensions that are often backgrounded or assumed away in system-level, market-centred, or offence-driven analyses.

2.6 Limits of Existing Governance and Control Approaches

This section examines how prevailing governance and control approaches across both academic research and industry practice produce fragmented understandings of cyber financial crime. It argues that disciplinary and organizational silos constrain how cyber financial crime is identified, interpreted, and managed, limiting the capacity of existing frameworks to account for its relational and evolving character. As a result, governance responses tend to focus on isolated risks, technologies, or actors, rather than on the sociotechnical configurations through which

cyber financial crime emerges. This fragmentation also obscures how responsibility, harm, and prevention are distributed across institutional boundaries, shaping uneven and sometimes contradictory governance outcomes.

Fragmentation across Disciplines and Institutional Domains

In academic research, cyber financial crime is examined across disparate domains such as criminology, cybersecurity, finance, linguistics, and policy studies. Each field privileges distinct problem definitions, analytical tools, and evaluative criteria, often approaching cyber financial crime from within its own epistemic boundaries. As a result, these literatures rarely engage one another in sustained or systematic ways, producing partial and sometimes incompatible accounts of cyber financial crime.

Cybersecurity scholarship tends to frame cyber financial crime primarily as a technological problem, focusing on software vulnerabilities, infrastructure weaknesses, and system-level security failures. Within this literature, cyber financial crime is often understood as a consequence of insecure devices or networks, with an implicit assumption that technological problems can be addressed through technical solutions alone (Kuehn & Mueller, 2014; Qabajeh et al., 2018; Tabassum et al., 2018). This approach focuses on prevention and detection through system design while downplaying institutional judgment, user practices, and governance dynamics.

Criminology scholarship, by contrast, places greater emphasis on human actors. Research in this field frequently examines offender motivations, psychological pathways, and lifestyle choices, as well as situational factors that may increase victim susceptibility to cyber financial crime (Cornish & Clarke, 2016; Murphy & Dacin, 2011). Related work in cyber victimology highlights the emotional, psychological, and social impacts of cyber financial crime, challenging

assumptions that such crimes are victimless and drawing attention to victim stigma and harm (Button & Cross, 2017; Lee & Wang, 2022). While these studies deepen understanding of human experience, they often treat technological and institutional arrangements as background conditions rather than as co-constitutive elements.

Complementing these perspectives, linguistics research demonstrates how cybercriminals deploy persuasion techniques and linguistic strategies to manipulate victims' trust, emotions, and perceptions of intimacy (Anesa, 2022; Lee et al., 2022). These insights frequently inform investigative and adjudicative practices within financial institutions, particularly in assessing intent, credibility, and responsibility.

Business and management research, meanwhile, focuses on organizational risk, cost structures, and strategic decision-making, including investments in cybersecurity infrastructure, regulatory compliance, remediation, and fraud investigation units (Hasham et al., 2019; Kuo & Tsang, 2023). Across these domains, harm is often evaluated through financial loss metrics, which can narrow how risk and responsibility are understood within governance frameworks.

Similar patterns of fragmentation are reproduced within industry practice. Cyber financial crime is institutionally distributed across fraud management, cybersecurity, compliance, customer experience, product development, and financial performance units, each operating under different priorities, metrics, and risk assumptions. Governance and control strategies are therefore developed in relative isolation, addressing discrete symptoms, such as transaction anomalies, system vulnerabilities, or customer complaints, rather than the interconnected sociotechnical conditions through which cyber financial crime emerges.

The compartmentalization of business problems and security issues obscures the relational dynamics among technologies, users and (mis)users, organizational practices, and

regulatory frameworks. Consequently, existing governance models struggle to account for how cyber financial crime is continuously enacted, contested, and reconfigured across institutional boundaries, often stabilizing narrow interpretations of risk and responsibility while overlooking the broader configurations through which cyber financial crime takes form.

Financial Institutions as Sites of Governance and Constraint

Within the Canadian context, financial institutions occupy a central position in the governance of cyber financial crime, as they facilitate digital financial services and adjudicate a large proportion of incidents in practice. This dissertation therefore places particular emphasis on financial institutions as sites where technologies, policies, and human judgment intersect. These institutions not only mediate financial transactions but also play a decisive role in determining how cyber financial crime is identified, interpreted, and managed.

Existing literature documents a wide range of technological strategies deployed by financial institutions to address cyber financial crime, including statistical models, machine learning systems, biometric authentication tools, and cybersecurity infrastructures (Dilek et al., 2015; Mills & Byun, 2006; Siddiqui et al., 2018; Zhang et al., 2021). Although the specific design of these systems is often proprietary, their underlying principles draw on shared bodies of technical knowledge such as anomaly detection, behavioural profiling, and pattern recognition. Patents and published research provide insight into how fraud detection models are conceptualized and operationalized within financial institutions (Shao et al., 2009; Taylor, 2003; Varadarajan et al., 2009; Zoldi & Xu, 2020). Collectively, these approaches position cyber financial crime primarily as a technical problem to be detected, predicted, and mitigated through automated systems. As a result, governance within financial institutions relies heavily on fraud detection and prevention mechanisms that are largely statistical and machine-learning-based.

A key limitation of this approach is that statistical models are effective at identifying anomalous transactions but are less capable of explaining how and why fraud losses occur. Many cyber scams and unauthorized transactions are initiated outside of financial institutions, particularly on social media platforms, instant messaging services, and online marketplaces. Consequently, research attention has increasingly turned toward these platforms, where natural language-based detection models are deployed to identify suspicious behaviour through computational linguistic and psycholinguistic analyses of cybercriminal communication (Mbaziira & Jones, 2016; Mbaziira, 2017). However, insights generated within these environments rarely translate into preventative action within financial institutions, particularly in the Canadian context, where privacy regulations restrict data sharing across platforms (Gruzd et al., 2018). Consequently, financial institutions often become aware of cyber financial crime only after consumers initiate transactions, significantly limiting opportunities for early intervention.

Furthermore, financial institutions as sites of governance often fail to attend to the broader sociotechnical conditions through which cyber financial crime is produced. Governance practices tend to prioritize transaction-level indicators, compliance requirements, and loss metrics, while giving less attention to the upstream interactions among platforms, communication infrastructures, user practices, and institutional incentives that shape how cyber financial crime emerges and evolves.

In conclusion, the literature review suggests that prevailing governance and control approaches tend to treat cyber financial crime as a technical, legal, or behavioural problem in isolation. Technological systems, institutional policies, and human judgment are frequently examined separately rather than as interdependent elements. This fragmentation limits the capacity of existing frameworks to capture how cyber financial crime is produced through

ongoing interactions among technologies, institutions, users, and regulatory environments. These limitations point to the need for an analytical approach capable of engaging cyber financial crime as a dynamic and relational phenomenon rather than as a set of discrete risks to be controlled.

2.7 Conclusion

This literature review has examined how cybercrime has been conceptualized, defined, and governed across multiple bodies of scholarship, revealing persistent challenges in understanding cybercrime and cyber financial crime as coherent analytical objects. By tracing the emergence of cybercrime as a governance concern, the chapter has shown that cybercrime is not a fixed category but one assembled through technological change, institutional practices, and regulatory responses.

As discussed in Section 2.2, cybercrime emerged as a governance object rather than a stabilized analytical category, assembled through technological change, institutional practices, and regulatory responses. This origin has enduring consequences for how cybercrime—and cyber financial crime in particular—is understood, defined, and governed.

The chapter has shown that definitional instability remains a persistent feature of the literature. As outlined in Sections 2.3 and 2.4, overlapping classifications and shifting interpretations of use and misuse complicate efforts to draw consistent boundaries between deviance and crime. In the context of cyber financial crime, these ambiguities are intensified by institutional judgments, loss-based risk metrics, and situational assessments of harm and responsibility.

By situating cyber financial crime within financial ecosystems in Section 2.5, this chapter has illustrated that risk is actively produced through interactions among financial

institutions, technologies, platforms, users and (mis)users, and regulatory frameworks. This perspective exposes the limits of governance and control approaches that isolate cyber financial crime as a technical, legal, or behavioural problem (Section 2.6).

In summary, the literature reviewed in this chapter underscores the inadequacy of existing frameworks for capturing the complexity and fluidity of cyber financial crime. These gaps motivate the need for an alternative analytical approach. The following chapter introduces an STS-informed theoretical framework that conceptualizes cyber financial crime as an assemblage in ongoing becoming, one continually reconfigured through heterogeneous relations and (mis)user-driven innovation.

Chapter 3 - Theoretical Framework

3.1 Introduction

This chapter develops the theoretical framework that guides the analysis of cyber financial crime in this dissertation. A theoretical framework facilitates researchers' critical understanding of a particular issue. Rather than treating cyber financial crime as a discrete event, a stable category, or the outcome of individual intent, the framework conceptualizes it as a relational, processual, and institutional phenomenon. From this perspective, cyber financial crime is viewed not as a singular object or event, but as an emergent achievement produced through ongoing interactions among users, digital infrastructures, investigative practices, organizational routines, policies, and regulatory expectations.

One of the biggest challenges to understanding cyber financial crime in this project is that one cannot easily comprehend the complex, intertwined human and non-human relationships situated within the technology black box. The intricacies of human and non-human relationships are accelerated when human choices, human emotions, and human behaviour become involved. Technology users engage with digital banking systems in heterogeneous ways, and their interactions with these systems can give rise to diverse and uneven experiences of cyber financial crime.

For example, a digital banking user may unknowingly interact with a phishing link, resulting in the compromise of sensitive financial credentials. The user may remain unaware of the breach until unauthorized transactions occur, at which point the user becomes positioned as a cyber financial crime victim. The mechanisms through which the exploitation unfolds often remain opaque to both the user and the financial institution, generating frustration, anxiety, and mistrust. Importantly, victimization does not end with the initial compromise or financial loss.

Users must then engage in extended institutional processes—reporting incidents, submitting claims, undergoing investigations, and awaiting adjudication decisions—often with uncertain outcomes. In cases where claims are declined, victims may pursue appeals or escalations, further extending the fraud "journey" and intensifying affective and institutional pressures.

As this example illustrates, cyber financial crime cannot be understood as a singular experience or uniform process. Fraud incidents unfold differently depending on who the users are, how the exploitation occurs, what technologies and devices are involved, how evidence is interpreted, and how investigators and adjudicators evaluate responsibility and intent. Consequently, cyber financial crime is best understood as a phenomenon in the making, one that emerges through situated practices and evolves across time, organizational sites, and technological configurations.

To engage this complexity, the dissertation adopts Science and Technology Studies (STS) as its primary disciplinary orientation. STS scholarship offers analytical tools for examining how scientific knowledge, technological artifacts, human–machine interactions, and social order are co-produced within networks of power, expertise, and materiality (Haraway, 1989; Hayles, 1999; Jasanoff, 1999; Latour, 1993b). STS perspectives foreground the mutual shaping of technologies and social practices, highlighting how legitimacy, authority, and responsibility are constructed rather than assumed (Pinch & Bijker, 1984; Shapin & Schaffer, 2011; Winner, 1988; Wynne, 2007). These insights are particularly valuable for analyzing cyber financial crime, where governance emerges through complex sociotechnical arrangements that intersect with formal regulatory frameworks, institutional processes, and organizational practices.

Building on STS, this chapter mobilizes assemblage thinking to conceptualize cyber financial crime as a provisional alignment of heterogeneous human and non-human elements.

Assemblage thinking emphasizes contingency, instability, and emergence, directing analytical attention toward how relations are assembled, disrupted, and reconfigured over time. Within this assemblage, (mis)user-driven innovation plays a central role: user practices—both compliant and exploitative—do not merely respond to technological systems but actively participate in reshaping them. User experimentation, adaptation, and misuse prompt institutional responses, system redesigns, and policy adjustments, generating recursive dynamics through which governance is continually reassembled.

Together, these perspectives position cyber financial crime governance as an ongoing accomplishment rather than a settled structure. The framework developed in this chapter organizes the empirical analysis around four core analytical characteristics—heterogeneity, multiplicity, affectivity, and fluidity—which function as conceptual operators for tracing how cyber financial crime is enacted across institutional settings. These characteristics structure the chapters that follow and enable a process-oriented analysis attentive to becoming, uncertainty, and institutional negotiation.

The rest of this chapter explains the ontological and epistemological commitments that support the theoretical framework, highlights the contributions of assemblage thinking and (mis)user-driven innovation, and specifies the four analytical characteristics that guide the empirical analysis. The chapter concludes by placing the framework in dialogue with criminological scholarship and other relevant approaches, justifying its adoption and preparing the analytical ground for the empirical chapters that follow.

3.2 Assemblage Thinking: Cyber Financial Crime as Relational Becoming and Enacted Realities

This section develops the conceptual rationale for adopting assemblage thinking as the primary analytical framework for examining cyber financial crime. The core claim advanced is that cyber financial crime cannot be adequately captured through approaches that assume stable actors, bounded systems, or linear causality. Instead, cyber financial crime unfolds through distributed responsibility, the entanglement of automation and human judgment, and institutional arrangements that remain siloed yet co-function in practice. Meanings of intent, harm, and legitimacy are continually interpreted, challenged, and reworked rather than determined in advance. Assemblage thinking offers a conceptual orientation capable of holding these tensions together without resolving them prematurely.

Relational Sociotechnical Lineages: Actor Network Theory as Background, Not Destination

Relational sociotechnical thinking within STS has long emphasized that social order emerges through relations among heterogeneous actors. Actor-Network Theory (ANT), developed in the 1980s by scholars such as Callon and Latour, was instrumental in challenging explanations that privilege either human agency or technological determinism (Callon, 1986; Latour, 1987, 2005). ANT conceptualizes society as the outcome of associations and performances among human and non-human actors, treating material objects, technologies, and inscriptions as integral to the production of social realities.

ANT's emphasis on tracing relations, mediations, and black-boxed arrangements remains analytically valuable, particularly for revealing how complex sociotechnical systems come to appear stable or naturalized (Pasquale, 2015). In contexts such as cyber financial crime where

automated systems, risk models, and investigative tools often operate opaquely, ANT's insistence on following actors and unpacking hidden relations provides important conceptual grounding.

However, ANT is not adopted here as the primary methodological framework. Critics note that its emphasis on tracing associations and maintaining analytical symmetry makes ANT less suited to examining abrupt change, entrenched power asymmetries, and the affective and intentional dimensions of human action (Collins & Yearley, 1992; Haraway, 1991; Müller, 2015). For this dissertation in particular, ANT's focus on following networks can risk presenting relations as more stable than they are in practice. This limits its usefulness for analyzing rupture, contestation, and strategic agency—dynamics that are central to cyber financial crime. ANT therefore appears here as part of the intellectual lineage that informs assemblage thinking, rather than as a framework used directly in the empirical analysis.

Assemblage Thinking: Process, Becoming, and Heterogeneous Co-Functioning

Assemblage thinking builds on and moves beyond earlier relational approaches by conceptualizing social phenomena as provisional configurations of heterogeneous elements rather than as coherent systems or networks. Originating in the work of Deleuze and Guattari, the concept of assemblage (*agencement*) emphasizes how relations among diverse human and non-human components are formed without predetermined hierarchies or fixed organizational rules (Deleuze & Guattari, 1987, p.19). Assemblages are defined not by stability but by process, contingency, and becoming.

From this perspective, cyber financial crime is viewed not a singular object or event, but an emergent achievement produced through ongoing interactions among users, digital infrastructures, investigative practices, organizational routines, policies, and regulatory

expectations. These elements do not merely interact; they co-function, even when distributed across institutional silos. Assemblage thinking allows these fragmented yet interdependent arrangements to be analyzed together, without assuming coherence, equilibrium, or unified intent.

Key to assemblage thinking is the continuous work of assembling and reassembling relations among heterogeneous elements. Temporary stabilizations such as fraud typologies, risk thresholds, investigative classifications, or adjudicative routines are repeatedly reorganized and rearranged in response to new forms of exploitation, system errors, user appeals, regulatory interventions, and institutional learning. Cyber financial crime governance is therefore not a settled structure, but a moving configuration, continually assembled, disrupted, and reassembled as conditions shift.

Enacted Realities, Distributed Agency, and the Reinterpretation of Harm

Assemblage thinking aligns with an STS epistemological commitment to enacted realities, in which social phenomena do not exist independently of the practices through which they are made knowable and governable. From this perspective, cyber financial crime is not a pre-given object awaiting discovery, but a phenomenon that is performed and stabilized through situated institutional practices. Investigative routines, automated system outputs, evidentiary thresholds, and adjudicative decisions do not merely describe cyber financial crime; they actively participate in bringing particular versions of it into being (Law & Mol, 1998; Law, 2002).

Within financial institutions, cyber financial crime is enacted differently across organizational sites and moments. Detection systems may enact an incident as a potential risk, investigators may enact it as suspicious behaviour or misuse, while customers may experience it as victimization and loss. These enactments do not converge seamlessly into a single

authoritative account; instead, they coexist, overlap, and sometimes contradict one another. Following Law, these multiple realities are not errors or distortions but effects of practice, produced through specific material, organizational, and epistemic arrangements (Law, 2002, 2015).

Agency within this assemblage is therefore distributed and processual, rather than located in any single actor or decision point. Human judgment, algorithmic classifications, institutional protocols, and regulatory expectations collectively shape how incidents are interpreted and acted upon. In line with Latour's emphasis on heterogeneous agency, non-human actors—such as fraud detection models, transaction monitoring systems, and risk scores—do not simply mediate human intentions but actively shape the conditions under which responsibility, suspicion, and legitimacy are attributed (Latour, 1987).

This distributed agency has direct implications for how harm and responsibility are interpreted and reorganized over time. What counts as victimization, negligence, or misuse is not fixed at the moment of technical compromise but is continually reassessed as cases move through investigative and adjudicative processes. A single incident may be rearranged multiple times as new evidence emerges, appeals are lodged, or institutional priorities shift. These reclassifications are often accompanied by affective pressures—urgency, doubt, frustration, or defensiveness—that further shape decision-making and institutional responses (Anderson et al., 2012).

Importantly, assemblage thinking does not seek to resolve these divergent enactments into a singular truth. Instead, it treats the ongoing reinterpretation of harm and responsibility as analytically significant. By attending to how realities are enacted, stabilized, challenged, and reassembled in practice, this framework makes visible the contingent and negotiated nature of

cyber financial crime governance. In doing so, it highlights how responsibility is distributed across sociotechnical arrangements rather than assigned solely to individual users or isolated institutional actors.

3.3 (Mis)User-Driven Innovation as a Productive Force in the Cyber Financial Crime Assemblage

This section develops the conceptual rationale for examining (mis)user-driven innovation as a constitutive dynamic within the cyber financial crime assemblage. The core claim advanced here is that innovation in financial technologies and governance does not originate solely from designers, regulators, or institutional strategy, but emerges through ongoing interactions between users, misusers, technological infrastructures, and organizational responses. Rather than treating use and misuse as deviations from a stable system, this section conceptualizes them as productive forces that actively participate in the assembling and reassembling of financial technologies, policies, and institutional practices. Attending to (mis)user-driven innovation makes visible how cyber financial crime governance is continually reorganized in response to evolving practices of appropriation, exploitation, resistance, and adaptation—without presuming coherence, equilibrium, or unified intent.

Users, Misusers, and the Co-Construction of Financial Technologies and Policies

One of the earliest STS approaches to innovation that foregrounds use is the Social Construction of Technology (SCOT), which places users at the centre of technological meaning-making. SCOT conceptualizes users as a relevant social group that actively constructs diverse and sometimes competing interpretations of technology (Pinch & Bijker, 1984). From this

perspective, technologies are not fixed artefacts but are shaped through processes of consumption, modification, domestication, resistance, and reconfiguration, while technologies simultaneously shape users through ongoing human–machine interaction (Oudshoorn & Pinch, 2003).

As technologies move from early adoption toward relative stabilization, users introduce changes and interpretive flexibility that attach new meanings to technological artefacts (Oudshoorn & Pinch, 2003; Wajcman & Jones, 2012). Research on user-driven innovation demonstrates that users are not passive recipients of technological design but active agents whose practices can influence product development, policy adjustment, and institutional responses (Kline & Pinch, 1996; Oudshoorn & Pinch, 2003). Attending to use therefore provides insight into why certain technologies are accepted, resisted, or reworked in practice.

Within SCOT, *use* typically refers to intended and authorized engagements with technology, whereas *misuse* denotes unanticipated or unauthorized practices, such as gaming systems, abusing automated credit applications, hacking, or tampering (Gillespie, 2006; Latzko-Toth et al., 2019; Söderberg, 2010). Importantly, scholars have shown that the co-construction of users and technologies often produces unintended consequences (Oudshoorn & Pinch, 2003). While designers may not anticipate misuse, misuser practices can nonetheless become sources of innovation, prompting redesign, rule changes, and policy intervention, even when such practices are undesirable from an institutional standpoint (Hyysalo et al., 2016; Van Oost et al., 2009).

In this dissertation, the term *users* refers to individuals who engage with financial technologies according to their intended and authorized design, such as depositing cheques digitally, paying bills online, or transferring funds through legitimate channels. Users may adopt, resist, or selectively configure fraud-prevention measures, including multi-factor authentication,

identity verification tools, or biometric logins. Through these practices, users contribute to the ongoing refinement of digital financial products, while technologies simultaneously reshape user habits, risk perceptions, and trust relationships, particularly following fraud incidents or data breaches.

Misusers, by contrast, are those who deviate from normative frames of use and employ financial technologies in unintended ways. Examples include scammers exploiting digital money transfer services to move stolen funds, fraudsters using stolen identities to obtain credit products, or cybercriminals deploying malware and keyloggers to compromise credentials. Institutional responses to misuser practices, such as reconfiguring detection rules, revising service agreements, or redesigning product features, demonstrate how misuse actively participates in reshaping both technologies and governing policies.

Not all misuses, however, are inherently harmful. Some forms of misuse generate creative problem-solving and unanticipated benefits. For instance, users may transfer funds digitally to access cash indirectly and avoid ATM withdrawal fees. Although such practices fall outside intended design, they illustrate how users creatively rearrange technological affordances to meet everyday needs. These examples underscore the importance of treating use and misuse not as binary categories but as intertwined dynamics that drive technological and institutional change.

(Mis)User-Driven Innovation and the Reassembling of Cyber Financial Crime Governance

Recognizing the co-construction of users and technologies enables a critical examination of (mis)user-driven innovation within the cyber financial crime assemblage. Rather than viewing innovation as originating solely from designers or institutions, this perspective highlights how

user and misuser practices actively participate in assembling and reassembling financial technologies, investigative procedures, and policy frameworks.

This approach offers several analytical advantages. First, it allows for an examination of how human and non-human actors are assembled within cyber financial crime governance and how particular relations are activated or de-emphasized within financial institutions. Second, it facilitates analysis of the sociopolitical translations, technological nodes, and socio-material relations embedded in fraud detection, investigation, and adjudication processes. Third, it opens space to examine how non-human technological assemblages such as cybercrimeware, digital infrastructures, or online underground markets interact with financial institutions as hybrid and goal-oriented configurations (Müller & Schurr, 2016; van der Wagen, 2018; Van der Wagen & Pieters, 2015).

While traditional criminological approaches often privilege human intent, this dissertation treats cyber financial crime as an assemblage achievement, produced through the coordinated yet unstable interaction of human and non-human actors (Van der Wagen & Pieters, 2015). Existing scholarship on user-driven innovation across domains, such as patient-led medical innovation or user modification of sports equipment, demonstrates how end-users contribute meaningfully to technological evolution (Callon & Rabeharisoa, 2003; Oudshoorn & Pinch, 2003; Luthje et al., 2005). Comparable dynamics can be observed in financial technologies, though they remain under-examined.

By contrast, scholarship on misuser-driven innovation is comparatively sparse. While some studies explore technological misuse, only a limited body of work examines cybercrime through the lens of misuser-driven innovation (Hwang & Christensen, 2008; Latzko-Toth et al., 2019; Kraemer-Mbula et al., 2013; Lerner & Seru, 2017; Moitra, 2005; Söderberg, 2010).

Research applying assemblage-oriented approaches to misuser-driven innovation in cyber financial crime remains particularly rare.

When unauthorized users stimulate unintended innovation—for example, when hacking practices generate large-scale financial losses—new technological uses can give rise to novel subjectivities, institutional conflicts, and governance challenges (Söderberg, 2010). These innovations do not simply strengthen or weaken existing hierarchies; rather, they rearrange processes, meanings, and institutional identities, revealing the fluidity of both technological systems and governance arrangements. The heterogeneity of misusers and technologies involved—including hackers, malware, software firms, financial institutions, underground economies, and regulatory bodies—underscores the dynamic nature of the cyber financial crime assemblage.

This dissertation responds to a gap in the literature by positioning (mis)user-driven innovation as a constitutive dynamic of cyber financial crime governance. Rather than framing innovation as external to crime control, the analysis argues that user and misuser practices continuously participate in reorganizing financial technologies, policies, and institutional responses. In doing so, this section situates (mis)user-driven innovation as a productive force within the ongoing assembling and reassembling of the cyber financial crime assemblage, thus laying the groundwork for the four analytical characteristics developed in the following section.

3.4 Core Analytical Characteristics of the Cyber Financial Crime Assemblage

This section translates the theoretical commitments outlined in the preceding sections into a set of analytical characteristics that guide the empirical analysis in this dissertation. Rather than functioning as hypotheses, variables, or explanatory mechanisms, these characteristics operate as sensitizing concepts that orient how empirical material is approached, interpreted, and compared across interviews, institutional documents, and case narratives.

Sensitizing concepts, as originally articulated by Blumer, provide "a general sense of reference and guidance in approaching empirical instances" rather than fixed definitions or benchmark attributes (Blumer, 1954, p. 7, 1969). Unlike definitive concepts, which prescribe in advance what is to be found, sensitizing concepts suggest directions along which to look, shaping analytical attention without determining empirical outcomes. Subsequent qualitative methodologists have emphasized that sensitizing concepts function as background ideas that inform the research problem, serve as interpretive lenses throughout analysis, and offer starting points for engagement with data rather than end points of explanation (Bowen, 2006; Padgett, 2004). In this sense, sensitizing concepts do not replace empirical categories; instead, they enable researchers to move toward concepts and meanings as they are expressed, negotiated, and articulated in practice (Picchietti et al., 2011).

Positioning the framework in this way is methodologically deliberate. The four characteristics—heterogeneity, multiplicity, affectivity, and fluidity—do not predetermine what cyber financial crime is in any given case. Nor do they impose a priori classifications onto interview accounts or institutional practices. Instead, they sensitize the analysis to particular dimensions of the cyber financial crime assemblage, guiding how relations, interpretations, and

transformations are traced across empirical materials. This approach allows analytical consistency across cases while preserving openness to variation, contradiction, and surprise (DeLanda, 2006; Deleuze & Guattari, 1987).

Ontologically, this framework rests on an understanding of cyber financial crime as emergent, enacted, and continually reassembled through sociotechnical practices. *Becoming*, as used in this dissertation, does not imply analytical looseness, relativism, or chaos (Deleuze & Guattari, 1987). The becoming signals patterned instability: the observation that classifications of crime, misuse, innovation, victimhood, and responsibility are repeatedly reorganized over time in response to shifting technological configurations, institutional pressures, and user practices. Assemblage thinking provides the conceptual grounding for this position, while sensitizing concepts make it analytically workable.

Importantly, (mis)user-driven innovation operates across all four characteristics as a productive force that exerts pressure on existing arrangements. User adaptation, resistance, and misuse do not simply disrupt stable systems; they actively participate in reorganizing technologies, investigative practices, and governance frameworks. Attending to these dynamics helps explain why cyber financial crime governance is never fully settled, yet rarely arbitrary (DeLanda, 2006).

The following subsections briefly define each analytical characteristic and indicate how it is mobilized in the empirical analysis.

Heterogeneity

Heterogeneity refers to the composition of the cyber financial crime assemblage through diverse and unlike elements that co-function in practice. Drawing on assemblage thinking, social phenomena are understood not as unified or internally coherent objects, but as configurations

formed through relations among heterogeneous components. As Deleuze and Guattari describe, an assemblage is a multiplicity composed of “many heterogeneous terms” that establish relations without presuming uniformity or linear connection (Deleuze & Guattari, 1987, p. 69). Heterogeneity therefore signals that social processes emerge through the interaction of elements of different kinds rather than through the operation of a single dominant logic.

Within the cyber financial crime context, heterogeneity sensitizes the analysis to the simultaneous involvement of human actors, technological systems, organizational routines, policies, metrics, infrastructures, and discursive classifications. These elements do not operate independently, nor do they merge into a seamless whole. Instead, they co-function in contingent and uneven ways, producing outcomes that cannot be reduced to individual intentions, technical design, or institutional rules alone. Fraud detection models, investigative judgment, customer behaviour, compliance requirements, and affective pressures may align temporarily, but they remain analytically distinct and variably influential across cases.

Empirically, heterogeneity guides attention toward how these elements are assembled together in specific cases and how their relations enable or constrain particular outcomes. (Mis)user-driven innovation appears here as a catalyst that introduces new elements or rearranges existing ones, prompting reconfiguration across the assemblage. Rather than isolating single causes, the analysis examines how different components co-function—sometimes seamlessly, sometimes in tension—to produce decisions, classifications, and responses.

Multiplicity

Multiplicity refers to the presence of coexisting yet non-identical enactments of cyber financial crime within the assemblage. Drawing on Deleuze’s concept of multiplicity, this characteristic challenges the assumption that a phenomenon can be captured as a single, coherent

object or reduced to one authoritative account (Deleuze, 1994). From an assemblage perspective, cyber financial crime is not a unified entity but a dynamic configuration through which multiple practices, interpretations, and classifications are simultaneously performed.

Assemblage thinking treats multiplicity not as variation around a stable core, but as the production of multiple, overlapping realities through practice. As Law argues, realities are enacted rather than merely observed, and different practices generate different versions of the world (Law, 2002, 2015). Within financial institutions, the same incident may be enacted as anomalous risk by automated systems, as suspicious behaviour by investigators, as customer error or negligence through policy interpretation, and as victimization through user experience. These enactments do not necessarily converge; instead, they coexist, intersect, and sometimes compete.

Studying cyber financial crime as an assemblage thus involves tracing partial connections among these enacted realities, thereby examining how different versions remain entangled without collapsing into unity (Strathern, 2004). (Mis)user-driven innovation often intensifies multiplicity by destabilizing established categories and introducing interpretive uncertainty. The assemblage thinking approach enables relational analysis that respects variation and contingency, while remaining attentive to how institutional decisions are shaped through negotiations among competing enactments. In this sense, multiplicity provides an essential analytical lens for understanding how cyber financial crime governance is produced through the simultaneous performance of multiple truths rather than through a singular, stable reality.

Affectivity

Affectivity, as mobilized in this dissertation, does not refer to personal feelings or emotional states. Rather, in Deleuze and Guattari's sense—articulated in *A Thousand Plateaus*

and clarified by Brian Massumi in the translator's foreword—affect denotes a pre-personal intensity: the capacity of bodies to affect and be affected (Deleuze and Guattari, 1987). Drawing on Spinoza's concept of *affectus,* affect refers to a prepersonal intensity associated with a passage from one state of being to another. Affects are not internal emotions but movements produced through relations, encounters, and exposure to external forces. Affect, in this sense, is relational and processual rather than psychological or subjective.

Deleuze and Guattari extend this understanding of affect into the ontological dynamics of assemblages. For them, affectivity names the relational force through which heterogeneous elements enter into composition and transformation (Deleuze & Guattari, 1987). Affect is not located within individual actors but circulates across relations—human and non-human alike—enabling assemblages to assemble, destabilize, and reassemble. In this sense, affectivity is inseparable from becoming: it is the medium through which change is generated and through which capacities emerge or recede.

Within the cyber financial crime assemblage, affectivity sensitizes the analysis to how intensities such as urgency, suspicion, trust, anxiety, defensiveness, or risk sensitivity shape institutional practices. These intensities do not merely accompany decision-making; they actively participate in configuring how cases are interpreted, escalated, or resolved. (Mis)user-driven innovation often amplifies affective pressures by introducing perceived novelty, threat, or uncertainty. Automated alerts may generate urgency, customer narratives may evoke trust or doubt, and institutional pressures may amplify defensiveness or caution. Such affective forces alter the capacities of both human and non-human actors to act, intervene, or withhold action.

Fluidity

Fluidity refers to the capacity of assemblage components to shift positions, roles, and relations over time without dissolving the assemblage itself. This analytical characteristic draws on the principle of relations of exteriority, articulated by Deleuze and Guattari and systematized by DeLanda (Deleuze and Guattari, 1987, p.4; DeLanda, 2006, p.17). From this perspective, assemblages are composed of heterogeneous elements whose relations are contingent and detachable rather than internal or fixed. Components are not fused into a unified whole; instead, they remain capable of entering new relations and acquiring different functions as arrangements are reorganized. Assemblages endure not through stability of parts but through the ongoing reassembly of relations.

STS scholarship further develops this insight by showing how sociotechnical entities persist through adaptive, shifting connections rather than rigid boundaries (Latour, 2005; Law, 1992; Law & Mol, 1998; Mol, 2002). Actors and technologies retain enough continuity to participate in new relations while remaining open to modification across practices. Objects and arrangements hold together by bending, overlapping, and transforming rather than by maintaining fixed form. Fluidity thus represents a mode of endurance through reconfiguration in which coherence is achieved through movement rather than stability.

Within the cyber financial crime assemblage, fluidity sensitizes the analysis to the instability of boundaries surrounding responsibility, intent, and harm. Classifications of transactions, determinations of victimhood or culpability, and interpretations of liability are repeatedly reorganized as cases move through detection, investigation, adjudication, and appeal. Institutional practices themselves are fluid: guidelines may be selectively reinterpreted, investigative labour reconfigured, and reimbursement decisions adjusted in response to

evidentiary developments, affective pressures, or operational constraints. (Mis)user-driven innovation plays a central role here by forcing institutions to revisit and rearrange existing distinctions. Treating fluidity as an analytical characteristic makes visible how cyber financial crime governance is accomplished through temporal reorganization rather than fixed rule application, reinforcing the dissertation's focus on assembling and reassembling as core dynamics of governance in practice.

3.5 Theoretical Framework Justification: The Conjunction of Criminal Opportunity (CCO) Framework and Related Approaches

Criminological theories of opportunity and choice provide a foundational point of reference for understanding why and how crime occurs, particularly through analyses of motivation, situational conditions, and decision-making processes (Clarke & Felson, 2017; Cook, 1986; Cornish & Clarke, 2014). Within this tradition, the Conjunction of Criminal Opportunity (CCO) framework has been especially influential in explaining criminal events through the convergence of motivated offenders, suitable targets, and enabling situations (Akers, 2017; Cornish & Clarke, 2014; Ekblom, 1994). These perspectives have been widely mobilized in cybercrime research and practice, where technological vulnerabilities, guardianship mechanisms, and perceptions of risk play a central role in structuring opportunities for offending (Choi & Lee, 2017; Grabosky et al., 2001; Holt et al., 2020; Yar, 2005). Any attempt to theorize cyber financial crime without engaging with these criminological foundations would therefore be analytically incomplete.

A key strength of the CCO framework lies in its explicit and structured articulation of the immediate conditions that make crime possible. By specifying offender-related factors (such as

predisposition, resources, and readiness), situational and environmental conditions (such as target suitability and enclosure), and the presence or absence of human agents who prevent or promote crime, the CCO framework provides clear guidance on what analysts and practitioners should attend to when examining criminal events. This explicitness offers strong analytical direction and has proven especially valuable for prevention-oriented work, informing the design of controls, safeguards, and deterrence mechanisms (Cornish & Clarke, 2014; Ekblom, 2010). In this respect, the CCO framework offers a disciplined way of identifying where cyber financial crime may occur and which configurations of conditions make offending more likely.

Criminological opportunity perspectives also recognize that crime is adaptive and evolutionary. Ekblom's work on crime prevention emphasizes that offending and control develop in tandem, describing crime as an ongoing process in which new forms of prevention generate new forms of circumvention (Ekblom, 1994, 2010). This "arms race" dynamic is particularly evident in cyber financial crime, where enhanced authentication, monitoring, or access controls are frequently followed by the development of new techniques to bypass them. In this sense, the CCO framework resonates with insights from innovation studies, as misuse and adaptation actively shape technological design, institutional responses, and governance arrangements over time.

At the same time, the CCO framework is oriented primarily toward explaining why cyber financial crime occurs, rather than how criminal events are interpreted, governed, and transformed within institutional settings. Opportunity-based models tend to treat criminality as a relatively stable outcome once an offence has taken place (Ekblom, 2010). Empirical engagement with cyber financial crime governance reveals a more fluid reality, in which incidents may shift between classifications such as fraud, misuse, error, or legitimate activity as

investigations unfold, evidence is reassessed, and institutional judgments are revised. The CCO framework also offers limited analytical traction for examining multiplicity, where the same incident may be enacted simultaneously as technical anomaly, suspicious behaviour, customer victimization, and institutional risk across different systems, departments, and actors.

For these reasons, the present dissertation does not adopt the CCO framework as an analytical model. Instead, it engages with CCO as a theoretical reference point, placing it in dialogue with assemblage thinking. Assemblage thinking builds on the strengths of opportunity-based criminology—particularly its clarity in directing analytical attention toward motivation, capacity, and situational conditions—while extending analysis to dimensions that remain under-theorized in criminology, most notably fluidity and multiplicity (DeLanda, 2006). From an assemblage perspective, criminality is not a fixed outcome of converging conditions, but a provisional and revisable achievement produced through sociotechnical practices of detection, investigation, adjudication, and appeal.

Other potentially relevant theoretical approaches were considered but not adopted due to limitations in analytical fit with the core empirical problem of this dissertation. Governance and institutional theories, for example, tend to assume relative stability, coherence, and legitimacy in organizational arrangements, making them less suited to examining case-by-case reclassification and instability (Brammer et al., 2012; Chhotray & Stoker, 2009). Systems theory and infrastructure studies offer valuable insights into structural organization but rely on comparatively rigid analytical architectures that struggle to capture rapid reorganization and affective judgment in practice (Furlong, 2014; Whitchurch & Constantine, 1993). Meanwhile, subcultural and interactionist theories contribute important accounts of meaning-making and social learning, yet they privilege human actors and face difficulty accounting for automated

systems, distributed decision-making, and sociotechnical coordination across time and institutional sites (Fine & Kleinman, 1979; Serpe & Stryker, 2011).

Assemblage thinking provides the most suitable conceptual approach for this dissertation. It allows cyber financial crime to be understood as a heterogeneous, affectively charged, multiple, and fluid phenomenon—one that is continually assembled, contested, and reorganized through interactions among users, misusers, technologies, and institutions (Deleuze & Guattari, 1983). This perspective is particularly useful in a context where digital infrastructures, financial systems, regulatory practices, and everyday user engagements are tightly interconnected and constantly changing. Rather than assuming stable categories or linear causality, assemblage thinking draws attention to how relations form, how temporary stabilizations occur, and how configurations shift as new actors, devices, and practices enter the field.

Assemblage thinking is useful for examining the relational and evolving nature of cyber financial crime, but it also presents important limitations that affect the design and interpretation of this dissertation. Scholars have raised concerns about its open-ended analytical boundaries, its treatment of causality and power, and its limited normative guidance (Brenner et al., 2011; Buchanan, 2015; Kinkaid, 2020; Rutzou & Elder-Vass, 2019). These limitations cannot be fully eliminated, but they can be made explicit and addressed through careful methodological and analytical choices.

First, assemblage thinking can make it difficult to define analytical boundaries and establish causality. Assemblages are potentially open-ended because their components can connect to many other actors, technologies, institutions, and practices (Anderson & McFarlane, 2011; DeLanda, 2006). In cyber financial crime, the assemblage may extend across financial institutions, customers, malicious (mis)users, regulators, law-enforcement agencies, payment

networks, technologies, policies, and wider social conditions. This creates a practical limitation for this dissertation because it is neither possible nor methodologically appropriate to trace every actor and relation connected to cyber financial crime.

The study therefore draws an explicit empirical boundary around the Canadian financial institutional context, based on the research objectives, available data, participant access, and ethical constraints. Claims concerning heterogeneity, multiplicity, affectivity, and fluidity are consequently limited to the configurations that can be supported by the empirical material. The relational nature of assemblage thinking also limits the ability to isolate single causes (Müller, 2015). Instead of merely asserting that one technology, policy, behavior, or vulnerability is responsible for a specific outcome, this dissertation argues how diverse outcomes arise from the intricate interactions among various conditions. This approach offers a more comprehensive understanding of the complexities involved. Nevertheless, the boundary remains researcher defined, and some relevant relationships and perspectives inevitably fall outside the study (Anderson et al., 2012). Similarly, while the dissertation can identify relational conditions that contribute to particular outcomes, it cannot determine the precise causal weight of each individual component (Rutzou & Elder-Vass, 2019).

Second, assemblage thinking may understate uneven relations of power and the persistence of institutional structures. Its emphasis on distributed agency helps visualize that human and non-human components can all contribute to an assemblage, but distributed agency does not imply equal agency. Brenner et al. (2011) caution that assemblage approaches may give insufficient attention to wider structural and political-economic conditions, while Kinkaid (2020) raises related concerns about power, inequality, and social difference. This limitation is particularly relevant to this dissertation because the research is primarily conducted from an

industry and practitioner perspective. Financial institutions are therefore represented in greater empirical depth than customers, victims, offenders, regulators, law-enforcement agencies, and other actors. This creates a risk that institutional interpretations and forms of power become more visible than those operating outside financial institutions.

To mitigate this limitation, the analysis does not treat all components as equally influential and explicitly considers differences in legal authority, institutional control, access to information, technological capacity, material resources, and decision-making power. It also examines how institutional structures, regulatory requirements, organizational hierarchies, and technological infrastructures can stabilize particular arrangements and limit fluidity. However, the dissertation cannot provide a complete account of power across the broader cyber financial crime assemblage because the perspectives of all relevant actors are not represented to the same empirical depth. The analysis of power should therefore be understood as situated within, and partly shaped by, the Canadian financial institutional perspective of the study.

Third, assemblage thinking provides limited normative guidance for evaluating justice, fairness, and responsibility. While the framework can explain how policies, technologies, institutional decisions, and forms of responsibility emerge through relations among multiple actors, it does not determine whether those arrangements are fair, proportionate, or sufficiently victim-centred. This limitation is relevant to cyber financial crime because victims may experience not only financial loss, but also emotional harm, secondary trauma, and victim-blaming (Button & Cross, 2017; Cross, 2017; Cross et al., 2018; Cross et al., 2019).

In this dissertation, this concern is partially addressed by drawing on criminological and victimization literature to remain attentive to victim impacts, institutional accountability, and the unequal consequences of fraud management decisions, rather than treating operational efficiency

or regulatory compliance as equivalent to fairness. However, the study does not develop an independent theory of justice and therefore cannot fully resolve normative questions concerning how responsibility, loss, and institutional obligations ought to be distributed.

These limitations do not invalidate the use of assemblage thinking in this dissertation. Rather, they define the boundaries of what the framework and the empirical evidence can reasonably support. The study mitigates these concerns by clearly delimiting its empirical scope, avoiding strong linear causal claims, examining uneven power and institutional stabilization, and recognizing the distinction between relational explanation and normative evaluation. At the same time, these measures do not fully resolve the limitations. The analysis remains shaped by selective empirical boundaries, an industry-oriented perspective, unequal representation of actors, and the absence of an independent normative framework. These constraints are therefore treated as continuing limitations of the study rather than as problems that can be completely removed through methodological design.

Recognizing these limitations does not diminish the value of assemblage thinking for this project; rather, it clarifies the conditions under which it is used. In this dissertation, assemblage thinking functions as an analytical orientation for tracing relations, identifying points of stabilization and transformation, and examining how vulnerabilities and criminal opportunities take shape within sociotechnical configurations. At the same time, the challenges it presents—particularly around accountability, measurement, operationalization, and the analysis of structural power—are kept explicitly in view throughout the study. These tensions also indicate directions for future research which can provide additional research opportunities. Assemblage thinking is therefore used here not as a complete explanatory solution, but as a productive way of opening up the complexity of cyber financial crime while remaining attentive to what this

perspective leaves less visible. By combining it with complementary criminological approaches, the dissertation seeks to balance sensitivity to relational complexity with the need for analytical clarity and governance relevance.

3.6 Conclusion

This chapter has developed an assemblage-based theoretical framework for examining cyber financial crime as a relational, processual, and institutionally enacted phenomenon. It conceptualized cyber financial crime as a dynamic configuration produced through ongoing interactions among users, misusers, technologies, organizational practices, and governance arrangements. By situating cyber financial crime within assemblage thinking and STS, the chapter has established an analytical orientation attentive to becoming, reorganization, and the contingent stabilization of meaning.

The subsequent chapters will utilize this framework to explore how cyber financial crime is enacted through specific cases, institutional processes, and governance practices and to therefore demonstrate how assemblage thinking enables a nuanced analysis of cyber financial crime as a phenomenon that is continually assembled and reassembled.

Chapter 4 - Research Design and Methods

4.1 Introduction

Building on the theoretical framework developed in the previous chapter, this dissertation adopts assemblage thinking as its primary analytical orientation for examining cyber financial crime. Central to this approach is an emphasis on becoming: cyber financial crime emerges through ongoing sociotechnical processes of interpretation, intervention, and reorganization rather than through linear causality or fixed classifications. This orientation addresses the methodological gap in existing research that struggles to capture the fluid, multiple, and innovation-driven nature of cyber financial crime as it is governed in practice.

Within the Canadian personal financial ecosystem, financial institutions occupy a central position in the governance of cyber financial crime, functioning as key sites where detection, investigation, adjudication, and reimbursement are enacted in practice. Rather than standing apart from the ecosystem, financial institutions are examined through their internal arrangements of human judgment, automated systems, policies, metrics, and affective pressures, which mediate how ecosystem-level interactions are interpreted and acted upon. Particular attention is paid to (mis)user-driven innovation as a productive force within this assemblage, tracing how user adaptation, misuse, and institutional response recursively shape financial technologies, investigative routines, and policy frameworks. Assemblage thinking enables analysis of how responsibility, intent, and harm are continually interpreted and reorganized through these interactions rather than determined in advance.

This institutional focus also defines the scope of the dissertation's empirical claims regarding heterogeneity, affectivity, multiplicity, and fluidity. Although these four characteristics are developed conceptually to describe the broader cyber financial crime assemblage, the

empirical findings and analytical claims advanced in this dissertation are bounded by the Canadian financial institutional context in which the research is situated. In other words, the framework provides a broader conceptual vocabulary for understanding cyber financial crime as an assemblage, while the empirical analysis demonstrates how these characteristics are manifested within Canadian financial institutions.

This distinction is particularly important in relation to multiplicity. The dissertation does not claim to capture the full range of perspectives or configurations that may constitute cyber financial crime across different institutions, sectors, actors, or jurisdictions. In this project, multiplicity refers to the different configurations of technologies, policies, operational practices, customer interactions, forms of misuse, and institutional responses that are observable within the Canadian financial institutional setting. Other actors, including customers, offenders, regulators, law-enforcement agencies, and technology providers, remain theoretically important components of the broader assemblage and are incorporated into the analysis where their relationships with financial institutions are visible in the empirical material. However, because these actors are not represented in the data to the same extent as financial industry practitioners, the analysis of multiplicity is limited to the configurations and relationships observed within this study.

The research design is structured to operationalize assemblage thinking empirically across multiple scales and sources of data. The study is organized into three phases. Phase I consists of a systematic document analysis of regulatory materials, institutional policies, industry reports, and publicly available documents related to cyber financial crime in Canada. This phase provides contextual grounding and traces how cyber financial crime is formally defined, categorized, and governed across institutional and regulatory domains. Phase II and Phase III comprise qualitative data collection through semi-structured interviews with fraud management

professionals, investigators, compliance personnel, and related practitioners within Canadian financial institutions. These interviews generate rich empirical material that captures how cyber financial crime is interpreted, negotiated, and managed in practice.

Across all phases, data analysis is guided by the four core analytical characteristics developed in Chapter 3. Heterogeneity sensitizes attention to the diverse human and non-human elements involved in cyber financial crime governance. Multiplicity directs analysis toward coexisting and sometimes competing enactments of the same incident across systems and institutional roles. Affectivity foregrounds the intensities, pressures, and judgments that shape investigative and adjudicative decision-making. Fluidity enables tracing how classifications of crime, misuse, victimhood, and responsibility shift over time as cases move through institutional processes. Together, these characteristics provide a coherent analytical structure for examining cyber financial crime as an assemblage in motion, while remaining open to empirical variation and contradiction.

The sections that follow detail the specific methods, data sources, and analytical procedures employed in each phase of the research, including interview recruitment strategies, approaches to qualitative data analysis, and ethical considerations. The chapter also reflects on the researcher's positionality, outlining how professional background, access, and interpretive standpoint shape the research process, as well as the limitations and constraints that emerge from these situated conditions.

4.2 Phase I: Document Analysis

Document analysis refers to a systematic procedure for reviewing or evaluating printed and/or electronic documents (Bowen, 2009). Any documents containing text—such as books, newspaper articles, academic journal articles, and institutional reports—are considered potential

sources for document analysis (Morgan, 2021). When performing document analysis, the emphasis is on context, understanding the descriptions of documents and underlying meanings, and discovering patterns and processes, rather than quantifying numerical relationships between two or more variables (Altheide, 1996; Berger, 1992).

There are strengths and limitations to conducting a document analysis. On the upside, document analysis has fewer ethical concerns compared to other forms of qualitative research such as participant observation or structured interviews, and document analysis is an unobtrusive form of research that is cost-effective (Morgan, 2021). Other advantages of document analysis include stability from non-reactive documents, exactness of references, and broad coverage over an extended timespan (Bowen, 2009).

In terms of limitations, document analysis as a research method often exhibits limited information with fewer opportunities to check for validity and biases (Morgan, 2021). In addition, there are often not enough data to complete a study that perfectly aligns with the researcher's interests (Morgan, 2021). Some scholars also argue that document selection may be biased as the documents may be chosen to align with the agenda of the project (Yin, 1994).

Bowen suggests document analysis can often be used in combination with other qualitative research methods to triangulate data: by examining information collected through different research methods, the researcher can conclude findings across data sets and therefore reduce the level of potential bias from one single document (Bowen, 2009). Patton also explains how triangulation helps increase research validity and can help avoid accusations that the study's findings are simply based on one single source or one single document (Patton, 1990).

I adopted document analysis as a foundational method in order to triangulate empirical insights, strengthen interpretive accuracy, and reduce the risk of analytical bias. Given the

complexity and fluidity of cyber financial crime, document analysis provides a critical means of tracing how the phenomenon is variously defined, operationalized, interpreted, and governed across institutional, technological, and social contexts.

My professional background in fraud operations and fraud strategy has afforded me extensive familiarity with cyber financial crime practices, investigative workflows, and institutional responses. This hands-on experience enables me to navigate large volumes of cyber financial crime-related documentation efficiently and with a strong sensitivity to operational context. It also positions me to identify meaningful patterns, contradictions, and silences within documents that may not be immediately apparent to researchers without industry experience. As such, the document analysis phase was conducted with a high degree of domain specific literacy.

The professional expertise in this field requires careful methodological reflexivity. Familiarity with specific fraud processes or typologies can lead to uneven attention when encountering practices, technologies, or regulatory arrangements outside prior experience. Engaging in systematic and structured document analysis mitigates this risk by necessitating sustained attention to a wide range of sources and perspectives. This approach promotes a comprehensive and nuanced engagement with cyber financial crime, thereby reducing the likelihood that unfamiliar or less visible dynamics will be overlooked.

The document analysis in Phase I draws on both formal and informal documentation. Materials reviewed include academic literature, policy reports, regulatory guidance, legal and quasi-legal documents, industry publications, institutional service agreements, cybersecurity communications, and publicly available case narratives. Collectively, these documents were analyzed to inform an assemblage-based understanding of cyber financial crime, organized through four sensitizing characteristics—heterogeneity, multiplicity, affectivity, and fluidity—

which orient the analysis toward how cyber financial crime emerges, stabilizes, and is continually reconfigured through sociotechnical practices.

When understanding cyber financial crime through the lens of assemblage thinking, the analysis attends to how it is continuously reconfigured through sociotechnical practices, organizational judgments, and shifting interpretations of responsibility and harm. In addition, the document analysis includes media coverage of cyber financial crime drawn from major Canadian news outlets between 2017 and 2024. This time frame was selected to reflect the technological and temporal specificity of cyber financial crime, as forms of exploitation, institutional responses, and governance strategies evolve rapidly and may lose relevance over extended periods. The selected period also aligns with the duration of my doctoral research, during which I have consistently tracked public reporting on cyber financial crime. Media materials are treated not as neutral representations of events but as active elements in the assemblage that shape public understanding, institutional priorities, and regulatory attention.

All qualitative data generated through document analysis contribute to an organized assemblage analysis of cyber financial crime. Instead of isolating documents by sector or institutional type, this phase examines how heterogeneous actors, technologies, rules, and narratives interact to stabilize and destabilize cyber financial crime as an ongoing phenomenon of becoming. The insights generated in Phase I inform subsequent phases of the research by shaping interview design, sensitizing analytical categories, and clarifying the empirical terrain in which cyber financial crime is enacted and contested.

As I mention in the discussion of the limitations of the document analysis, data availability can be a challenge. Selecting documents from other countries is an option when Canadian databases simply do not exist or are not published or available. In these cases, I have

chosen available data that best align with the industry practices in Canada. I analyze documents from other regions and countries similar to Canada, such as those within the European Union or the United States. While I acknowledge the data limitation for Canadian databases and that foreign data contexts might be different, I have aimed to leverage international data that best mirror Canadian contexts.

In the course of conducting my research, I have found that Canadian media outlets may not have enough coverage of different types of cyber financial crime, so I turn at times to international media outlets, such as BBC News, CBS News, *U.S. News & World Report*, *The New York Times*, and *Forbes*, to better manage the limitations of document analysis as a research method. I have opted for these newspapers and media outlets mainly because of their reputations, trustworthiness, and credibility when it comes to publications related to digital technology.

I have chosen to use media coverage as one of the most significant sources for document analysis because many consumer complaints about cyber financial crime are articulated and mobilized through news and media outlets. In practice, individuals who experience fraud often turn to the media when institutional complaint or remediation channels are perceived as inaccessible, ineffective, or unresponsive. Published media documentation therefore provides valuable insight into consumer concerns, lived experiences of harm, and public-facing controversies surrounding cyber financial crime.

Within this research phase, document analysis enables a systematic rethinking of cyber financial crime as an assemblage composed of heterogeneous actors, practices, technologies, and narratives. This phase of data collection serves three primary goals. First, it examines how cyber financial crime is variously framed, defined, and problematized across institutional, legal, media, and organizational texts. Second, it analyzes how interpretations of cyber financial crime diverge

across formal documentation and public narratives, revealing tensions between official representations and everyday experiences of fraud as (mis)user-driven innovation contributes to the ongoing reconfiguration of practices, meanings, and responses. Third, it establishes an empirical foundation for examining how formal practices of governance intersect with routine operational practices, thereby informing subsequent phases of the research that engage with the perspectives and experiences of Canadian financial institution employees.

I have stored documents within the reference management application Zotero. Zotero is open-source reference management software that helps users collect, organize, annotate, cite, and share research. Zotero allows users to sort documentation into collections and tag sources using keywords and themes (Corporation for Digital Scholarship, n.d.). The application also automatically retrieves Portable Document Format (PDF) metadata and stores the documents for easy research and reference (Zotero, n.d.).

4.3 Phase II: Semi-Structured Interviews: The Technology Experts

Magaldi and Berler define the semi-structured interview as an exploratory interview which often follows a guide or protocol that is devised prior to the interview (Magaldi & Berler, 2020). Semi-structured interviews also allow for discovery, as they give space for interviewers to follow topical trajectories together with interviewees, which can unfold organically.

Semi-structured interviews are generally organized around a set of pre-determined but open-ended questions that allow for emerging dialogue between interviewers and interviewees (DiCicco-Bloom & Crabtree, 2006). Rubin and Rubin suggest that ideal interviews consist of a balance between central questions, follow-up questions, and probing questions (Rubin & Rubin, 2011). The freedom provided by follow-ups and probing questions could help interviewers tailor

their queries to the specific interview context as well as to the people being interviewed (Lindlof & Taylor, 2017). To fully utilize the advantages of semi-structured interviews, interviewers need to be "smart, sensitive, poised, and nimble, as well as knowledgeable about the relevant substantive issues" (Adams, 2015, p. 493).

This phase of the dissertation includes data insights from 12 interviews, each lasting 45 to 60 minutes, undertaken to examine how use and misuse configure technological developments used by financial institutions to counter cyber financial crime. The primary research method for this phase was semi-structured interviews carried out via video conferencing software. I asked interviewees to answer questions related to cyber financial crime technology concerns such as identity theft and APP scams from the document analysis conducted in Phase I.

The primary research objects in this section are major domestic banks (Schedule I) participating in the Canadian Bankers Association (CBA). The majority of the interviewees have been selected from the Big Five banks: Bank of Montreal (BMO), Bank of Nova Scotia (Scotiabank), Canadian Imperial Bank of Commerce (CIBC), Royal Bank of Canada (RBC), and Toronto-Dominion Bank (TD). Some participants also come from other domestic banks, including local credit unions. In Canada, the Big Five banks hold close to 80% of the market share. Many interviewees have worked for more than one bank, so they often shared experiences that could be applicable across multiple financial institutions in Canada. About 80-90% of interviewees were working for the Big Five banks at the time of writing. The other 10-20% of interviewees were working for or had previously worked for the remaining major domestic banks, including credit unions in Canada.

I have selected semi-structured interviews as my research method due to my background as an industry professional, which provides me with prior knowledge of the subject matter. I

possess operational familiarity with common fraud detection technology platforms as well as an understanding of standard fraud policies and procedures within the Canadian financial ecosystem. While I considered structured interviews for gathering qualitative data, I believed that semi-structured interviews would enable me to capture the affective dimension of my research participants—specifically, how they understand, perceive, define, interpret, and convey knowledge about cyber financial crime. Discussions on this topic can be challenging to navigate in unstructured interviews, given the diverse opinions and perspectives in the field. Additionally, in corporate settings, participants may inadvertently disclose proprietary information when expressing their thoughts freely, which is not the objective of my research data collection. Semi-structured interviews have allowed me to guide the conversations while maintaining focus on the core interview questions, ultimately leading to valuable insights.

Phase II focuses on in-depth interviews with participants selected for their technical and professional expertise in the design, deployment, and governance of digital financial technologies. Participants were recruited to support an analysis of how cyber financial crime is enacted and reconfigured through everyday technical practices, organizational decision-making, and design choices (see Table 2). This phase seeks to understand how cyber financial crime emerges from within sociotechnical arrangements rather than as an external disruption to them.

Table 2. Interviews by Position Categorization: Technology Experts

Technology Experts – Position Categorization	Number
Fraud Analytics Analyst	1
Fraud Modeling Expert	1
Fraud Technology Product Owner	1
Fraud Business System Analyst	1

Fraud Business Consultant	2
Fraud Technology Consultant	2
Fraud Portfolio Leader	2
Fraud Product Leader	2
Total	12

Key interview priorities include examining how users and misusers are defined and differentiated in the context of cyber financial crime technologies; analyzing how digital technologies are used, adapted, and repurposed in practice; exploring how (mis)user-driven innovation shapes product development, risk assumptions, and governance strategies within Canadian financial institutions; and attending to how trust is affected, negotiated, and re-established through ongoing processes of technological redesign. Through these lines of inquiry, the interviews support an assemblage-based analysis attentive to heterogeneity, multiplicity, affectivity, and fluidity, and to the ongoing becoming of cyber financial crime.

Key questions asked in the interviews included but were not limited to how the actions of users and misusers influence and reshape financial technologies in practice; how feedback on use, misuse, and adaptation is generated, interpreted, and acted upon by financial technology designers and institutional decision-makers; and how Canadian financial institutions make decisions about digital products and technology design in the context of cyber financial crime. Collectively, these questions were oriented toward understanding how cyber financial crime is enacted through heterogeneous actors and technologies, how multiple interpretations and practices coexist, how affective judgments such as trust and risk inform decision-making, and how sociotechnical arrangements remain fluid and continually reconfigured through processes of (mis)user-driven innovation.

4.4 Phase III: Semi-Structured Interviews: The Policy Experts

As with Phase II, Phase III draws on data from 12 semi-structured interviews and employs semi-structured interviewing as the primary qualitative method. This approach was selected because pre-designed interview guides allow interviewers to gather focused and comparable data within a limited interview timeframe (Jamshed, 2014), while still leaving room for participants' situated interpretations, reflections, and experiential accounts (Kallio et al., 2016). Phase III builds analytically on insights generated from the document analysis conducted in Phase I and extends the inquiry to examine how cyber financial crime policies are shaped, interpreted, and reconfigured in practice within the Canadian financial ecosystem.

Participant recruitment for Phase III followed a similar strategy to Phase II. In addition to interviewees previously known to me through professional experience, participants were recruited using snowball sampling through professional network referrals. Participation was entirely voluntary and did not involve any form of payment or monetary compensation. Participants were selected based on their proximity to the development, interpretation, and operationalization of cyber financial crime policies within financial institutions, including individuals working in policy design, operational governance, training, escalation management, and strategic advisory roles (see Table 3).

Table 3. Interviews by Position Categorization: Policy Experts

Policy Experts – Position Categorization	Number
Fraud Training Facilitator	1
Fraud Team Lead	1
Fraud Resource Officer	1

Fraud Investigator	1
Fraud Strategy Analyst	1
Fraud Vendor Manager	1
Fraud Capabilities Coach	1
Fraud Claims Adjudicator	1
Fraud Recovery Analyst	1
Fraud Policy Leader	1
Fraud Team Manager	2
Total	12

The analytical priorities of Phase III focus on how cyber financial crime policies are enacted through heterogeneous configurations of actors, technologies, organizational routines, and institutional judgments. Interviews examine how users and misusers are imagined, categorized, and mobilized within policy frameworks, how policies are interpreted, adapted, or contested in everyday practice, and how (mis)user-driven innovation contributes to the ongoing reconfiguration of governance arrangements. Particular attention is paid to multiplicity, as multiple policy logics and interpretations often coexist; to affectivity, as judgments of trust, risk, responsibility, and fairness shape decision-making; and to fluidity, as policies are continuously revised in response to emerging practices, technologies, and incidents.

Key interview questions included, but were not limited to, how Canadian financial institutions develop and implement policies related to cyber financial crime; how user and misuser practices influence policy interpretation and adjustment; how decisions are made regarding responsibility, restriction, remediation, and institutional response; and how automation and human judgment are balanced within governance processes. Rather than treating policy as a

stable or purely top-down instrument, Phase III examines policy as an evolving sociotechnical arrangement, one continually shaped through practice and through the ongoing becoming of cyber financial crime.

4.5 Interview Recruitment

In terms of recruitment methods, some research participants were previously known to me from my work in the field or identified through organizational and professional websites (e.g., LinkedIn). When I explore an unidentified industry practitioner's LinkedIn page, the platform displays our mutual connections, which can expedite the recruitment process once the referral is given. I would then choose practitioners who possessed relevant experience and seemed capable of answering my open-ended questions, as pre-defined in my semi-structured interviews.

These interviewees fall under the category of purposive interview recruitment. The term *purposive interview recruitment* refers to a selective process of choosing individuals for interviews (Blaikie & Priest, 2019). Based on specific criteria or characteristics, researchers can intentionally select interviewees that align with their research objectives.

The benefits of using purposive interview recruitment in this interview stage include the following:

1. I can purposefully filter interview participants who have strong expertise in cyber financial crime and filter out those who recently joined the fraud industry and may not be familiar with the technologies and policies.
2. I can improve the quality of my interview data by selecting those who can articulate their thoughts in a logical and clear way and are fluent in English.

3. I can tailor my questions based on the interviewee's expertise if I have previously worked with them.

However, purposive interview recruitment is not without its flaws. The intentional selection of interview participants based on specific criteria may limit the diversity of perspectives, potentially overlooking valuable insights from individuals with different experiences. Therefore, I have included the snowball technique as a second method for my interview recruitment.

Snowball sampling refers to first drawing a random sample of individuals from a given finite population, then having these individuals provide the names of others who were not in the random sample in the first stage. The second stage population then names the third stage population, and so on. The procedure helps researchers understand and estimate the number of mutual relationships or social circles in the population (Goodman, 1961).

The advantages of snowball sampling have been particularly evident in my project. Cyber financial crime professionals from different financial institutions might work together, for example, to tackle a cyber attack, or to adopt a new technology such as Apple Pay. Using snowball sampling as a recruitment method has efficiently helped me find interviewees to connect with. In addition, the quality of my interviews was high as the participants who were referred by other practitioners tended to be well-versed in their own areas of expertise. These interviewees delivered high-quality conversations and therefore generated useful and impactful qualitative data.

There have been two significant downsides to using a snowball sampling procedure for my project. The first resulted from the use of a non-probability sampling method. The probabilities of selecting the research participants in the sample cannot be calculated (Voicu &

Babonea, 1997). At the time of beginning the research, there was no statistical method available to determine who would be able to participate in my research project, which therefore reduced the randomness and objectivity of the data.

Secondly, Voicu and Babonea identify that participants may "hide" referrals and try to protect friends or acquaintances, and that this could be a problem when there is a concern regarding the confidentiality of data (Voicu & Babonea, 1997). This also became an issue in this project. Most of the cyber financial crime practitioners deal with confidential data, and it became hard to build interviewer-interviewee trust. Those who participated in the study might not be willing to refer others because of the potential risks involved, and it is possible that they may have been participating in the study without their colleagues knowing. They also might have been concerned about the outputs of the dissertation or simply worried that there may be unknown risks involved in referring others.

Finally, it is crucial to highlight the gender distribution in my qualitative interviews in this interview recruitment section. While I made every effort to boost the involvement of non-male participants, the distribution is still, unfortunately, unevenly distributed. Up to 75% of my interview participants identified as male. Male industry practitioners were more inclined to accept my research invitations and generally expressed a greater interest in and willingness to allocate time for the study. When unable to participate, invited male participants usually declined the invitation verbally or in writing, providing clear responses.

Conversely, female participants were less likely to accept research invitations. This led to an interesting observation from my research study: over 20 invited female participants did not even respond to the invitation. Unlike their male counterparts, who typically disclosed their participation decision explicitly, many invited female participants did not communicate their

decision of acceptance or decline, possibly because of discomfort surrounding refusing others. They may fear being perceived as impolite or worry about the potential consequences of declining. I did my best to empower the invited female participants, encouraging them to express their decisions freely without fear of judgment or repercussions. However, one of my speculations is that some might have worried about encountering me again in the industry and felt that refusing to participate in my research project could potentially create discomfort. Especially for invited participants who held a lower job rank than my current position, choosing not to respond might have seemed a preferable strategy to outright declining.

Among the decline responses received, four invited female participants mentioned their inability to participate in the research study due to family responsibilities, such as having young children to attend to. Additionally, three invited female participants explicitly stated their concern about the potential disclosure of certain information in the research, leading them to decline the research invitations. Comparatively speaking, only two invited male participants voiced concerns related to the project. Following my additional explanation and clarifications, one of them decided to participate in the study.

While the gender distribution is unequal in my research study, I did try my best to invite participants with different job functions or positions to garner different perspectives. Most of the interviews were productive, and I was able to acquire high quality interview data from these conversations.

4.6 Data Analysis

All research participants have been individually coded using serial codes generated by a code randomizer (https://www.randomcodegenerator.com/) to ensure the confidentiality of participants' identities.

All recorded calls were transcribed by Otter.ai, an artificial intelligence and machine learning-empowered transcription tool that offers real-time transcription services (Sterne & Sawhney, 2022). The Otter.ai account is secured with a strong password and enhanced by two-step verification authentication, providing a reliable layer of protection for the data. Transcription notes have been coded to protect participants' information and downloaded transcriptions were exported to password-protected Excel and Word files.

While Otter.ai is able to deliver a useful initial draft of the transcription, it lacks the capability to accurately transcribe industry jargon or effectively capture the names of commonly used software. To enhance transcription accuracy, I manually edited the generated transcriptions following their automatic generation by the transcription tool.

Calls were also recorded on a physical digital voice recorder device (Kinpee 64GB portable audio sound recorder with micro-USB port) for audio file retention purposes. The exported audio file is currently stored in an encrypted file folder on a password-protected Apple MacBook Air with biometric authentication enabled.

Interviews were conducted online or over the telephone and recorded for data analysis. The interviews were transcribed using Otter.ai and then analysed using qualitative data analysis software as well as the Microsoft Office suite. Transcripts were stored in a locked filing cabinet; electronic files are password protected; storage disks are encrypted; the data will be stored for approximately seven years for research purposes; both electronic and hard copies of data will be

destroyed on 12/31/2029. Data from this research project may be used for conferences and presentations, written papers and the dissertation, and policy reports; aliases will be used for individuals and organizations.

The documentary material was analyzed through a structured qualitative coding process utilizing ATLAS.ti and the Microsoft Office suite, employing a multi-stage and iterative coding design that integrated deductive, inductive, and relational coding strategies. Instead of treating the documents as mere contextual or descriptive background, they were systematically coded as empirical data in their own right. Each document was segmented into meaningful units—such as sentences, paragraphs, or functional sections—before coding. These segments were subsequently assigned multiple codes, where appropriate, facilitating overlapping interpretations of actors, technologies, practices, vulnerabilities, institutional responses, and relational dynamics pertaining to cyber financial crime. The codebook containing child code items is attached as Appendix A in this dissertation. The coding process has enabled me to systematically organize the data, which later helped me to categorize the results using assemblage thinking and create a multiscale cyber financial crime assemblage.

Table 4. Overview of Coding Themes

Code	Theme Description
T1	(Mis)users
T2	Technology and Strategies
T3	Policies and Strategies
T4	Customer Experience
T5	Authentication
T6	Human Vulnerabilities
T7	Automation

The initial coding phase implemented open coding, strategically attaching descriptive labels to discrete empirical references within the data. This approach generated a dynamic and comprehensive code set that captures a wide array of observable entities and actions, including

specific fraud techniques, authentication mechanisms, customer behaviors, institutional controls, and technological interventions.

Following this initial stage, an axial coding process was implemented to organize related open codes into larger conceptual categories. This methodology resulted in the identification of seven parent code families: (1) misusers, (2) technology strategies, (3) policies and strategies, (4) customer experience, (5) authentication, (6) human vulnerabilities, and (7) automations. These parent codes acted as organizing nodes, linking disparate empirical observations across various documents and enabling comparisons across different institutional contexts. Within each parent code, multiple child codes were developed to capture nuances and specificity. For example, under the category of "misusers," the child codes included Cybercriminals, Hackers, Customers, Client Intentional (CI), First Party Fraud, Misuse, Abuse, and Take Advantage.

A further stage of selective and relational coding was then undertaken to identify how coded elements interacted across categories. At this stage, codes were not only grouped but also linked through ATLAS.ti network views, allowing relationships such as dependency, escalation, substitution, and vulnerability exploitation to be explicitly mapped. For instance, links were created between "human vulnerabilities" and "social engineering," between "automation systems" and "false positive fraud detection," and between "policy constraints" and "authentication friction." These relational links were used to move beyond thematic categorization toward an analysis of how components co-constituted cyber financial crime assemblages.

During the initial structuring of the dataset, the coded material was also organized into five process oriented analytical phases: vulnerability, exploitation, investigation, adjudication, and restoration. These phases were used as a secondary coding lens to identify where and how

coded elements appeared within broader cyber financial crime processes. In ATLAS.ti, this was operationalized through code grouping and temporal sequencing of coded segments, allowing the same code (e.g., “authentication failure”) to be examined across multiple phases of the fraud lifecycle. However, as coding progressed, it became evident that many coded elements were not phase-bound but instead operated across multiple stages simultaneously, leading to frequent cross-phase code co-occurrence.

In response, the analysis shifted toward a more relational and assemblage-based coding structure. Parent and child codes were re-mapped using ATLAS.ti network analysis tools and visualized through mind maps. Finally, the coded dataset was reinterpreted through the four analytical characteristics used in the dissertation—heterogeneity, multiplicity, affectivity, and fluidity. This involved re-examining coded relationships to identify how different components gained analytical significance through their connections rather than their isolated presence. The iterative movement between open coding, axial structuring, relational linking, and assemblage mapping—supported by ATLAS.ti’s coding, query, and network functions—formed the methodological foundation through which the empirical findings and assemblage constructions presented in the dissertation were developed.

4.7 Research Ethics

Social researchers must balance the anticipated research benefits against any potential physical, psychological, social, political, economic, or legal harm the research may cause (Blaikie & Priest, 2019). Ethical practices in research help to protect individuals, communities, and the environment and to avoid (or at least minimize) long-term, systematic harm (Israel & Hay, 2006).

I have received ethics approval for this project from the Office of Research Ethics (ORE) at York University. This project is defined as minimal risk and does not involve any clinical trials.

I provided interviewees with the Research Project Information Sheet and an Informed Consent Form prior to the initial interview. All interviewees were required to sign the informed consent form. As some of the participants were previously known to the principal investigator, the following steps were taken:

- Oral consent and verbal agreements are not considered sufficient evidence of consent in this project. Thus, consent must be given voluntarily without any undue influence.
- All informed consent forms would be sent to participants' email addresses.
- All signed consent forms would be safely filed and stored.

Prior to each interview, I proactively identified questions that would potentially induce negative emotional reactions and made sure to handle such questions with caution. Recruitment materials explicitly clarified that participation was unrelated to any professional, supervisory, academic, or personal obligations, and that the investigator held no evaluative authority over participants in the context of this study. Invitations were framed as optional requests rather than direct solicitations, and participants were encouraged to consider participation privately and respond at a later time rather than immediately. Throughout each interview, I consistently monitored participants' emotional reactions and provided frequent breaks as needed. In closing, I would re-emphasize that all data would be securely stored confidentially and that the participant had the right to withdraw from the study at any time.

If the participant named their institution or provided identifying information, the data were de-identified and stripped of all identifiable information and related elements. All

identifiable characteristics that could be potentially linked to an individual or an organization have been replaced with pseudonymized data. Identifiable information relating to pseudonymized data has been stored and protected separately in a password-protected file.

I have completed the following steps to address any potential conflicts of interest. I acknowledged the potential conflicts of interest and that participants may feel social pressure to participate. I provided the decline option in the interview invitation. I avoided making assumptions or judgment when collecting data. I consciously resisted incorporating personal opinions when analyzing data. And I periodically reviewed potential conflicts of interest and worked to learn from any errors or missteps.

During the ethics approval process, the ethics committee voiced concerns about the potential for involuntary participation in the research project, specifically addressing issues such as participants feeling pressured to join, particularly among colleagues with whom I have personal connections. To manage this potential risk, I have ensured that all interviewees understood their informed consent and were explicitly advised that they have the option to decline the opportunity to participate in the study and withdraw at any time with no consequences. In the end, I utilized the snowball sampling technique more than I originally anticipated, which helped manage the risks. Even though I know many fraud professionals in the field, I minimized collecting data directly from known contacts. Instead, I leveraged my contacts' networks to snowball sample appropriate interviewees.

In some cases, my identity as a Manager of Strategic Initiatives with a major financial institution raised suspicions from prospective interview participants when I attempted to recruit them. Some worried that my research might potentially collect proprietary information that would benefit another financial institution, and they therefore declined to participate. Some

prospects asked for financial compensation, which I declined. As declared in my research ethics applications, I could not offer any inducements to participants such as money, gift certificates, or academic credit. Participation in the study was entirely voluntary with no financial compensation, and refusal to participate carried no consequences. Potential interviewees were initially contacted via email, followed by further communication by email or telephone where appropriate. All written communication clearly described the purpose of the study, the voluntary nature of participation, and participants' right to decline or withdraw at any stage without penalty.

My professional position and managerial rank within the financial services industry may also have influenced how interview participants understood the research relationship and shared their experiences. Participants who were aware of my industry background may have perceived me as holding professional authority, institutional knowledge, or access to industry networks, even when I had no direct supervisory or decision-making relationship with them. This perceived difference in position may have encouraged participants to present institutionally acceptable views, withhold criticism, or limit the disclosure of sensitive operational concerns. To reduce this influence, participants were informed that their participation was voluntary, that they could decline to answer any question or withdraw from the study, and that their responses would remain confidential and would not affect their employment or professional relationships. Nevertheless, the possibility of self-censorship, social desirability, or strategic disclosure cannot be fully eliminated and is recognized as an ethical and methodological limitation of the qualitative data collection process.

4.8 Considerations and Limitations: Positionalities

Several considerations and limitations shape this dissertation and warrant explicit reflection. As an independent researcher, I have not received external funding from any organization or institution. Although I am employed as an industry practitioner within the private sector, I deliberately chose not to accept funding from any financial institution in order to preserve the intellectual independence of the project and to retain autonomy in determining its analytical focus, scope, and direction.

As a social science-based qualitative study, this research requires careful articulation of researcher positionality. Positionality refers to the researcher's worldview and the position they occupy in relation to the research topic and its broader social and political contexts (Foote & Gau Bartell, 2011; Rowe, 2014, as cited in Holmes, 2020; Savin-Baden & Major, 2013). These positions are not static; they are shaped by prior training, professional experience, and institutional location, and they influence how research questions are framed, how data are interpreted, and how findings are presented.

Closely related is the concept of reflexivity, understood as an ongoing process of critically examining one's assumptions, actions, and interactions throughout the research process (Corlett & Mavin, 2018). Reflexivity involves continuous attention to how epistemological commitments, professional identities, and affective responses may shape data generation and analysis, including how the researcher engages with participants and how meaning is co-produced during interviews.

In reflecting on my positionality, I recognize that I occupy multiple, intersecting roles that carry both analytical advantages and limitations. As an STS scholar with formal training in criminology and cybercrime, my academic background equips me to examine how crime,

technology, and governance are co-constituted. My criminology training supports an understanding of how criminalization, responsibility, and harm are socially produced, while my STS orientation sensitizes me to how digital technologies, classifications, and institutional practices shape the enactment of cyber financial crime. This interdisciplinary positioning allows me to question why certain forms of cyber financial crime are framed as more severe or legitimate objects of intervention than others, and how such distinctions are stabilized in practice.

At the same time, my professional experience as an industry practitioner introduces potential constraints. Familiarity with fraud operations may shape how I interpret documents and interview data, particularly when encountering practices that align closely with my prior experience. Given the volume of qualitative data encountered during this research, it is neither possible nor desirable to include all available materials. While care was taken to maintain analytical rigor, some selections inevitably reflect my situated understanding of cyber financial crime. For example, this dissertation engages less deeply with cybersecurity infrastructure research, reflecting the fact that my professional expertise lies primarily in fraud operations rather than technical cybersecurity domains.

Another consideration concerns the interview dynamic itself. During interviews, participants frequently sought affirmation or confirmation through verbal cues such as “you know?” or “right?”, suggesting an assumption of shared professional understanding. My role as an industry practitioner may have contributed to this interactional dynamic, potentially shaping how participants articulated their experiences or justified their decisions. While this shared familiarity facilitated rapport and depth of discussion, it may also have influenced what participants assumed did not require elaboration.

In addition, feedback from peers and committee members indicated that my writing style and terminology at times reflected business or professional discourses more than conventional social science prose. While this orientation can enhance clarity for practitioner audiences, it also risks narrowing interpretive space or unintentionally importing industry framings into the analysis. To engage reflexively with this influence, I adopted several methodological strategies. Beyond iterative textual revision, I maintained analytic memos throughout the research process to document moments where professional assumptions, institutional logics, or taken-for-granted categories appeared to shape my interpretations. I also made a deliberate effort to approach assemblages through multiple conceptual lenses—experimenting with different ways of mapping relations, identifying elements, and tracing processes of stabilization and change—in order to avoid defaulting to familiar institutional perspectives. For example, in the early stages of the project, I organized the empirical field into multiple sub-assemblages, reflecting my professional habit of analyzing systems according to distinct business units and functional divisions. Through ongoing theoretical engagement and revision, however, I reconsidered this structure and ultimately adopted a single, larger assemblage framework, as it better captured fluidity across institutional boundaries and more effectively demonstrated multiplicity and relational interdependence. Theory was thus used not simply as a lens but as a resource for questioning industry narratives that might otherwise seem self-evident. During data analysis, I paid particular attention to instances where my professional experience aligned too neatly with participants' accounts, treating these moments as prompts for further interrogation rather than confirmation. Ongoing discussions with doctoral peers, committee members, and scholars outside the financial sector further supported this reflexive process, helping to identify where terminology,

assumptions, or problem framings required rearticulation to enhance conceptual precision and accessibility.

My insider experience and professional expertise within the financial services industry created both the opportunity for this research and an important analytical resource for undertaking it. My familiarity with fraud operations, institutional terminology, technological systems, policy development, organizational routines, and industry ways of working allowed me to understand comments that may not have been immediately meaningful to an external researcher. It enabled me to recognize indirect references, interpret technical and operational language, and identify relationships among policies, technologies, organizational priorities, and fraud management practices. This situated knowledge also provided access to first-hand institutional accounts that are often difficult for researchers outside the financial sector to obtain and interpret. Without this experience, many of the practices examined in the dissertation may have remained within an institutional black box, either inaccessible or insufficiently understood.

At the same time, my insider position shaped how the data were interpreted and created the risk that my own professional knowledge could extend beyond what participants had directly stated. Familiarity with institutional practices sometimes made particular interpretations appear self-evident because they corresponded with my own experience, even where they were not fully supported by the interview data. I therefore sought to distinguish between findings grounded in participants' accounts and observations informed primarily by my practitioner knowledge. This required ongoing reflexivity concerning when my experience strengthened the analysis and when it risked introducing assumptions, subjectivity, or bias. My practitioner perspective also directed greater analytical attention toward institutional concerns such as fraud prevention, operational effectiveness, regulatory compliance, resource allocation, technological control, and financial

loss. Consequently, the analysis may provide greater visibility to organizational decision-making than to the experiences of victims, customers, and actors situated outside formal industry structures.

My insider position also imposed boundaries on what could be disclosed, criticized, and examined in detail. As an employee of a financial institution, I remained subject to confidentiality, privacy, security, and professional obligations that restricted how internal practices, operational processes, technological vulnerabilities, and institutional concerns could be presented. Public criticism of my employer or detailed discussion of fraud controls could create professional consequences, reputational risks, deductive identification of participants, or knowledge that may be used by malicious (mis)users to evade institutional systems. For these reasons, certain findings are discussed at a conceptual level rather than through detailed procedural explanations, and some institutional criticisms could not be developed as fully or explicitly as they might have been from a position outside the industry. These omissions do not show a lack of knowledge or understanding. Instead, they highlight the challenges of insider research. When researchers have expertise in a certain area, they can access and interpret information well. However, their professional, ethical, and security responsibilities also limit what they can share.

Finally, the analytical framework developed in this dissertation is necessarily partial and provisional. Cyber financial crime is a continually evolving phenomenon, shaped by creative practices, technological change, and shifting institutional responses. My professional experience is grounded primarily in the Canadian context and within a limited number of financial institutions, which constrains the horizontal and comparative scope of the analysis. As such, the assemblage-based analytical framework proposed here should be understood not as definitive,

but as open to revision and extension. This openness is a central strength of assemblage thinking, which accommodates modification, expansion, and reconfiguration as new practices, actors, and relations emerge through the ongoing becoming of cyber financial crime.

4.9 Conclusion

This Research Design and Methods chapter has outlined the qualitative methodologies deployed in this doctoral project to examine cyber financial crime as a dynamic and evolving sociotechnical phenomenon. The research design is structured across three interconnected phases. Phase I employed document analysis to develop a contextual and analytical grounding for the study through engagement with formal and informal texts related to cyber financial crime in Canada. Phases II and III built upon this foundation through semi-structured interviews with fraud industry practitioners working within Canadian financial institutions, enabling an in-depth examination of how cyber financial crime is enacted, interpreted, and governed in practice.

The chapter has detailed how data were systematically collected, organized, and analyzed across these phases using qualitative research tools appropriate to an assemblage-oriented approach. Instead of treating methods as discrete or linear steps, the research design supports iterative movement between documents, interviews, and analysis, allowing empirical insights to inform subsequent data collection and refinement of analytical focus. This design enables sustained attention to heterogeneity, multiplicity, affectivity, and fluidity, and to the ways in which cyber financial crime is continually reconfigured through everyday practices, institutional judgments, and (mis)user-driven innovation.

The chapter has also addressed key ethical considerations and reflected critically on researcher positionality. My dual position as an industry practitioner and independent researcher

introduces both analytical strengths and methodological constraints, which have been explicitly acknowledged and managed through reflexive engagement, transparent methodological choices, and iterative peer and supervisory feedback. To summarize, the research design and methods presented in this chapter establish a rigorous and flexible foundation for the empirical chapters that follow, supporting an analysis of cyber financial crime not as a fixed object of governance, but as an assemblage in ongoing processes of becoming.

The following chapters transition from methodological design to empirical analysis. Utilizing the document analysis and interview data introduced in this chapter, the empirical sections explore cyber financial crime through four analytical dimensions: heterogeneity, multiplicity, affectivity, and fluidity. Each chapter delves deeply into one of these characteristics, illustrating how cyber financial crime unfolds through dynamic configurations of actors, technologies, practices, and institutional judgments. Instead of viewing these characteristics as mere abstract theoretical constructs, the empirical analysis reveals how they arise from and are reinforced by everyday practices and (mis)user-driven innovations, collectively enhancing our understanding of cyber financial crime as a complex assemblage in continuous processes of becoming.

Chapter 5 - Heterogeneity: Assembling Elements and Differences

5.1 Introduction

In *A Thousand Plateaus,* Deleuze and Guattari describe complex social systems as assemblages composed of diverse and unlike elements that co-function. An assemblage is defined as "a multiplicity which is made up of many heterogeneous terms and which establishes liaisons, relations between them" (Deleuze & Parnet, 2007, p.69). Deleuze and Guattari use the term *heterogeneous* to convey that an assemblage is not a single, unified object with simple, linear connections; elements of different kinds dynamically interact to produce effects that no individual component could generate on its own. One of the key characteristics of an assemblage is this heterogeneity, in which human and non-human elements—social practices, material infrastructures, technologies, and discourses—co-function to create relations and outcomes that are contingent, emergent, and irreducible to any one part (Deleuze & Guattari, 1987).

Seeing assemblages through the lens of heterogeneity enables a methodological practice that closely examines how relations and performances unfold across human and non-human, organic and inorganic, and technical and natural domains (Anderson & McFarlane, 2011). By examining these heterogeneous elements, the practices of the assemblage emerge as processes of continual becoming: contingent achievements that resist pre-existing analytical categories and challenge any single, privileged first principle of social explanation (Sullivan, 2022). This perspective underscores that what appears to be a stable social formation is, in fact, the outcome of ongoing negotiations among diverse actors and forces (Anderson & McFarlane, 2011).

Similarly, when conducting a social analysis of cyber financial crime, it is essential to recognize the constitutive yet contingent elements that continually shape distributed relations within the assemblage (Law et al., 2012). The cyber financial crime assemblage is not merely a

group of cybercriminals, a set of exploitative malicious codes, or a collection of vulnerable financial instruments. Nor is it a linear chain of events or a fixed pattern of criminality in cyberspace. Instead, the cyber financial crime assemblage represents an active ordering and reordering of documents, codes, people, and practices. These heterogeneous elements both perform and (de)stabilize relations within the cyber financial crime assemblage. The ongoing accomplishment is driven by heterogeneous elements, including legal and technical, human and non-human, and material and discursive forces.

In this chapter, I present empirical findings that illuminate the key heterogeneous elements of the cyber financial crime assemblage. By "following the actors," I trace relations across legal texts, regulatory documentation, technological infrastructures, malicious codes, institutional practices, and financial instruments, assessing how these elements enact and reshape connections. This examination of heterogeneity reveals that the cyber financial crime assemblage is not a static, descriptive list, but an active configuration continually enacted by diverse categories of actors.

The cyber financial crime assemblage is provisional in the sense that its alignments are always temporary and contingent upon ongoing coordination among people, technologies, and regulatory frameworks. These alignments hold only so long as practices unfold in anticipated ways. When (mis)users engage financial services and products in unintended ways, existing arrangements are disrupted, and previously stabilized relations begin to unravel. (Mis)user-driven innovation unsettles earlier temporary stabilizations and initiates a reconfiguration of relations among heterogeneous elements: legal documents are rewritten or reinterpreted, technological infrastructures are patched or redesigned, institutional practices are reviewed and revised, and new authentication mechanisms are introduced. Through these ongoing adjustments,

the heterogeneous elements of the cyber financial crime assemblage continually perform and generate new networks of connection and effect, producing fresh, contingent, yet consequential configurations that reshape the assemblage itself.

This chapter argues that the cyber financial crime assemblage is inherently heterogeneous, composed of materially and socially diverse elements that do not share a single logic, temporality, or mode of operation. Documents, technical artifacts, financial instruments, regulatory texts, and human practices differ in form, institutional location, and capacity to affect and be affected. In this context, autonomy does not mean independence from others. Instead, it refers to the way these heterogeneous elements remain distinct enough to act in ways that are not fully determined by the assemblage they temporarily compose. Their capacities therefore exceed any single configuration, allowing them to be detached, reinterpreted, and rearticulated in new arrangements (Deleuze & Guattari, 1987).

Because these elements are never fully absorbed into a unified system, the assemblage does not hold together through fixed structure. Instead, it depends on continuous work: coordination, negotiation, and adjustment among heterogeneous parts (DeLanda, 2006). What appears as order is therefore an ongoing accomplishment rather than a stable condition. By examining how documents, technologies, financial instruments, regulatory texts, and human practices interact and sometimes disrupt one another, this chapter shows that stability in cyber financial crime governance is always provisional—an effect of temporary alignment among unlike elements, not a settled or coherent whole (Law & Mol, 1998; Law & Singleton, 2014).

5.2 The Documented Words: Defining Legal and Regulatory Documents

Briassoulis argues that much governance and policy research operates from a system ontology, treating governance as a fixed and stable structure (Briassoulis, 2019). As a result, policy and regulatory frameworks are often detached from the complex, context-specific settings in which heterogeneous elements frequently interact to produce emergent effects and transform sociotechnical or socio-cultural arrangements. This approach often produces uniform and inflexible applications of policy that overlook diversity, infrastructural influences, and shifting power relations. In contrast, Briassoulis proposes assemblage thinking as a methodological approach for tracing how governance is enacted in practice by following actors, relations, and infrastructures, rather than treating governing documents as expressions of a singular, centralized process. Guided by this perspective, this dissertation examines cyber financial crime through an assemblage thinking lens to show how institutions, rules, and documents co-constitute its governance as a dynamic and continually evolving phenomenon.

Within the cyber financial crime assemblage, multiple governing documents operate across institutional levels to guide policies and responses. These range from international agreements to the Canadian Criminal Code and from law enforcement bodies such as the Royal Canadian Mounted Police (RCMP) to coordinating organizations like the Canadian Anti-Fraud Centre (CAFC), each approaching cyber financial crime from a distinct institutional standpoint. While core understandings may overlap, some frameworks prioritize specific technical mechanisms or behavioural indicators in assessing offence severity, whereas others concentrate on institutional consequences, including sanctions, liability, or regulatory response. These variations in emphasis nonetheless shape how cyber financial crime is interpreted, categorized, and governed in practice.

International Treaties and Organizations

The first international treaty specifically addressing cybercrime, the Convention on Cybercrime—commonly known as the Budapest Convention—was signed on November 23, 2001. It was developed under the leadership of the Council of Europe, which coordinated negotiations among member states and invited participation from non-European countries such as Canada, the United States, and Japan. The Council of Europe provided the institutional forum through which legal experts worked to harmonize national laws, define core cybercrime offences, establish investigative powers, and create mechanisms for international cooperation. The treaty defines cybercrime offences to include illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery and fraud, child exploitation offences, and copyright-related offences (Council of Europe, 2001). In this way, the Budapest Convention functions both as a legal framework and as a cooperation mechanism, shaping how states structure domestic cybercrime legislation and collaborate across borders in investigation and enforcement.

What cyber financial crime means to the Council of Europe is highly correlated to the concept of cybercrime, which comes down to "action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct" (Council of Europe, 2001).

In its 2001 definition, the Council of Europe describes cybercrime in terms of activities involving computer systems, networks, and computer data. This formulation can be read as pointing to a set of heterogeneous elements that operate together to produce effects such as illegal access and interception, interference with data or systems, and the misuse of devices and

content. From an assemblage perspective, these elements—technical infrastructures, data flows, and mediated practices—are not arranged in a fixed hierarchy, nor does any single component determine outcomes on its own. Instead, cybercrime emerges through the interaction and alignment of multiple, distinct elements whose roles and significance shift depending on context. Viewed through the lens of assemblage thinking, these heterogeneous elements draw attention to "the creative capacities of matter and energy, and the processes that instantiate them in their great variety," showing how cybercrime emerges from the dynamic interplay of diverse human and technological forces (Acuto & Curtis, 2014). This perspective opens the possibility of moving beyond state-centric or fixed-structure understandings of cybercrime, allowing for a more nuanced analysis that accounts for the contingent, evolving relations.

One important implication is that cyber financial crime cannot be seen as a fixed category that exists on its own, separate from the practices, technologies, and institutional interpretations that shape it. Instead, it should be viewed as a result of the alignment among various elements, including legal definitions, technical infrastructures, user behaviours, organizational procedures, and regulatory decisions. What counts as an offence, a vulnerability, or a harm therefore depends on how these elements are temporarily stabilized in particular contexts. This shifts analytical attention from asking what cybercrime is in abstract terms to examining how it is enacted, recognized, and governed through situated sociotechnical arrangements. Such an approach makes visible the processes through which responsibilities are assigned, risks are calculated, and interventions are justified, while also highlighting why these arrangements remain open to disruption, reinterpretation, and reconfiguration over time.

Canada, Criminal Code, and More

The Convention on Cybercrime offers a forum called the Cybercrime Convention Committee (T-CY) where participants can collaborate with confidence, trust, and efficiency. T-CY consists of 77 States either participating as members (Parties) or observers (signatories or invitees), and the committee remains the most relevant intergovernmental body dealing with cybercrime (Council of Europe, 2023). T-CY members work together to exchange information on cybercrime detection and investigation, facilitate the adequate implementation and utilization of the Convention, and offer feedback and recommendations for future amendments (Council of Europe, 2023).

Canada signed the Convention as an observer state in 2001 and ratified membership in July 2015 (Government of Canada, 2015). As an active T-CY participant, one of the most important legislative steps Canada has taken to make the ratification happen has been to introduce the Protecting Canadians from Online Crime Act S.C. 2014, c. 31 (Government of Canada, 2014b). The enactment amends the Criminal Code to further define criminal acts in cyberspace, for example, by outlining non-consensual distribution of intimate images as a new offence and granting agencies the authority to remove such images from the internet; by providing the power to demand and preserve electronic evidence, communication data, and transaction locations; and by streamlining the process of obtaining warrants and orders related to authorization to intercept private communications.

These changes have had direct implications for cyber financial crime. By formally recognizing digital data, communication metadata, and transaction information as objects of legal intervention, the amendments expanded the range of evidentiary elements through which financially motivated cyber offences could be detected, investigated, and adjudicated. Activities

such as online fraud, identity misuse, and unauthorized financial access increasingly came to be governed through data preservation orders, production demands, and digital trace analysis. In this way, the legal adjustments did not merely redefine cybercrime in abstract terms; they reconfigured the practical conditions under which cyber financial crime could be assembled as a legal object, thereby shaping what counted as evidence, how responsibility could be attributed, and how investigative authority could be exercised.

The Criminal Code of Canada has thus evolved its conception of cybercrime in dialogue with the 2001 Council of Europe framework. As Canadian law has adapted to digital environments, both the understanding of cybercrime and the mechanisms used to govern it have shifted alongside broader sociotechnical developments. Viewed through the lens of assemblage thinking, the evolution reflects the dynamic character of assemblages. In this case, the Criminal Code increasingly incorporates digital traces such as electronic evidence, communications data, and transaction records into the legal infrastructure that stabilizes cyber financial crime as a governable category. Prior to the digital era, the Criminal Code largely addressed conventional, physically situated offences, leaving a gap in how technologically mediated harms were conceptualized and managed (Dass, 2019). The incorporation of digital evidentiary elements marks a shift from this earlier focus, aligning legal mechanisms with the sociotechnical conditions under which contemporary cyber financial crime emerges.

Viewed through assemblage thinking, heterogeneous elements enter into relations whose liaisons generate temporary alignments, giving the assemblage a degree of coherence even as it remains unstable and open to change (Deleuze & Guattari, 1987). Because these elements may be material or discursive, organic or technological, Canada’s ratification of the Convention on Cybercrime (T-CY) can be understood as the introduction of additional components into the

cybercrime assemblage. This did not simply add legal rules but brought new actors, evidentiary practices, institutional procedures, and technical mechanisms into relation with existing ones. From this perspective, ratification reconfigured how elements interact within the assemblage, producing new arrangements that continue to reshape how cybercrime is interpreted, investigated, and governed in legal and regulatory contexts.

Major laws and regulations covering cybercrime in Canada include but are not limited to the Criminal Code, the Royal Canadian Mounted Police Act, the Firearms Act, and the Safe Streets and Communities Act (Public Safety Canada, 2016). The highest law enforcement agency in Canada, the RCMP, is responsible for ensuring Canadian public safety in relation to serious and organized crime and to financial crimes and criminal activities (Royal Canadian Mounted Police [RCMP], 2023). The RCMP's 2021-22 Departmental Plan states that its new National Police Service, the National Cybercrime Coordination Unit (NC3), reached its initial operating capability in 2020 (Minister of Public Safety and Emergency Preparedness, 2021). Since then, the NC3 has coordinated investigations across multiple agencies and supported prosecution of multi-jurisdictional and international pandemic-related cybercrimes (Minister of Public Safety and Emergency Preparedness, 2021). The NC3 shares intelligence and facilitates the notification of cybercrime victimization with Canadian businesses and individuals (Minister of Public Safety and Emergency Preparedness, 2021). In the coming year (at the time of writing this dissertation), the NC3 aims to continue developing the National Cybercrime and Fraud Reporting System for Canadian victims of cybercrime, and to offer technical assistance for cybercrime investigations (Minister of Public Safety and Emergency Preparedness, 2021). Through the fraud reporting system, NC3 collects a growing range of fraud and scam cases reported by victims, including techniques that may not have existed previously.

(Mis)user-Driven Innovation: Evolving Cyber Elements, Strategies, and Collaborations

As (mis)users began adopting digital technologies in diverse and often unexpected ways, they prompted legal reforms and policy updates to address emerging technological risks. Over the past two decades, international and regional bodies have likewise introduced new policies and regulatory frameworks that continue to reshape the governance of cybercrime (Broadhurst, 2006). The European Union, for example, adopted Directive 2013/40/EU on attacks against information systems and later advanced both the Cyber Resilience Act and the Digital Operational Resilience Act (DORA) to impose horizontal cybersecurity requirements and strengthen technology risk management in the financial sector. Specifically, DORA sets out six core pillars—an ICT risk management framework, ICT-related incident reporting, digital operational resilience testing, ICT third-party risk management, information and intelligence sharing, and oversight of critical third-party providers—all aimed at safeguarding the financial ecosystem's cybersecurity and protecting entities such as banks, insurance companies, investment firms, crypto-asset service providers, and technological service providers including cloud platforms (European Insurance and Occupational Pensions Authority, 2025).

Organizations such as the United Nations Office on Drugs and Crime (UNODC), Interpol, and the Association of Southeast Asian Nations (ASEAN) have developed and revised cybercrime frameworks, capacity-building initiatives, and cooperative mechanisms to strengthen cross-border policing and regulatory coordination. These efforts extend cybercrime governance beyond criminalization to include institutional practices, technical standards, and shared expectations around cybersecurity resilience and information sharing.

For example, UNODC's Global Programme on Cybercrime provides technical support and capacity building to member states across legislative development, international cooperation, prevention, and operational assistance, including tools such as the Mutual Legal Assistance Request Writer Tool (UNODC, n.d.). Interpol's Project Gateway facilitates transnational cybercrime investigations through coordinated intelligence sharing and operational collaboration among law enforcement agencies (Interpol, n.d.). At the regional level, the ASEAN Cybersecurity Cooperation Strategy promotes collective capacity building, incident response coordination, and policy dialogue among member states, linking cybersecurity governance to broader regional digital integration efforts (ASEAN, n.d.).

Taken together, these initiatives illustrate how cyber financial crime governance is enacted through the interaction of heterogeneous human and non-human elements, including international organizations, legal texts, investigative tools, digital infrastructures, and institutional practices. These efforts broaden legal definitions of cybercrime, incorporate technical standards and resilience requirements into law, and promote multi-stakeholder collaboration. In doing so, they highlight how heterogeneous human and non-human elements—from legal texts and regulatory institutions to technological infrastructures—continually reshape and reconfigure the global cyber financial crime assemblage.

Collaborative arrangements for cross-border cooperation in cybercrime policing have become more prominent with the expansion of digital networks and transnational online activity. While earlier forms of international policing cooperation existed, the scale, speed, and technical complexity associated with cybercrime have prompted new collaborative practices and governance arrangements. Innovation within these contexts is often shaped by multiple drivers, including cost considerations (price-driven innovation), technological developments

(technology-driven innovation), and practices emerging from users' engagement with systems and infrastructures (user-driven innovation) (Jensen, 2012). Jensen argues users may have unacknowledged needs which may eventually lead to innovations (Jensen, 2012). Research by anthropologist Suchman at XEROX illustrates how users can drive changes to products and system designs, as well as rules of using technologies (Suchman, 1983). In this research at XEROX, while system designers acknowledged the importance of procedural tasks in office environments, they overlooked the actual day-to-day routines required to complete those administrative tasks and the implications the machine could bring to the social environment in the office.

Viewed through this lens, cross-border cybercrime governance can be understood as similarly shaped by practices that exceed institutional design. Collaborative frameworks, investigative tools, and procedural rules evolve not only through formal agreements and technological upgrades, but also through the adaptations, improvisations, and workarounds of those who use them. This perspective supports the argument that innovation in cyber financial crime governance is not solely top-down or technology-led but also emerges from the distributed practices of actors operating within and across institutional arrangements.

Similarly, early designers of digital financial systems did not anticipate the scale of financially motivated cybercrime that would later emerge. For instance, phishing attacks targeting online banking customers began to appear in the late 1990s and grew rapidly in the early 2000s, exploiting email systems and web interfaces to harvest credentials and facilitate unauthorized financial transfers (Furnell, 2007). However, many of the legal and regulatory tools used to address these practices developed later. In Canada, for example, the Protecting Canadians from Online Crime Act expanded investigative powers related to digital evidence and

communications data, while anti-spam legislation such as CASL addressed certain deceptive electronic communications practices only after phishing had already become a widespread method of financial fraud (Canada's Anti-Spam Legislation, 2014; Protecting Canadians from Online Crime Act, 2014). Governance responses therefore evolved in reaction to the operational realities of cyber financial crime rather than in anticipation of them, illustrating how regulatory frameworks tend to co-develop with, rather than precede, emerging criminal practices.

In Canada, the meaning of cybercrime has expanded alongside the increasing integration of digital technologies into everyday social and economic life. Earlier understandings often focused on crimes targeting computer systems or using computers as instrumental tools. By January 2023, however, the RCMP defined cybercrime as "any crime where a cyber element has a substantial role in the commission of a criminal offence," where a cyber element includes the internet and devices such as computers, tablets, and smartphones (RCMP, 2023). This broader formulation reflects the widespread adoption of mobile devices, online platforms, digital banking, and e-commerce infrastructures. Practices such as online-enabled fraud, phishing, account takeovers, and platform-based financial exploitation proliferated as these technologies became routine features of everyday life, extending criminal activity beyond earlier computer-centred understandings. The RCMP's revised definition therefore corresponds to an expanded field of digitally mediated harms and uses that were not fully anticipated in earlier system designs or crime classifications (RCMP, 2023).

From an assemblage perspective, the importance of this shift lies in the relation between these sociotechnical developments and the subsequent rearticulation of governance categories. The definitional revision does not itself produce change; rather, it represents an institutional effort to stabilize an object that has already been reconfigured through evolving practices. As

heterogeneous elements—devices, platforms, users, institutional procedures, and regulatory instruments—enter into new relations, previously stabilized understandings of cybercrime are unsettled and reassembled (Carter, 2018; Deleuze & Parnet, 2007). Policies emerge through ongoing processes of translation, embedding, and legitimation across institutional and material arrangements, remaining subject to continual evaluation and reformulation (Lysgård, 2019). The RCMP's expanded definition thus reflects how (mis)user-driven innovation and technological change rework the boundaries of cybercrime over time. In this sense, cyber financial crime is not a fixed object but an evolving arrangement—an instance of what assemblage scholarship describes as an ontology of becoming in which diverse material and human components form provisional yet productive configurations that enable action while generating new forms of agency (Briassoulis, 2019).

In addition to the Criminal Code of Canada, the Canadian Anti-Fraud Centre (CAFC) is the primary federal agency providing information and support to victims of cyber financial crime. CAFC functions as Canada's central repository for collecting and organizing data related to fraud. It is jointly managed by the RCMP, the Competition Bureau of Canada, and the Ontario Provincial Police (Canadian Anti-Fraud Centre, 2020). The platform enables Canadians to report suspected fraud, access educational materials, and adopt preventative practices. It presents scam information through multiple classificatory formats, including alphabetical listings, delivery methods, target populations, and categories such as identity theft and financial fraud (Table 5).

Table 5. Canadian Anti-Fraud Centre Frauds by Medium

Email and text frauds	Internet frauds	Mail frauds	Phone and fax frauds
Bomb threat	Business grants and loans	Extortion	Air duct cleaning
Business executive spoof and wire fraud	Card-not-present	Fake business proposals	Bank investigator
Car wrapping	Charity and donation	False billing	Calls targeting the Asian community
Card-not-present	Counterfeit merchandise	Foreign money offers	Canada Revenue Agency
Charity and donation	Cryptocurrency	Inheritance	Card-not-present
Denial of Service (DOS)	Extortion	Job	Charity and donation
Emergency	Fake grant	Mystery shopper	Collection agency
Explicit video	Financial agent	Prize	Directory
Extortion	Franchise/businesop portunity	Psychic	Emergency
Fake business proposals	Government documents, help with		Extortion
False billing	Government grant		False billing
Financial agent	Immigration website		Franchise/businesopportunit
Financial industry client spoof	Initial Coin Offerings		Gem
Foreign money offers	Investment		Grandparent scam
Grandparent scam	Job		Head office spoof
Hitman	Job: counterfeit cheque		Hostage
Hostage	Loan		Hydro
Inheritance	Merchandise		Immigration extortion
Initial Coin Offerings	Pardon		Investment
Investment	Prize		Low interest rate offers
Job	Ransomware		Office supplies
Merchandise	Romance		Personal information
Mystery shopper	Service		Ponzi
Payroll spoof	Sextortion		Prize
Phishing	Subscription trap and continuity		Prize winner call
Ponzi	Tech support		Pump and dump
Prize	Vendor fraud		Pyramid
Pump and dump	Weight loss grants		Recovery pitch
Pyramid			Resale
Romance			Service
Spear phishing			Sim card swap
Supplier/contractor swindle			Taxpayer
			Tech support
			Timeshare resale
			Timeshare Vacation

Note. Adapted from “Frauds by Medium,” by the Canadian Anti-Fraud Centre, n.d., Canadian Anti-Fraud Centre. https://www.antifraudcentre-centreantifraude.ca/scams-fraudes/medium-moyen-eng.htm

From an assemblage perspective, the CAFC scam typology reflects neither purely expert-produced knowledge nor entirely user-generated content. Rather, it is co-produced through the interaction of victim reports, institutional classification practices, and law enforcement priorities. The typologies are grounded in patterns emerging from reports submitted by individuals who have experienced cyber financial crime, meaning that victims play an active role in shaping what counts as recognizable and reportable fraud. At the same time, these reports are translated, stabilized, and rendered actionable through expert-driven processes, including categorization, aggregation, and interpretation by governmental actors.

As a result, the knowledge embedded in the CAFC’s scam lists is situated and context-dependent. The reported scam types reflect victimization patterns that are salient within Canadian economic, political, and social environments, rather than offering a universal or exhaustive account of cyber financial crime. For instance, studies from sub-Saharan Africa document cyber-enabled frauds involving counterfeit alcohol, artificial meat, and fake agricultural seeds in countries such as Kenya, Uganda, and Zimbabwe, phenomena that are rarely reported in Canada due to differing consumer markets, regulatory regimes, and material conditions (Soon-Sinclair et al., 2023). These contrasts illustrate how cyber financial crime manifests differently across regions, shaped by local infrastructures, consumer practices, and vulnerabilities.

In this sense, the CAFC typology exemplifies a key characteristic of the cyber financial crime assemblage: its configuration is contingent but not accidental (Baker & McGuirk, 2017).

The arrangement of heterogeneous elements—victims, reporting platforms, classificatory schemas, and institutional actors—remains flexible, allowing governance knowledge to be continuously reworked within specific temporal and spatial contexts (Buchanan, 2015; Suchman, 2008; Vertesi, 2014). Canadians encounter particular forms of cyber financial crime more frequently than others not because these crimes are universally dominant, but because local social, economic, and political conditions shape distinct patterns of exposure and recognition.

In this section, I examined how these documents articulate their definitions and associated penalties and how the documented words of law and regulation move through institutional layers. As legal and regulatory requirements move through different sites, they are translated and reinterpreted, and their meaning shifts in step with the evolving practices of cyber financial crime. Examining this process through the perspective of assemblage thinking reveals why the phenomenon resists a static description. The definition of cyber financial crime is constantly evolving, enacted and re-enacted as new crimes emerge and diverse elements—both human and technological—enter the arena. The institutional powers renegotiate what counts as cyber financial crime. These shifts show that definitions and rules must constantly adapt, as different cyber incidents continually reshape both the understanding and the governance of cyber financial crime as new heterogeneous elements enter. Any apparent order represents only a temporary stabilization, an ongoing achievement that can be easily disrupted; once destabilized, the assemblage reassembles, generating new documents and interpretations whose interactions are themselves productive.

5.3 Technological Infrastructure: Malware, Files, and Codes

When Silvast and Virtanen conducted their multi-sited ethnography to trace how infrastructures are assembled across different sites and to understand the distributed, interconnected nature of energy networks, they noted that they treated documents, technologies, routines, and household practices as equally important elements in the assemblage of energy infrastructures (Silvast & Virtanen, 2019). Silvast and Virtanen did not view energy infrastructures as fixed systems with a hierarchical order, nor did they limit their analysis to macro policies or micro practices. Instead, they saw the energy assemblage as an ongoing achievement that was continually undergoing processes of stabilization, rupture, destabilization, and re-stabilization. Their analysis underscores the critical need to assess technologies and infrastructures when examining modern social assemblages through the lens of assemblage thinking. Without close attention to technical systems—including the codes and signals circulating through material networks—it is difficult to understand how these processes are initially formed and how they evolve over time. Without considering heterogeneous elements such as technological routines, operational practices, and the hardware and software situated on the platform as active participants in the distributed energy network, analysis risks overlooking the fundamental mechanisms by which relations are formed, stabilized, destabilized, and transformed within the assemblage.

This account differs from other approaches that either focus on large governance systems or individual user behaviour as the main reasons for outcomes. Rather than seeing infrastructures as systems imposed from above or as results of individual decisions, Silvast and Virtanen show that both people and technology share the ability to act. Stability in these systems is not guaranteed; it comes from ongoing coordination among various parts. Changes occur due to

misalignments, new interpretations, and material limitations, as well as from formal institutional reform (Silvast & Virtanen, 2019). By highlighting these relationships, their work shows that infrastructures survive not because they are well-structured but because everyday practices—technical, organizational, and personal—keep creating a temporary order. This offers a different view: infrastructures are not fixed systems controlled from above, but dynamic collections that depend on constant negotiation among people, technologies, and institutions.

Within dominant governance and security discourses, the initiation of cyber financial crime is often framed as originating in technological infrastructure, cybersecurity practices, and technical vulnerabilities. Following in Silvast and Virtanen's footsteps, I investigated how technological infrastructure shapes the cyber financial crime assemblage. In this section, I trace how technological infrastructure forms relations within the assemblage and show how heterogeneous elements such as malware, files, and codes function as active participants that freely generate new configurations.

The Canadian federal agency responsible for providing expert advice, guidance, services, and support on cyber security—the Canadian Centre for Cyber Security—offers a non-exhaustive list of common tools and techniques typically implicated in the cyber financial crime assemblage. These include, but are not limited to, bots and botnets, (distributed) denial-of-service attacks, exploit kits, malware, password cracking, person-in-the-middle techniques, reconnaissance, social engineering, and web-based exploits (Canadian Centre for Cyber Security, 2022b). I use them as empirical entry points for tracing how technological elements participate in the production of cyber financial crime events.

Approached through assemblage thinking, these tools and techniques are not merely instruments deployed by human actors but active participants in shaping relations, possibilities,

and constraints. Malware scripts automate decision processes; botnets redistribute agency across dispersed infrastructures; phishing kits standardize deceptive interactions; and platform vulnerabilities condition what forms of exploitation become viable. These technological elements interact with regulatory rules, institutional procedures, user practices, financial platforms, and investigative mechanisms, forming provisional configurations that enable certain actions while foreclosing others. Their significance therefore lies not in their isolated technical properties but in how they enter into relations with heterogeneous components across the financial ecosystem.

By presenting heterogeneous elements in this way, the analysis shifts from a threat taxonomy toward a relational account of how cyber financial crime is assembled in practice. The focus moves from identifying types of tools to examining how material infrastructures, codes, interfaces, and automated processes help stabilize, transform, or destabilize events categorized as cyber financial crime. The following section builds on this approach by demonstrating how these heterogeneous technological elements contribute to the enactment and ongoing reconfiguration of the cyber financial crime assemblage.

Malware and Files

The first example is malware. Malware refers to malicious codes that adversely impact the confidentiality, integrity, or availability of an information system (National Institute of Standards and Technology [NIST], 2023). The malicious code is often intended to perform a series of unauthorized computing processes that will impact the victim's data, applications, or operating system (NIST, n.d.-a). Malware can impact all kinds of digital devices such as computers, tablets, phones, and smart devices including smart TVs, smart fridges and smart thermostats (Kebande et al., 2017; Zawoad & Hasan, 2015). As technology advances, new types

of digital devices may become newly incorporated heterogeneous elements within the cyber financial crime assemblage. Signs of malware infection also vary; some may experience sudden slowdowns or crashes of the operating system, failures in shutting down or restarting devices, an inability to remove software, or unexpected pop-ups on user interfaces, while others may find that batteries run out faster than they should, or user preferences may be modified automatically (Federal Trade Commission, 2021).

Malware can be introduced when users interact with files or links from untrusted sources, such as compromised software, contaminated documents, or malicious emails. It may also spread through compromised platforms or devices, or via hidden code embedded in tainted webpages (NIST, n.d.-b). In this framing, the device operates as an intermediary that mediates interactions between users and digital infrastructures, shaping how cyber financial crime takes form in practice. Viewed through the lens of assemblage thinking, the moment a user initiates a malware infection, new heterogeneous elements are drawn into the cyber financial crime assemblage. This action introduces vulnerabilities across devices and platforms that interface with financial institutions' technological infrastructures, therefore affecting system integrity and contributing to the enactment of cyber financial crime.

Bennett (2005) analyzes the 2003 North American blackout, which affected approximately 50 million people across eight U.S. states and Ontario, Canada. Although the event was initially traced to a software alarm failure and overgrown trees in Ohio, it quickly escalated into a cascading grid failure that lasted up to two days, revealing significant vulnerabilities within the energy infrastructure. Bennett argues that the blackout was not caused by a single technical fault. Rather, it emerged from the interaction of diverse human and material elements—including power lines, software systems, trees, electrons, grid operators, market

deregulation, weather conditions, and regulatory frameworks. Together, these heterogeneous elements interacted in ways that produced the conditions for large-scale disruption. In a similar way, malware incidents reveal how cyber financial crime emerges from diverse elements: malicious code, unsuspecting users, operating systems, communication networks, and institutional security protocols. These heterogeneous components collectively create temporary arrangements that the introduction of malware can easily destabilize. Once malware enters the cyber financial crime assemblage, it opens new pathways through which technological infrastructures become vulnerable to exploitation. From an assemblage perspective, malware is understood as emerging through the contingent relations among technical systems, users, institutional practices, and regulatory arrangements, with these relations simultaneously shaping the vulnerabilities that can be exploited and the criminal opportunities that become actionable.

Social Engineering and Phishing

The second example is social engineering. Social engineering refers to the practice of obtaining sensitive information by manipulating legitimate user vulnerabilities. Classic examples include phishing, water holing (targeting regular website visitors), and baiting (leaving malware-infected devices such as USB flash drives around for curious targeted victims to plug in) (Canadian Centre for Cyber Security, 2022; Salahdine & Kaabouch, 2019).

Phishing is one of the most common social engineering attacks that aims to get a target's attention, prompt a target's action, and compromise their attention. Varieties of phishing include phishing through email, phishing through telephone (vishing), phishing through text message (smishing), search engine phishing (fake websites at the top of search results), in-session phishing (interfering with a normal web browsing client session), and spear phishing (aka

whaling: targeted phishing based on previous reconnaissance, using any of the above techniques) (Gonzalez, 2022).

For example, Check Point Research reveals that Canadian banks have long been targeted by a Ukrainian organized crime ring through a massive phishing campaign (Check Point Research, 2019). Cybercriminals first send out legitimate-looking phishing emails containing a PDF attachment to targeted users, and then prompt users to update their banking credentials through the website using the Uniform Resource Locator (URL) provided in the PDF document. Once victims enter the phishing website, fraudsters can then harvest victims' sensitive financial credentials.

Phishing techniques are often considered "low-tech" and do not require extensive technical knowledge to complete (Leukfeldt et al., 2017). In these cases, unauthorized users simply screenshot the real, legitimate website pages, paste the picture on the website, and add textboxes on the pictures to harvest victims' information. Victims are encouraged to enter personal information, and upon successfully obtaining the victims' sensitive financial credentials, the unauthorized users can impersonate the real customer and conduct fraudulent transactions.

Sullivan employs assemblage thinking to analyze data-driven security, arguing that security practices are shaped not only by formal legal systems—rules and norms established by legislatures and courts—but also by technical infrastructures, data practices, and informal regulatory arrangements (Sullivan, 2022). Knowledge and practice, in this view, emerge through the assembling of heterogeneous elements. Such cases illustrate how policies and regulations are not merely the backdrop of the cyber financial crime assemblage; technical infrastructure is an inseparable and active component of it. Phishing campaigns exploit weaknesses in email

formality, spoofed web domains, and user authentication protocols, demonstrating how malicious actors mobilize both technological and human factors to bypass formal controls.

Codes and Attacks

The continued evolution of digital technologies has diversified both the forms and methods of phishing attacks, extending social engineering beyond familiar channels such as email and messaging platforms. Increasingly, cybercriminals exploit the everyday infrastructures through which people access digital services. During the COVID-19 pandemic, for example, many restaurants adopted digital menus to reduce physical contact, often relying on Quick Response (QR) codes as the primary access point. In this setting, QR codes function not simply as technical tools but as infrastructural gateways linking physical spaces to networked digital systems.

Scanning a QR code is typically experienced as a routine and low-risk action, particularly when it occurs in trusted physical environments such as restaurants, donation boxes, or public venues. This sense of familiarity can obscure the sequence of redirections that follow a scan, as users are seamlessly transferred to external websites, payment interfaces, or application downloads. Cybercriminals may take advantage of this infrastructural role by discreetly replacing or altering QR codes so that users are redirected to malicious websites designed to collect payment credentials or initiate malware downloads (Barr, 2022). In such cases, users may unknowingly disclose sensitive financial information or compromise their devices, not because of a single technical failure but because the QR code mediates access in ways that conceal these transitions.

From an assemblage perspective, the vulnerabilities associated with QR code phishing do not reside solely in devices or malicious code. Instead, they emerge through the interaction of

heterogeneous elements, including the physical placement of QR codes, assumptions of legitimacy in public spaces, user access practices, mobile operating systems, web browsers, payment interfaces, and financial institutions' backend systems. By translating physical proximity into digital authorization, QR codes collapse spatial and institutional boundaries and reconfigure how cyber financial crime is enacted.

QR code-based phishing therefore illustrates how new access infrastructures introduce novel forms of vulnerability as attack methods evolve. Static or device-centred descriptions of cyber financial crime struggle to capture these dynamics because they locate risk in a single technical object rather than in the relations that organize access, trust, and routine action. This orientation is visible in the definition provided by the Canadian Centre for Cyber Security, which describes quishing as "a phishing attack that uses QR codes," noting that threat actors may distribute malicious codes via email, overlay legitimate QR codes, or place them in public locations so that victims are redirected to attacker-controlled websites (Canadian Centre for Cyber Security, 2020). While technically accurate, this framing centres the QR code as the primary threat vector and emphasizes delivery mechanisms and security bypasses.

An assemblage approach clarifies what this framing leaves underexamined. Vulnerability does not reside in the QR code itself but emerges through the alignment of mobile devices, visual scanning habits, platform authentication systems, public signage, institutional branding, and users' expectations that QR codes function as routine and trustworthy connectors between physical and digital environments. The effectiveness of quishing depends on these already-stabilized relations: organizations normalize QR-based access for efficiency, while attackers redirect those same channels of trust and authentication. What appears as a discrete phishing technique is therefore better understood as a reconfiguration of relations within the cyber

financial crime assemblage, where interface design, spatial placement, embodied practice, and security protocols converge to produce shifting sites of exposure.

The final example is Person-in-the-Middle (PITM), sometimes also known as Man-in-the-Middle (MITM), which refers to when a threat assemblage intercepts communications signals and compromises sensitive information without the victim's knowledge (Canadian Centre for Cyber Security, 2022a). Victims may think they are having a secure and direct communication client session with the web server, without knowing that the data may have been rerouted for malicious purposes and their sensitive information compromised through the PITM technique. While PITM can happen on personal computers (PCs), the more infamous PITM trend is phone number fraud.

Subscriber Identity Module (SIM) security is one of the most concerning threats for phone number fraud. Financial institutions and online service providers typically send a One-Time Passcode (OTP) to users' phone numbers for verification purposes. When fraudsters attempt to log in to users' accounts, they are required to enter the OTP.

In SIM porting fraud, fraudsters typically call telecommunication service providers and request to port the victim's phone number to the scammer's account at a different wireless carrier. For SIM swapping fraud, cybercriminals may call telecommunication service providers to report a stolen phone and request a new SIM card; or sometimes, cybercriminals may bribe employees of the telecommunication service providers to ensure successful delivery of a SIM card for fraudulent uses (Andrews, 2018; Department of Justice, 2021).

To examine the heterogeneous elements involved in SIM porting fraud, the technological infrastructure includes mobile devices, SIM cards, communication platforms operated by telecommunication service providers, and the signals transmitted across cellular networks. These

material and technical elements interact with institutional processes such as customer authentication protocols, regulatory requirements, and service-provider routines, as well as with human actions ranging from routine customer service requests to coordinated social engineering attempts (Andrews, 2018). Importantly, none of these elements operates in a fixed or subordinate role. Each retains a degree of autonomy, entering into and exiting relations with other elements as circumstances change.

From an assemblage perspective, SIM porting fraud does not result from a single point of failure but emerges when particular configurations of elements temporarily align. Technical infrastructures may function securely in many contexts, yet they become vulnerable when combined with institutional pressures for efficiency, fragmented authentication practices, or persuasive human interventions. Fraudsters exploit these moments of alignment, mobilizing elements such as customer service scripts, verification codes, and network access in ways that exceed their intended functions. When control of a phone number is successfully transferred, the fraudster gains the capacity to intercept calls, text messages, and two-factor authentication codes, thereby reconfiguring access to financial accounts and other sensitive data.

More importantly, the elements involved in SIM porting fraud retain a high degree of autonomy and are not permanently bound to one another. Devices, credentials, institutional procedures, and human actors circulate independently and enter into relations only temporarily, forming arrangements that may stabilize momentarily before dissolving and recombining in new configurations. Vulnerabilities therefore arise not from static or defective infrastructures, but from the contingent alignment of heterogeneous elements across technical, organizational, and social domains. Viewed through the lens of assemblage thinking, SIM porting fraud demonstrates how material artifacts, institutional routines, and human practices generate

opportunities for cyber financial crime through ongoing processes of reassembly and reconfiguration, rather than through isolated technological breakdowns.

5.4 The Human Actors: (Mis)users, Insiders, and Institutional Actors

Human actors—regardless of their roles, responsibilities, status, power, wealth, or background—each contribute in unique ways to shaping the agencies, relations, and configurations of togetherness within the assemblage (Latour, 1987, 1993). Assessing human actors through the lens of assemblage thinking makes it possible to examine their roles without imposing hierarchical order or predetermined social structures. This perspective highlights their co-functioning as a distributed, contingent, and emergent achievement, enabling an analysis that treats heterogeneous elements equally and resists any fixed or prescriptive notion of structure (Blok, 2013; Law et al., 2012; Müller, 2015).

Human actors, from skilled cybercriminals to unwitting users of digital financial products and services, intentionally or unintentionally shape technological infrastructures, financial systems, regulatory environments, and operational practices. At the same time, insiders within organizations may deliberately or inadvertently compromise security through negligence or collusion, creating heightened risks because of their privileged access and specialized knowledge. Institutional actors such as banks, regulatory agencies, and law enforcement bodies adapt their countermeasures as cyber financial crime itself evolves. Viewed through the lens of assemblage thinking (AT), these varied human roles reveal agency as distributed and contingent: the actors are neither isolated nor arranged in a strict hierarchy but are entangled with non-human elements—malware, networks, authentication systems—in shifting relations that continually produce, destabilize, and reconfigure the assemblage.

In this section, I analyze three key groups of human actors who actively shape the cyber financial crime assemblage: everyday users of digital financial products and services, insiders within financial institutions, and institutional actors such as banks, regulators, and law enforcement bodies. These groups illustrate how human actors, as heterogeneous elements of the assemblage, co-function to create a constellation that is both dynamic and fragile, always vulnerable to disruption (Baker & McGuirk, 2017). Following Baker and McGuirk's approach to tracing the material, discursive, and relational dimensions of heterogeneity, I examine the cyber financial crime assemblage without privileging any single category of actor. Instead, I recognize the capacity of all human participants to shape, destabilize, and reconfigure the assemblage on equal terms.

Human (Mis)users and Human Decisions

My analysis begins with human vulnerabilities by examining the behaviours and decisions that everyday users make when engaging with digital financial products and services. These psychological susceptibilities are closely linked to the concepts of Authorized Push Payment (APP) scams and social engineering, where fraudsters exploit trust, urgency, or fear to manipulate users into authorizing fraudulent transactions. APP scams happen when fraudsters deceive consumers into sending payments under false pretences to bank accounts controlled by fraudsters. As payments made using real-time payment schemes are irrevocable, victims cannot reverse transactions once they realize they have been scammed (Ma et al., 2022). Social engineering, as indicated in the earlier section, refers to the practice of obtaining sensitive information by manipulating legitimate users' vulnerabilities.

The key difference between APP scams and social engineering is that APP scams occur when users authorize transactions themselves, and victims tend to think the initiation of the

transactions is legitimate, whereas social engineering commonly refers to unauthorized users obtaining victims' sensitive data without victims realizing or acknowledging the compromise.

For the purposes of this dissertation, I have classified human vulnerabilities into three categories: psychological vulnerabilities, vulnerabilities of people with mental, physical, and social disadvantages, and vulnerabilities resulting from lack of fraud awareness. Though these three categories have the possibility of overlapping, I group them as such in order to analyze the root cause of each human vulnerability.

The first category is psychological vulnerabilities. In this section, I leverage public education and public resource documents from public sector assemblages in Canada, the US, the UK, Australia, and Singapore to summarize common online scam and fraud types (Australian Competition and Consumer Commission, 2018; City of London Police, 2023; Canadian Anti-Fraud Centre, 2023; Singapore National Crime Prevention Council, 2023; US Federal Trade Commission, 2021). APP scams are typically authorized transactions without fraudulent intent, as the APP scam victims usually do not understand the consequences of granting banking access, sharing financial credentials, or authorizing transactions on their accounts. I broadly capture some of the typical APP scam and social engineering techniques targeting human psychological vulnerabilities in Table 6.

Table 6. Psychological Vulnerabilities and Classic Cases

Psychological Vulnerabilities	Classic APP Scams or Social Engineering Techniques
Loneliness	Romance Scams; Sextortion; Companionship Scams; Sugarbaby Scams
Greed	Investment Scams; Cryptocurrencies Scams; Counterfeit Merchandise Scams
Opportunism	Job Scams; Health or Weight Loss Scams; Fake Lottery Wins; Holiday Scams; Mystery Shoppers Scams; Inheritance Scams; Fake Business Opportunities; Ticket Fraud; Education or Training Fraud; Rental and Housing Scams
Fear of Authority	Taxpayer Scams; Fake Law Enforcement Agencies; Bank Investigator Scams; Fake Collection Agencies; Immigration Scams; Fake Hydro or Utilities; Fake Politician or Influencers Scams; Business Email Compromise or CEO Scams
Curiosity	Psychic Scams; Online Auction Fraud; Free Trial Scams; Wangiri Scams; Gift Card or Shopping Credit Scams; USB Baiting Scams
Distress	Ransomware Scares; Fake Bomb Threat; Help Desk/Tech Support Scams
Urgency or Emergency	Accidents or Emergency Scams; Hostage Scams; Fake Charities

Note. Data compiled from Australian Competition and Consumer Commission (2018), City of London Police (2023), Canadian Anti-Fraud Centre (2023), Singapore National Crime Prevention Council (2023), and US Federal Trade Commission (2021).

This dissertation does not intend to explore cyber scams or cyber fraud techniques targeting human vulnerabilities in extensive detail. The design of my classification approach is based on my years of operational experience in the field and can be further improved as fraud trends change and vary over time as per the AT methodology.

Most of the classic cyber financial crime case types mentioned above are easily searchable online with public access. Many local news media outlets have also reported on these cases. However, cyber financial crime is not local in the sense that the criminal operation may

not be conducted in the same location. A perpetrator may operate from one country while the cloud server hosting the stolen data is located in another. At the same time, the victim might reside in a different country, using a foreign financial institution's digital banking services to transfer funds into mule accounts based in another jurisdiction. This transnational character exemplifies how human actors—victims, perpetrators, intermediaries, and institutional responders—function as heterogeneous elements whose actions cut across national and organizational boundaries.

A similar interweaving of diverse human roles can be seen outside the realm of cybercrime in AT scholarship. In their study of the interconnectedness of the fertility industry, Müller and Schurr highlight that parents, surrogates, donors, medical professionals, and clinic staff all function as key human actors in the socio-material processes of surrogacy (Müller & Schurr, 2021). They describe how the organization called My Baby enables Manuel and Rodrigo from Spain, who wish to have a child and have the financial means, to connect with Anita, an egg donor in Sweden, with Benita, a young mother of two from Chiapas who provides the womb, and with Dr. José in Cancun, whose clinic is equipped with state-of-the-art medical technology from the United States. These individuals and resources come together at the right time and under the right conditions, illustrating how heterogeneous human actors assemble across national borders to make complex social processes possible. This example illuminates how assemblages are socio-spatial formations that are also temporal and continually subject to ruptures, changes, and reorganizations (Anderson & McFarlane, 2011).

My second category identifies vulnerabilities of people with mental, physical, and social disadvantages. Some cybercriminals target mentally, physically, and socially disadvantaged groups, often leading to financial abuse. Elder abuse victims, domestic violence victims, child

and youth abuse victims, human trafficking victims, and individuals with mental or physical disadvantages all have a higher risk of becoming victims of cyber financial crime (Cross, 2017; Cross et al., 2018; Currie & Spatz Widom, 2010; Findley et al., 2016; Ssewamala & Ismayilova, 2009).

Specific scam techniques often employ scripted language designed to exploit the vulnerabilities of mentally, physically, and socially disadvantaged groups, targeting semiotic cues such as care, kindness, curiosity, interest, and attention. By appealing to these sensitivities, malicious actors are able to build deceptive trust, making vulnerable individuals more likely to comply with requests and transfer money to scammers (Lee et al., 2022). More importantly, mentally, physically, and socially disadvantaged groups often need additional protection to safeguard their financial assets—protection that is frequently absent. The lack of a capable guardian, as described by Felson and Cohen's routine activity theory and supported by Junger et al., increases the likelihood of cyber financial crime, making these individuals especially vulnerable to exploitation (Felson & Cohen, 1980; Junger et al, 2020).

Assemblage thinking also attends to what human actors and institutional arrangements fail to provide. It highlights not only the presence of diverse elements but also the absences—missing protections, weak oversight, or gaps in regulation—that shape how relations are formed and how vulnerabilities persist (Blok, 2013; Law et al., 2012; Müller, 2015). By focusing on both what is assembled and what is absent, AT reveals how the cyber financial crime assemblage is continually reconfigured by the interplay of human actions, technological infrastructures, and the very omissions that create opportunities for crime.

(Mis)user-Driven Innovation: Fraud Educator

My third category identifies the user group that lacks general fraud awareness. Cybercriminals may leverage technology vulnerabilities or human vulnerabilities to further target users' lack of fraud awareness. For example, upon compromising users' digital banking credentials, cybercriminals may attempt to log into the victim's account but be blocked by OTP. Cybercriminals may attempt to reach out to the victim, pretending they are from the financial institution and ask for the OTP to be sent to the victim's device (Singapore National Crime Prevention Council, 2023). Victims may not be aware of the implications of disclosing such sensitive information, which can ultimately lead to account compromises.

Similarly, the human actors missing in this context include educators and information sharers who can continually raise awareness among everyday users about emerging forms of exploitation. These actors could provide timely guidance on how scammers target specific psychological or technological vulnerabilities, explain new attack vectors such as evolving phishing schemes or social engineering tactics, and share best practices for safeguarding personal data and financial credentials. Their absence leaves everyday users without up-to-date knowledge of threats and without the practical skills to recognize early warning signs.

Viewed through the lens of assemblage thinking, the absence of educators and communicators itself becomes a heterogeneous element that helps constitute the cyber financial crime assemblage. Anderson and McFarlane emphasize that assemblage thinking attends not only to presence but also to erasure and absence, recognizing that what is missing can be as consequential as what is present (Anderson & McFarlane, 2011). Similarly, Star and Griesemer argue that intersecting social worlds are co-produced through particular configurations of human

and non-human actors, such that absences actively shape how assemblages form and operate (Star & Griesemer, 1989).

From a criminological perspective, this absence also intersects with established insights about opportunity and learning. Clarke and Felson show that crime opportunities emerge where capable guardianship is weakened, while Akers emphasizes how behaviours are learned, reinforced, and normalized through social interaction (Clarke and Felson, 2017; Akers, 2017). In the cyber financial crime assemblage, the absence of educators and communicators diminishes both collective guardianship and opportunities for preventive learning, increasing individuals' susceptibility to evolving forms of cyber financial crime. This absence does not merely indicate a lack of information; it actively conditions how vulnerabilities are perceived, interpreted, and addressed in practice.

If educators and communicators were introduced as a form of (mis)user-led innovation, their presence would disrupt the existing configuration of the assemblage, prompting a rearticulation of relationships among users, institutions, and technologies. Such a reconfiguration would reshape how risks are understood and how protective practices are enacted, illustrating how the cyber financial crime assemblage remains open to transformation through the autonomous addition or withdrawal of heterogeneous elements.

Insiders and the Silent Risks

Alongside everyday users, insiders who work closely with digital financial services and products are also key elements of the cyber financial crime assemblage. The term insiders typically refers to individuals who have access to internal systems and networks or who have knowledge of an organization's resources. The internal information is usually confidential and only available to internal employees. According to the U.S. Cybersecurity & Infrastructure

Security Agency, the sensitive data are typically protected by internal knowledge infrastructure and/or an organization's security perimeters. Insider threats occur when company insiders intentionally or unintentionally use their authorized access or understanding of an organization to harm an organization. For this dissertation, third-party threats such as threats presented by contractors or vendors are included for discussion, since they also introduce direct or indirect insider threats. There are different expressions of insider threats, including but not limited to violence, espionage, sabotage, theft, and cyber attacks (Cybersecurity & Infrastructure Security Agency, 2023).

Intentional and unintentional insider threats both create enormous cybersecurity risks. According to the Cybersecurity & Infrastructure Security Agency, intentional insider threats refer to when hostile insiders facilitate insider knowledge or use technical means to disrupt an organization's regular business operations (Cybersecurity & Infrastructure Security Agency, 2023). Here, insider knowledge refers to situated, experience-based understanding of workflows, security procedures, institutional norms, and informal workarounds—in other words, knowledge that enables actions to appear routine while reducing the likelihood of detection. Unintentional insider threats are non-malicious insiders who are unaware of the threat and unintentionally harm an organization without understanding the consequences.

Intentional insider threats can take different forms, such as collaborator (working with a third party to intentionally create threats collaboratively) or lone wolf (creating threats independently) (OpenText, n.d.). Employee contexts are also different: the unauthorized user can be a full-time employee, part-time employee, contractor, partner, consultant, temporary worker, or former employee (Shaw et al., 1998). Reasons to trigger an insider threat also differ. Greitzer,

for example, creates a typology called Sociotechnical and Organizational Factors for Insider Threat (SOFIT) that includes both individual and organizational factors (Shaw et al., 1998).

On an individual level, factors such as concerning work habits, authentication issues, data manipulation, poor job performance, personal financial concerns, ideological beliefs, as well as mental health can all lead to insider threats. Organizational factors such as security practices (e.g., hiring and training practices), communication issues (clear procedures and employee communication), management systems (workplace practices and management styles), and work planning and control (workload, autonomy, and scheduling) also play important roles in managing risks related to insider threats. This intricate framework suggests that a combination of these individual and organizational factors shapes the landscape of workplace security and behaviour.

For cyber financial crime, one of the most infamous recent insider threat incidents in the banking industry is the Capital One cyber incident. In July 2019, Capital One announced that an attacker had gained unauthorized access to the personal information of approximately 98 million US consumers, and approximately one million Canadian consumers' Social Insurance Numbers were also compromised (Capital One, 2022, 2023a). The attacker, Paige Thompson, was able to exploit a misconfigured firewall in Capital One's infrastructure which allowed her to gain access to sensitive data stored in the cloud (Capital One, 2023b). Thompson was a former employee of Amazon Web Services (AWS), and AWS was the cloud service provider for Capital One (Nguyen, 2021). Thompson had good insider knowledge about the infrastructure and was able to penetrate the cloud. The attacker posted the compromised data on GitHub, a company commonly used by programmers that allows users to store codes, software development documents, and revisions of projects (see Figure 5) (*United States v. Paige Thompson*, 2019).

Figure 5. Incident Email to Capital One's Responsible Disclosure Program



Capital One

Responsible Disclosure (Shared) <responsiblediscloure@capitalone.com>

[External Sender] Leaked s3 data

[redacted] Wed, Jul 17, 2019 at 1:25 AM

To: "responsiblediscloure@capitalone.com" <responsiblediscloure@capitalone.com>

Hello there,

There appears to be some leaked s3 data of yours in someone's github / gist:

https://gist.github.com[redacted]

Let me know if you want help tracking them down.

Thanks,

[redacted]

Note. A screenshot of an incident report email from an unknown security researcher. From materials in *United States v. Paige Thompson* (2019). Copyright 2019 by the United States District Court for the Western District of Washington.

The compromised data in this cyber incident included names, addresses, credit scores, credit limits, and bank account numbers, among other sensitive personal information (Edwards, 2021). Capital One agreed to pay $190 million to settle this class-action lawsuit filed by impacted consumers (*Nguyen*, 2021). According to court records, Thompson "devised and intended to devise, a scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises" (*United States v. Paige Thompson*, 2019, p. 1).

In the Capital One incident, the human actor, together with sensitive personal information, vulnerable technical infrastructure, and incomplete security controls, co-produced the cyber incident, demonstrating how agency and accountability are distributed across human and non-human components of the assemblage. Responsibility, too, is not simply located in one individual or one organization, but emerges from the interactions and dependencies that allowed the breach to occur. Beyond Thompson, responsibility also extends to the organizational security

governance that failed to remediate known misconfigurations, the cloud service environment whose default settings and complexity shaped the attack surface, and institutional oversight mechanisms that did not detect anomalous access in time. These interacting conditions formed the enabling environment through which the intrusion became possible.

Assemblages are not organic wholes in which the differences of the parts are absorbed into a single higher unity. Instead, their components maintain their own identities and interact in ways that are contingent and constantly reconfigured (Briassoulis, 2019; McFarlane, 2011). This raises critical questions about where agency, causality, and responsibility lie within an assemblage and how these forces should be understood and allocated (Anderson & McFarlane, 2011). Intentional insider threats provide a clear example of how heterogeneous elements create relationships, assume responsibility, and generate effects that emerge through complex chains of causality. The Capital One case therefore exemplifies how insider threats reveal the assemblage as a dynamic, heterogeneous formation, one in which relations between human agency, technological systems, and institutional oversight continually generate both vulnerabilities and their consequences.

Aside from intentional insider threats, there are also unintentional insider threats. Business email compromise scams are one of the most classic unintentional insider threats in the field of cyber financial crime. Cybercriminals send an email message that appears to come from a legitimate or a known source (Federal Bureau of Investigation, n.d.). Documented cases include, for example, a company's Chief Executive Officer (CEO) asking her assistant to buy gift cards and a staff member from a company's purchasing department instructing the finance department to send out wire payments to vendors (Federal Bureau of Investigation, n.d.).

There are various techniques employed in the execution of business email compromise scams. The RCMP reports that common schemes include compromising or spoofing e-mail accounts belonging to an existing employee, compromising or spoofing e-mail accounts belonging to existing suppliers, wholesalers, or contractors, and compromising or spoofing e-mail accounts belonging to financial services providers (RCMP, 2021). Other variations of business email compromise scam techniques can combine with other technology or human vulnerabilities, such as the techniques of posing as a company's authority and demanding that victims download malicious software or asking for urgent payment from the business account for emergency purposes.

The example of an unintentional insider threat illustrates how the cyber financial crime assemblage produces victimization through the autonomous participation of human actors. From an assemblage perspective, human actors do not merely experience the effects of the assemblage; they retain the capacity to act, interpret, and respond, and in doing so actively contribute to its ongoing achievement. Here, ongoing achievement refers to the idea that the assemblage is not a fixed structure but something continually enacted through everyday actions, decisions, interpretations, and interactions among people, technologies, rules, and environments. Victimization, therefore, is not a one-time outcome produced by a stable system; it is repeatedly brought into being as users follow prompts, trust interfaces, apply organizational procedures, overlook anomalies, or rely on habitual understandings of "normal" system behaviour. Lysgård, in his study of culture-led policies in small towns and rural communities, similarly argues that actors such as voluntary organizations, amateurs, and lay citizens are not passive recipients of policy interventions (Lysgård, 2019). Rather, they operate with a degree of autonomy, translating

institutional decisions into practice and shaping behavioural patterns that stabilize—or unsettle—assemblage configurations.

Within the cyber financial crime assemblage, this autonomy means that no human actor simply receives information or passively becomes a victim. Instead, individual decisions and practices enter into relation with institutional routines, technological systems, and regulatory expectations. These interactions align with insights from the CCO model, which emphasizes that criminal opportunities emerge through the convergence of actors, situational conditions, and the absence or presence of controls (Ekblom, 1994). In this context, unintentional insider actions can reconfigure opportunity structures by weakening guardianship, enabling access, or amplifying existing vulnerabilities.

Every action, whether undertaken knowingly or unknowingly, contributes to the co-production of the assemblage. Human autonomy in this context does not imply intent to cause harm; it refers to actors' everyday capacities to interpret situations, follow routines, make adjustments, and rely on practical judgment. These ordinary practices help stabilize workflows, maintain trust in systems, and normalize ways of working. At the same time, they can reproduce unnoticed assumptions, habitual shortcuts, or misplaced confidence, all of which can shape where vulnerabilities emerge. The assemblage is therefore continually re-stabilized through routine action.

Assemblage thinking offers a distinctive contribution here by showing how harm can arise from normal, legitimate activity without being reducible to either individual mistake or system failure alone. It shifts the analytical focus from isolated causes to relations—how human judgment, interface design, security procedures, institutional expectations, and technical settings come together in particular situations. Unintentional insider threats thus demonstrate that cyber

financial crime emerges through the alignment of autonomous human action with evolving sociotechnical conditions. Vulnerability is produced relationally, across interacting elements, rather than originating from a single actor or a single flaw.

Private Sector Institutional Actors

Private sector institutional actors are also key human participants in the cyber financial crime assemblage. Within the Canadian financial ecosystem, critical private sector institutional actors include financial institutions, the telecommunications industry, major credit card companies, the Canadian Bankers Association, and the cybersecurity sector. These actors collectively shape how cyber financial crime is defined, prevented, and responded to: they develop security standards, implement detection technologies, share threat intelligence, and coordinate with regulators and law enforcement. Their policies and practices influence both the vulnerabilities and the defensive capacities of the assemblage, illustrating how private sector institutional agency is integral to the continual formation and reformation of cyber financial crime.

As previously mentioned in the literature review chapter, cyber financial crime in the Canadian financial ecosystem can include heterogeneous components such as financial service providers, internet service providers, telecommunication companies, cybersecurity companies, software service providers, payment platforms, authentication solution providers, and so on (Ololade et al., 2020; Tade, 2022; Tade & Adeniyi, 2020). Big Tech companies such as Google, Microsoft, Amazon, Meta, and Apple are also situated within the financial ecosystem as their products and services often serve as the communication or payment infrastructure for cyber financial crime.

Telecommunication service providers are also a critical component in non-public sector assemblages of cyber financial crime. In Subscriber Identity Module (SIM) porting fraud, unauthorized users typically contact telecommunication service providers, seeking to transfer victims' phone numbers to the fraudulent account with another wireless carrier. In SIM swapping fraud, unauthorized users may call these providers to report a stolen phone and request a replacement SIM card. In other cases, unauthorized users may resort to bribing telecommunication service provider employees to secure the successful delivery of a SIM card for fraudulent purposes (Andrews, 2018; Department of Justice, 2021). Telecommunication service providers are important institutional actors determining policies on who owns the telecommunication account, who has access to the account, how the person has access to the account, and how the telecommunication service is being used to authorize transactions.

Lysgård structured his empirical analysis of culture-led policies around three questions: what kinds of policies are created, how they are produced, and who are the producers (Lysgård, 2019). Human actors not only create rules and policies that shape the performance of an assemblage, but through their legitimization, these institutionalized ideas gain material support, ultimately shaping how the assemblage functions. Similarly, telecommunication service providers operating as private sector institutional actors play a decisive role in shaping how cyber financial crime unfolds. Loopholes in their authentication procedures and SIM card delivery rules create openings that malicious actors can exploit, illustrating how private sector institutional actors become integral elements of the cyber financial crime assemblage and influence both its vulnerabilities and its capacity for reconfiguration.

Financial institutions also often rely heavily on third-party service providers for their IT infrastructure, software, telecommunication services, or payment facilities; therefore, it is critical

to strengthen cyber resilience for both financial institutions and third-party service providers, as they are integral parts of the assemblage (Fintech News Malaysia, 2023). As a result, cyber resilience is distributed across both financial institutions and their external service providers, which together constitute interdependent components of the cyber financial crime assemblage. For example, the Society for Worldwide Interbank Financial Telecommunication, commonly known as SWIFT, functions as a financial services infrastructure to facilitate payment worldwide (Scott & Zachariadis, 2012). SWIFT is widely regarded as the most secure and trusted third-party network in the world, serving 200 countries with over 8000 users (Scott & Zachariadis, 2012).

Cybercriminals have repeatedly leveraged the SWIFT network as a financial infrastructure through which stolen funds can be transferred. In February 2016, for example, attackers attempted to move nearly US$1 billion from the Central Bank of Bangladesh using the SWIFT system, while in 2017, unauthorized transactions totaling approximately US$60 million were executed through Far Eastern Bank in Taiwan and routed to overseas destinations (Tariq, 2018). These cases illustrate how payment infrastructures such as SWIFT operate with a degree of autonomy, executing transactions according to embedded protocols, authorization rules, and validation processes rather than assessments of criminal intent.

From a situational perspective informed by the CCO model, opportunities for cyber financial crime emerge when institutional routines, technological permissions, and contextual conditions align in ways that enable fund movement (Clarke & Felson, 2017; Ekblom, 1994). For SWIFT and other payment network providers, the classification of an event as cyber financial crime is therefore contingent on situational factors such as whether the infrastructure permits or blocks a transaction, the apparent legitimacy of beneficiary accounts, and the presence

or absence of authorization signals. Human oversight, automated controls, and network protocols each operate semi-independently, entering into temporary alignment that may either constrain or facilitate illicit transfers.

Viewed through an assemblage lens, these infrastructures do not simply transmit value; they help shape the conditions under which cyber financial crime takes place. The relative autonomy of payment networks, together with the situational configurations highlighted in the CCO model, suggests that cyber financial crime emerges from the contingent alignment of technical systems, institutional procedures, and human practices rather than from a single point of failure.

By contrast, non-assemblage approaches often treat infrastructures as neutral channels and focus on discrete causes such as offender intent, organizational mistakes, or specific technical flaws. Causality is framed more linearly, and responsibility is traced to identifiable failure points. An assemblage perspective shifts attention to how infrastructures, people, and institutions jointly produce the environment in which action becomes possible, emphasizing distributed agency and relational causality rather than isolated breakdowns.

(Mis)user-Driven Innovation: Payment Controls

SWIFT now offers various products and services to prevent and control cyber financial crime as (mis)user-driven innovation. For example, SWIFT offers a product called Payment Controls, which screens outgoing SWIFT payment messages against configurable rules and alerts financial systems on high-risk transactions (SWIFT, 2024). SWIFT allows financial institutions to configure their rule requirements based on their risk appetite and business needs. If the financial institution intends to stop more cyber financial crime, the rule can be stricter and block transactions in real time (SWIFT, 2024).

In this case of the SWIFT Payment Controls launch, the SWIFT network, as a third-party service provider, experienced a cyber financial crime incident alongside financial institutions, revealing that its previous cybersecurity controls were no longer effective. The SWIFT network is not a passive background facilitator but an institutional actor actively shaping the formation and reconfiguration of the cyber financial crime assemblage. When hackers destabilized the assemblage's structure, the malicious act prompted (mis)user-driven innovation, leading SWIFT to introduce Payment Controls, a new product designed to reassemble and strengthen its defence mechanisms. Human actors within the cyber financial crime assemblage, including the private sector institutional actors, work collectively to assemble, stabilize, and disrupt processes within the assemblage (Baker & McGuirk, 2017).

This case shows how (mis)user-driven innovation unfolds through heterogeneous and partially autonomous actors that collectively reconfigure the cyber financial crime assemblage. SWIFT's Payment Controls do not operate as a singular or uniform mechanism but emerge through interactions among diverse elements, including configurable rule-based algorithms, institutional risk appetites, regulatory expectations, transaction infrastructures, and human oversight practices. These controls are introduced in response to malicious (mis)use that exposes the limits of existing cybersecurity arrangements, demonstrating how offender-led innovation precipitates institutional reconfiguration rather than linear risk mitigation. By enabling financial institutions to independently configure rule strictness and intervention thresholds, Payment Controls distribute decision-making authority across organizational, technical, and contractual sites, granting institutions autonomy in how cyber financial crime risks are interpreted and acted upon. At the same time, this autonomy produces variability in how suspicious activity is identified, interrupted, and adjudicated across the network, illustrating that (mis)user-driven

innovation continually reshapes cyber financial crime governance through heterogeneous and partially autonomous sociotechnical arrangements rather than centralized or standardized solutions.

(Mis)user-Driven Innovation: E-Commerce Defence

From an assemblage perspective, institutional actors are not assumed to occupy fixed hierarchical positions, and service providers are not analytically ranked according to their size or operating influence. Instead, their roles and degrees of influence are treated as empirically variable and relational, becoming visible through analysis of how heterogeneous material and discursive and organizational elements interact in specific contexts (Baker & McGuirk, 2017). Assemblage analysis therefore does not deny differences in power but examines how such asymmetries are produced, stabilized, or contested within particular configurations, rather than presuming them in advance. Accordingly, even actors operating at smaller scales—such as e-commerce merchants and online service providers—constitute significant private-sector participants whose practices, platform choices, and security arrangements shape how risks and responsibilities are distributed across the assemblage.

E-commerce merchants and online service providers often face the risk of compromising the integrity of their customers' payment information (Chargeback Gurus, 2020). Stolen sensitive financial information is often sold on the Dark Web. The Dark Web refers to encrypted and overlaid networks designed for secure communications which are typically only accessible via specialized software such as the Onion Router (Tor) (Haasio et al., 2020; Hayes et al., 2018). The act of forwarding encrypted messages resembles peeling off layers of an onion, which is intended to make users unidentifiable to a certain degree (Haasio et al., 2020). Dark Web marketplaces are similar to legitimate online marketplaces such as Amazon or eBay, but they

offer illicit goods and services (Akhgar et al., 2021). Online drug markets, firearm markets, commercial child sexual abuse markets, counterfeit products markets, and confidential and financial data exchanges are examples of available products and services (Chertoff, 2017; Kigerl, 2020; Liggett et al., 2020).

When cybercriminals obtain compromised credit cards from the Dark Web, they often leverage botnets' computing power to test the usability of these credit cards: are these cards expired? Did the consumer report a lost or stolen credit card? Are the Card Verification Value (CVV) codes valid? Does the credit card still have available credit? Even though the Dark Web sells credit card data, not every credit card is available to use. Compromised credentials on the Dark Web are often sold in batches, and sometimes these data dumps can be enormous.

In the notorious 2015 Ashley Madison data breach, a cybercriminal released a 40GB data dump containing personal details and credit card credentials (Cross et al., 2019). Testing each stolen credit card individually would be both time-consuming and resource-intensive. Cybercriminals therefore prioritize quality over quantity, seeking compromised card data that include complete card numbers, accurate billing addresses, correctly spelled cardholder names, CVV codes, and valid expiry dates (Bulakh & Gupta, 2015; O'Connor, 2021). From these patterns of credit card credential compromises emerged a cyber attack: botnet card testing. Botnets allow unauthorized users to automate the testing of stolen card data so that the quality of a data dump (in other words, its completeness and validity) can be assessed before it is sold. Because the market value of stolen data depends on its reliability, automated testing determines price ranges and resale potential. This evolution places new demands on e-commerce merchants and online service providers, who must monitor website traffic and analyze transaction-arrival patterns to detect suspicious activity (Chargeback Gurus, 2020).

In response, a corresponding (mis)user-driven innovation has emerged on the defensive side. By analyzing when and how consumers complete transactions, merchants and vendors can identify the velocity anomalies and irregular transaction patterns associated with botnet card-testing activity, where automated scripts attempt multiple small transactions to validate previously stolen card credentials (Chargeback Gurus, 2021a). Cybersecurity companies providing protective solutions for financial systems and online platforms are therefore drawn into the Canadian financial ecosystem as critical actors, participating in the ongoing co-production and reconfiguration of the cyber financial crime assemblage.

This sequence—where one (mis)user-driven innovation generates another—demonstrates how innovation unfolds relationally across the assemblage (Braune et al., 2022). The expansion of e-commerce creates opportunities to exploit compromised card data, and botnet card-testing attacks emerge as a (mis)user-driven innovation that repurposes automated botnet infrastructures specifically for credential validation rather than initial theft. Cybersecurity experts then develop detection and mitigation mechanisms (also a form of (mis)user-driven innovation) to identify and disrupt these patterns. As Latzko-Toth et al. and Law and Callon note, a single digital technology can generate multiple, layered assemblages as its uses and misuses proliferate, illustrating how technological infrastructures, human strategies, and defensive responses continually reshape the cyber financial crime assemblage (Latzko-Toth et al., 2019; Law & Callon, 1992).

Private sector institutional actors in this example, including e-commerce merchants, payment processors, credit card networks, and cybersecurity service providers, play pivotal roles in both enabling and countering these evolving practices situated within the assemblage. Their combined actions reveal that these private sector institutions are not merely passive defenders or neutral conduits but active participants in shaping the cyber financial crime assemblage.

5.5 Financial Instruments, Authentication, and Knowledge Practices

Actor-Network Theory (ANT) explores the networked nature of social and technological phenomena, mapping both human actors such as scientists, engineers, and policymakers and non-human actors like system data, technological artifacts, and biological entities within a heterogeneous network (Callon, 1986; Latour, 1987; Law, 1992). ANT emphasizes that non-human actors possess agency and can exercise power and influence within these networks (Law & Callon, 1992). Assemblage thinking complements and extends this perspective by focusing on how heterogeneous elements temporarily come together to co-function without pre-determined rules or stable hierarchies (Müller & Schurr, 2016). Bringing AT into dialogue highlights the conceptual bridge between AT and ANT: both approaches reject fixed social structures, prioritize the agency of human and non-human actors, and trace how associations are continually formed, destabilized, and reconfigured. The notion of an *assemblage network* captures this overlap, illustrating how diverse actors interact, how their relations evolve as power dynamics shift, and how social order remains an ongoing, contingent achievement (Callon, 1999).

In this section, I present findings from my semi-structured interviews to show how non-human actors—specifically financial instruments, authentication mechanisms, and knowledge practices—actively shape the ongoing formation of the cyber financial crime assemblage. These discursive, material, and inorganic elements are embedded within the assemblage and appear static, yet they continuously and proactively reconfigure its structure and dynamics. To illustrate this process, I examine the use of One-Time Passcodes (OTPs) as a customer authentication method for verifying the legitimacy of digital banking logins. At the same time, the knowledge practices of industry professionals and their attitudes toward these financial instruments and

authentication technologies play a decisive role, influencing how these elements function, how vulnerabilities emerge, and how the assemblage evolves over time.

OTP as a Fraud Prevention Strategy

With the widespread adoption of smartphones, tablets, and wearable technologies such as smartwatches, digital banking products and services have become an integral part of everyday financial life. In the digital age, financial instruments are no longer limited to physical credit or debit cards. Instead, digital banking platforms, instant payment networks, electronic funds transfer systems, and mobile wallets all function as key financial instruments (Hazar & Babuşcu, 2023). These digital instruments are typically protected by passwords and multi-factor authentication (MFA). MFA typically refers to the use of additional factors beyond a password to verify a customer's identity—employing security questions that ask for a user's mother's maiden name, for example. Canadian financial institutions have traditionally used MFA before granting access to online banking services. While banks initially relied on passwords to safeguard customer accounts, this single layer of protection quickly proved inadequate. Passwords, and even early forms of MFA such as static security questions, can be compromised through social engineering tactics or malware infections. In response, financial institutions introduced multi-factor authentication using OTP as a two-step verification method. OTPs provide time-sensitive, single-use codes delivered via SMS or app to add a dynamic layer of security and reduce the risk of unauthorized access. This evolution reflects how technological and institutional actors continually reconfigure the cyber financial crime assemblage by adapting authentication practices to emerging threats.

Most financial institutions in Canada recommend that consumers use two-step authentication such as OTP or an authentication application. When a high-risk login attempt

occurs on the customer's profile, such as a new digital device or a new internet service provider, Canadian financial institutions prompt an OTP challenge to authenticate the legitimacy of the login attempt. Sending authentication passcodes to users' devices increases technical complexities for fraudsters attempting to log into victims' accounts (BMO, 2023b; CIBC, 2023; Amato, 2018; Scotiabank, 2023; TD Bank, 2023b).

(Mis)user-Driven Innovation: Evolving OTP Practices

However, the two-step authentication via OTP is far from a bulletproof solution. Fraudsters quickly learn to trick victims into revealing their OTP credentials through social engineering or to hijack the OTP by attacking the victim's SIM card. As these tactics spread, industry practitioners come to recognize that OTP-based two-step authentication alone cannot stop fraud. This realization prompts financial institutions to explore additional layers of protection such as device-based authentication, biometric verification, and behavioural analytics, thus illustrating how the cyber financial crime assemblage continually adapts as both attackers and defenders innovate in response to each other's moves.

> I think this is kind of like an evolving thing. So I know that now that we're using OTP, right, as opposed to like the MFA [multi-factor authentication] that we used to use before with anything new. It works for like, a period of time. And then you're in the same position as before. I think like fraudsters are good at like, you know, migrating. (Interviewee #MBC5-GZ8U)

In this quote, Interviewee #MBC5-GZ8U explains how unauthorized users quickly learned to exploit technological vulnerabilities in this process by manipulating victims into sharing their credentials. In response, Canadian financial institutions introduced OTP to strengthen authentication for customer logins. Yet, as the interviewee notes, OTP soon proved

vulnerable, as well, with fraudsters developing tactics such as social engineering and SIM-card hijacking to intercept or steal these codes.

Tracing how OTP functions as a non-human actor offers a productive lens for understanding how such technological elements shape the becoming of the cyber financial crime assemblage. OTP is not simply a neutral security feature; it actively mediates relations between financial institutions, customers, and fraudsters. Latour's work *The Pasteurization of France* illustrates how microbes became crucial actors in the network of public health in France (Latour, 1993a). This approach diverges from traditional views that often place humans at the centre of sociological studies. Microbes were once perceived merely as abstract scientific concepts but became active participants in public health debates and practices due to Pasteur's work. Latour's study shows that scientific discoveries are not just accepted but are integrated into society through a series of interactions that include both human and non-human elements.

Similarly, OTP plays a significant role in acting as an influential non-human actor, participating in the assemblage's ongoing processes of formation, disruption, and reconfiguration. OTP is a technological artifact designed to stop suspicious logins and reduce the risk of cyber financial crimes. This perspective highlights the active role of OTP in the broader network, as it does not merely sit in the background but works in concert with other elements of the assemblage—financial institutions, telecommunications providers, end-users, and security protocols—to enhance protection and safeguard digital transactions. Its deployment requires continuous discussion and careful adjustment: financial institutions must coordinate the technical standards for code generation and delivery, telecommunications providers must guarantee the safe and reliable transmission of messages, and users must adapt their routines to accommodate an additional step in authentication. These collaborations and negotiations stretch beyond the

Canadian financial institutions, influencing global digital banking operations and setting international expectations for cybersecurity. Much like Latour's account of how scientific knowledge about microbes reshaped practices far beyond the laboratory, the adoption of OTP technology exemplifies how a single (mis)user-driven innovation can shape the financial ecosystem (Latour, 1993a).

Additionally, industry practitioners acknowledge that even though OTP was originally developed as a result of (mis)user-driven innovation, it could become outdated as more and more unauthorized users start targeting the technology vulnerabilities related to OTP. Interviewee #MBC5-GZ8U points out that, as a (mis)user-driven innovation, OTP also needs to continue its evolution in order to remain an effective defence mechanism.

> I think there's always has to be a continuous change. For, like, protecting customers in the space. So you can't just say, Oh, we've got OTP it's gonna work great. And you know, it's gonna be great for the next five years. Like, I think you should consistently be planning ahead to bring in new features and security measures. (Interviewee #MBC5-GZ8U)

Latour suggests that the networked whole is constantly evolving, and non-human actors also mobilize each other and are constantly forming relationships (Latour, 2005). (Mis)user-driven innovation is an indicator of an evolving assemblage that is never static. I asked another interviewee how they felt about the evolution of OTP. The interviewee validated Interviewee #MBC5-GZ8U's viewpoint in describing how malware could potentially be a new technology vulnerability as it compromises the validity of OTP. The interviewee spoke of how malware could automatically forward the authentication prompt and the OTP to another device:

> They don't need to hack your phone or wipe your phone to get the OTP, they will simply infect your phone with a malware and every time a message comes to your phone, it will be forwarded to fraudsters' mobiles. You won't even know … the message will be forwarded to them and they will have your OTP. (Interviewee #RPEN-N3VJ)

(Mis)user-Driven Innovation: Alternative Authentication

Industry practitioners share that Canadian financial institutions are increasingly exploring alternative authentication methods, particularly various forms of biometric verification. Banks see biometrics such as fingerprint or facial recognition for mobile banking sign-ins as a way for consumers to authenticate their identities more easily and quickly than with traditional passwords (Scotiabank, n.d.-a). Yet, these methods are not immune to fraud: voice biometrics, for example, can be compromised if the initial registration is falsified or if synthetic voice technologies are used to spoof legitimate users. Despite these risks, practitioners remain broadly optimistic about the potential of biometric authentication, arguing that it offers stronger protection than passwords and can counter specific technological vulnerabilities within the cyber financial crime assemblage such as attacks involving keyloggers.

> When logging into device now there's biometrics right, which prevents the option of keyloggers from getting the password. It's using an additional security measure, which shapes the way our policies are being used. (Interviewee #3NGU-8XTJ)

By embedding human biological traits directly into the authentication process as routinized operational practices, biometrics reshape both the technological infrastructure and the knowledge practices of financial security, illustrating how financial instruments and authentication technologies co-evolve to reinforce—yet continually reconfigure—the assemblage. STS literature exemplifies how the stabilization of an artifact or a technological

system relies on the relevant social group's power to manage conflicts and controversies (Bijker et al., 1987; Law et al., 2012; Law & Callon, 1992). When non-human actors such as OTP and biometric authentication become more productive than password protection or security question sets, OTP and biometric authentication can then mobilize more resources and therefore become more widely accepted within the Canadian financial ecosystem.

As a result, industry practitioners appear more inclined to promote OTP and biometric authentication as a method to protect the customers' accounts rather than unilateral password protection. Stopping fraudsters from logging into the account would usually be the first step to prevent the financial institution's financial losses. As OTP and biometric authentication are more reliable, Canadian financial institutions could spend less time authenticating the customer, as the customers' identities would be previously validated by OTP or biometric authentication, resulting in shorter wait times and better customer experiences.

> [Biometric authentication] reduces handle time. Biggest complaints, customers usually … [complain about] the long wait times on the call. With the voice biometrics, we are able to voice match to our clients quicker and more accurately, where we sometimes don't even need to get into (authentication) questions, where the tool will recognize the client with a 95% accurate rate. (Interviewee #76MW-WT9E)

Shorter wait times not only result in better customer experiences but also reduce overall operating costs. Because biometric authentication is associated with lower fraud rates than password-only protection, the Canadian financial ecosystem increasingly encourages its adoption to reduce operational costs and improve customer experience. This example illustrates how digital banking as a financial instrument, OTP as an authentication device, and the operational knowledge, fraud predictions, and confidence in accuracy held by industry practitioners function

as heterogeneous elements that continuously shape the formation and reconfiguration of the cyber financial crime assemblage. Although these elements are material and inorganic, they act dynamically, influencing security practices, prompting new defensive strategies, and driving the ongoing evolution of both criminal techniques and institutional responses. Their interactions demonstrate how non-human actors actively participate in producing and transforming the assemblage, rather than merely providing a passive backdrop (Vertesi, 2014).

My next authentication case example shows how inorganic non-human actors such as knowledge, trust, and proofs within the financial ecosystem hold equal ontological status in shaping the cyber financial crime assemblage. STS literature refers to this as symmetry—the idea that human and non-human actors are treated equally analytically when examining how sociotechnical relations produce effects (Callon & Rabeharisoa, 2003; Bruno Latour, 1992). This does not mean they are identical in form, intention, or moral standing, but that analysis does not assume in advance that causality or agency belongs only to humans. Instead, influence is traced through how different elements—people, artifacts, documents, codes, and infrastructures—participate in shaping action and outcomes. Non-human actors can therefore exert influence, change behaviours, and contribute to the development and consequences of social networks as part of these relational configurations (Latour, 1993b; Law & Callon, 1992).

For example, a stolen wallet containing personal identification and credit or debit cards provides a malicious actor with the informational resources needed to conduct cyber financial crime. These materials function not merely as passive objects but as carriers of credentials, identity signals, and institutional recognition that enable fraudulent transactions. This demonstrates how non-human elements shape the outcomes of the cyber financial crime assemblage by structuring what actions become possible, thereby actively participating in its

continual formation and transformation. According to Interviewee #LRPS-55Y3, if a wallet is stolen by an unauthorized user, the chance of identity theft increases as the unauthorized user has all the information needed to conduct a cyber financial crime:

> So when it comes to stolen wallets, typically customers would contain not just their credit or debit cards, but also their IDs. Because it's one thing for a fraudster to use… I think it's more risky to have their ID stolen, because then it all goes up room for ID theft, which might be used for true name fraud too. (Interviewee #LRPS-55Y3)

The wallet exerts influence and contributes to the development of cyber financial crime, shaping the social network as much as any human actor. By carrying identification documents, credit and debit cards, and other personal items, all non-human actors become active participants in enabling fraudulent transactions and the misuse of personal data. Its material presence transforms the interactions among victims, fraudsters, financial institutions, and law enforcement. In this way, the wallet exemplifies how non-human elements can catalyze shifts in power relations, create new lines of agency, and drive the continual reconfiguration of the cyber financial crime assemblage.

5.6 Conclusion

Heterogeneity, a key characteristic of an assemblage, calls on AT scholars to trace the diverse human and non-human, material and discursive elements whose interactions continually shape and (de)stabilize the assemblage. These varied components—people, objects, and knowledge practices—are not organized through fixed structures or predetermined orders but come together to produce and enact relationships.

In this chapter, I have illustrated how documents, technological infrastructures, human actors, financial instruments, and institutional practices function as heterogeneous elements within the cyber financial crime assemblage. These elements continually perform liaisons and forge relationships among dynamic components, forming non-linear connections that cannot be reduced to a single, straight line of causality or organized into a fixed hierarchy. By tracing how these key heterogeneous elements configure the cyber financial crime assemblage, I followed both human and non-human actors to show why understanding cyber financial crime requires avoiding static descriptions or rigid definitions.

As these heterogeneous elements interact, policy documents are reproduced, technological infrastructures are updated, operational routines are redesigned, and authentication mechanisms are re-examined. Though each element retains a degree of autonomy, no single component can reshape the assemblage on its own; rather, they co-function to form temporary associations that break down when (mis)user-driven innovations introduce new forces of change.

Legal and policy documents generate evolving definitions and understandings of cyber financial crime, continually shaping both the treatment of the phenomenon and the institutional resources mobilized to address it. By expanding concepts and incorporating new details of criminal practice, laws and regulations act as active non-human actors that perpetually reassemble the cyber financial crime assemblage. Within the technological infrastructure, malware, files, and codes produce vulnerabilities that stimulate the continual evolution of the assemblage. Its inherent instability and unpredictability create provisional associations among technical systems that dissolve as new attacks rupture the existing order. Human actors likewise contribute across multiple dimensions: end-users bring psychological vulnerabilities; criminals deploy linguistic strategies to exploit victims' weaknesses; insiders introduce risks through

privileged access and specialized knowledge; and institutional actors make operational decisions that recalibrate the system. Regardless of role or status, all human participants possess the capacity to reconfigure the cyber financial crime assemblage. Finally, financial instruments, authentication technologies, and knowledge practices as non-human actors foster (mis)user-driven innovations that destabilize relationships within the assemblage, ensuring that its configuration remains dynamic, contingent, and perpetually open to reconfiguration.

Assemblage thinking rejects broad, reified categories and instead highlights the creative capacities of matter, energy, and the processes that bind diverse actors together in heterogeneity (Acuto & Curtis, 2014). In the context of cyber financial crime, analyzing the heterogeneous elements of the assemblage shows how documents, infrastructures, technologies, and practices co-function to generate dynamic relations, making the assemblage a continual process of becoming rather than a fixed system.

Revisiting the definition of cyber fraud as outlined in public guidance from the Canadian Anti-Fraud Centre, Canadians are encouraged to report incidents in which someone: impersonates them online, locks their device for ransom, installs malware, engages in blackmail, sends fraudulent banking information, deceives them into making purchases or donations, imposes hidden recurring charges, or poses as a bank or trusted organization (Canadian Centre for Cyber Security, 2025). This definition reveals a classification approach grounded in fixed, enumerated categories. While this list is operationally useful for reporting and triage, it frames cyber fraud as a set of discrete, recognizable event types rather than as an evolving and relational phenomenon.

Such a definition relies on abstraction and stabilization, treating fraud techniques as bounded and largely knowable in advance. This approach risks hiding how cyber fraud practices

constantly change, combine, and adapt to different situations, platforms, and user behaviours. From an assemblage perspective, cyber fraud is not limited to predefined categories but arises from contingent alignments of technologies, institutional routines, user expectations, and adaptive (mis)use. Overreliance on static typologies may therefore produce over-determined or simplified understandings that lag behind practice, limiting the capacity of governance and prevention strategies to respond to how cyber fraud is actively reconfigured within a changing financial and digital ecosystem. By focusing on these concrete interactions among heterogeneous elements rather than relying on fixed abstractions, researchers and policymakers can respond to the assemblage's evolving and contingent character without resorting to over-determined, simplified, or ineffective approaches.

Chapter 6 - Multiplicity: Enacting the Many Realities

6.1 Introduction

In the study of cyber financial crime, security incidents rarely present themselves as singular or stable phenomena. Each cyber financial crime is enacted through the interactions of human and non-human actors, giving rise to multiple, coexisting interpretations. A fraudulent cheque may appear perfectly legitimate to a scam victim; an intercepted email money transfer may seem successfully delivered according to the system's confirmation message; and a remotely controlled device may appear uncompromised to the bank's screening algorithm. These distinct versions of reality appear different but remain internally connected and justifiable within each actor's own logic. The overlapping and at times contradictory realities demand a theoretical framework capable of holding difference together without collapsing it into a single, unified truth.

The concept of multiplicity, a key characteristic of assemblage thinking, provides such a device, one that captures variation, movement, and the shifting winds of relation and transformation. Developed by Deleuze and Guattari and later extended within STS, multiplicity challenges the assumption that a phenomenon can be singular or fully representable as one coherent entity (Deleuze & Guattari, 1987). An assemblage is not a sum of parts, but a dynamic configuration that performs diverse practices and generates multiple, overlapping versions of reality (Law, 2002, 2015).

Through the lens of multiplicity, each reality is distinct yet interrelated—each is complex, partially connected, and continually in the making (Law, 2002, 2015). Multiplicity invites methodological pluralism, meaning that methodologically, the method requires multiple, situated approaches to trace how different realities are enacted across various (mis)users, practices,

technologies, policies, and institutions (Briassoulis, 2017; Law, 2004). The method acknowledges that different methodological choices do not simply reveal the same world from different perspectives, but rather help to enact different worlds, each producing its own version of reality through the practices, instruments, and relations it mobilizes (Law, 2004). Studying an assemblage thus entails following its partial connections and examining how each version of reality is produced through distinct perspectives of seeing, measuring, and intervening yet remains entangled with others (Strathern, 2004).

Multiplicity is employed in this dissertation as an analytical concept for examining how cyber financial crime can take shape through different configurations of actors, technologies, practices, institutional priorities, vulnerabilities, and responses. Its use does not imply that this study captures the full range of perspectives, experiences, or configurations that may constitute the broader cyber financial crime assemblage. Rather, the analysis of multiplicity is necessarily bounded by the empirical scope of the research and by the perspectives represented within the dataset.

The empirical focus of this dissertation is intentionally centred on Canadian financial institutions, consistent with the research questions and the defined scope of the project. Accordingly, the interview data provide substantially greater insight into financial industry and practitioner perspectives, including how financial institutions understand, respond to, and attempt to govern cyber financial crime. Other actors—including customers and victims, offenders, law-enforcement agencies, regulators, technology companies, and other organizations—remain important components of the broader assemblage, but they are not represented to the same empirical depth. Some of these actors enter the analysis through documentary materials or through practitioners' accounts of their interactions with them;

however, these sources do not provide equivalent access to those actors' own perspectives, experiences, or interpretations.

Therefore, the discussion of multiplicity in this chapter of the dissertation is intended to reflect the multiplicity observed within the context of Canadian financial institutions, rather than to represent the multiplicity of the cyber financial crime assemblage in its entirety. The analysis demonstrates how cyber financial crime is configured differently across institutional practices, technologies, policies, customer interactions, vulnerabilities, and forms of misuse within this specific power setting. These findings therefore support a situated understanding of multiplicity and power within Canadian financial institutions, while recognizing that other actors and contexts may generate additional configurations that fall beyond the empirical scope of this study.

This chapter examines three key dimensions of multiplicity within the cyber financial crime assemblage within the context of Canadian financial institutions: first, the multiple enactments of authorization, where no single mechanism defines access or control, as authorization is performed differently across diverse human and non-human actors; second, the multiple coexisting realities of victimization, where risks and harms are enacted through varying legal, procedural, and experiential lenses; and third, the multiple versions of responsibility, where accountability resists a singular cause and instead circulates across institutional policies, technological systems, and decision-making processes. Taken together, these dimensions exemplify how cyber financial crime operates as a multiplicity, a constellation of overlapping yet partially connected realities that continuously reconfigure what counts as access, harm, and fault within an evolving assemblage.

6.2 Authorized or Not: The Multiplicity of Access Controls

Deleuze uses multiplicity to describe the nature of Ideas in *Difference and Repetition* (Deleuze, 1994). He writes that "an Idea is an n-dimensional, continuous, defined multiplicity," shifting away from the Platonic conception of ideas as transcendent and abstract forms existing beyond material experience (Deleuze, 1994, p. 182). For Deleuze, Ideas are not static essences but "multiplicities made up of differential elements," as dynamic and generative fields of potential composed of interdependent relations, forces, and variations (p. 168). The concept of multiplicity operates as an analytical device for examining how heterogeneous human and non-human actors hold together within an assemblage, each shaping its formation and transformation in distinct yet interconnected ways.

Multiplicity, as Deleuze further elaborates, is "a system of multiple, non-localisable connections between differential elements which is incarnated in real relations and actual terms" (Deleuze, 1994, p. 182). It signifies a mode of being defined by interactions and relationships, a dynamic ontology in which reality continuously unfolds through interdependent processes. Rather than representing an abstract template of reality that organizes the world from above, Ideas articulate the process of becoming; they continually produce difference and transformation through the reciprocal interplay of their internal relations. In this view, reality is not organized by fixed essences or hierarchies but is continually composed through the multiple movements, tensions, and interconnections that give rise to new forms and multiple possibilities.

Within the cyber financial crime assemblage, multiplicity reveals that the system is neither singular nor static but composed of dynamic internal relations that generate multiple, coexisting realities—each enacted through distinct capacities, practices, and potentials. Instead of assuming the cyber financial crime assemblage as a unified entity, multiplicity invites inquiry

into how differences interact and coordinate productively within the cyber financial crime assemblage (Law, 2004).

In the following section, I explore how the cyber financial crime assemblage exhibits the characteristics of multiplicity by tracing the various ways in which access control is ignored, bypassed, or abused, revealing how authorization is continually reconfigured through diverse practices and relations. The multiple enactments of access control shape the continuous transformations of technology, regulation, and human conduct, and generate multiple realities that seemingly contradict each other yet are partially connected.

In this dissertation, access control refers to technical, procedural, and institutional mechanisms designed to regulate who can enter and use the protected digital financial infrastructures. Access control functions as a gatekeeping mechanism designed to distinguish legitimate users from unauthorized ones. To determine whether an activity is authorized, financial institutions typically establish multiple layers of verification that challenge users and restrict access to sensitive banking information and transactional functions. These controls take various forms such as bank card Personal Identification Numbers (PINs), online banking passwords, biometric authentication, and two-step verification through one-time passcodes. Their purpose is to safeguard financial systems, fence off unauthorized users, and prevent the occurrence and spread of cyber financial crime by maintaining boundaries of legitimacy, trust, and controlled access within the financial ecosystem.

However, I argue that access control, in practice, is far from a stable mechanism. What counts as authorized arises from a dynamic and distributed interplay rather than a single, fixed point of control. Authorization is continuously enacted through interactions among human and non-human actors, including users, fraudsters, algorithms, credentials, institutional policies, and

authentication infrastructures. Each act of authorization reconfigures its own meaning: who authorizes, how authorization occurs, and what is being authorized are all contingent and evolving. As these relations shift, different aspects and realities of access control emerge, revealing the assemblage as a performative multiplicity rather than a predetermined mechanism.

Remote Access Control

The first example of cyber financial crime examined in this section is remote access compromise. In such cases, victims may not have their credentials or identities directly stolen, yet their access to financial services or digital systems becomes compromised. Cybercriminals exploit this remote access to infiltrate banking platforms, manipulate transactions, or harvest sensitive information. Remote access control is a technique frequently leveraged by malicious actors to gain entry into financial infrastructures by tricking users into voluntarily authorizing access. According to a report by the RCMP, scams often start with unsolicited communication, such as emails, phone calls, or pop-up alerts that warn users about a supposed security threat or system malfunction (Royal Canadian Mounted Police, 2021). Victims are persuaded and manipulated into screen sharing and providing remote access to cybercriminals, thinking cybercriminals are employees of tech support companies or cyber security companies. As victims provide remote access to cybercriminals, malicious actors can then perform tasks such as signing into online banking platforms, making purchases using stored credit card information, installing malware, downloading/uploading files, using computing power without permission, and/or stealing other sensitive/private data.

Remote access control illustrates not only heterogeneity but the multiplicity of the cyber financial crime assemblage. While heterogeneity draws attention to the diverse human and non-human elements involved, multiplicity emphasizes that remote access is enacted in more than

one way at the same time. Authorization, trust, and control do not form a single, unified reality; they take different forms across institutional settings, technical configurations, and user practices. The same infrastructure can simultaneously support legitimate remote work, routine system administration, and pathways for compromise, depending on how relations are assembled in particular situations.

Multiplicity is therefore visible in the coexistence of different enactments of access within the same sociotechnical environment. Employees, customers, system administrators, authentication tools, devices, networks, and monitoring systems participate in configurations that may produce security, convenience, efficiency, or exposure. The overlapping interactions demonstrate how vulnerability and control are not opposites located in separate systems but coexisting realities generated through shifting relations within the cyber financial crime assemblage. Assemblage thinking invites a distributed analytical lens, one that attends to how heterogeneous elements—technologies, users, institutions, algorithms, and fraudsters—interact and co-produce events (Deleuze & Guattari, 1987; DeLanda, 2006; Law, 2004). Cyber financial crime, therefore, is not an abstract or transcendent concept but a material and relational assemblage composed of shifting actors and capacities that cannot be captured as a single, stable object.

Secondly, although the assemblage is multiple, its multiplicity cannot be counted. Multiplicity is not a matter of quantity but of force, energy, and potential: it describes relations that transform rather than elements that can be counted. The enactments and shifting relations that constitute an assemblage make it a field of qualitative potentials, not a discrete collection of measurable parts (Deleuze, 1994; Law, 2004). The remote access incident, for instance, cannot be captured by simply identifying and counting its components, such as a computer, a phishing

website, or remote control software, because the event transforms as its relations transform. If the same compromise occurs through a tablet instead of a computer or begins with a phone call rather than a pop-up window, the fraud still materializes but through a different configuration of relations. These potentials are not counted but enacted, continually reshaping the boundaries of authorization and control. Consequently, the multiplicity of authorization renders cyber financial crime particularly difficult to define, detect, and govern, as what counts as "secure," "authorized," or "legitimate" depends not on the number of defence mechanisms or access control strategies in place, but on the shifting alignments of human and non-human actors within a constantly reassembling field of relations.

Finally, multiplicity also directs analytical attention to the existence of coexisting realities within the same event. For the victim, the experience appears legitimate: they believe they are engaging with a trusted company to resolve a technical issue or address a fabricated concern. For the financial institution, the login appears authentic: the correct device, familiar IP address, and successful completion of two-step verification all indicate normal activity. For the fraudster, however, the same login represents a carefully devised deception, an unauthorized intrusion disguised as a routine customer session. Each perspective enacts a different reality of the same incident. The victim's reality is one of trust, the institution's reality is one of procedural normality, and the fraudster's reality is one of calculated manipulation. The non-human actors—passwords, one-time passcodes, authentication servers, fraud-monitoring algorithms—also participate in producing these realities, each interpreting and validating actions according to its programmed logic.

What appears, therefore, as a regular login event is simultaneously a fraudulent compromise, enacted and experienced differently by each actor in the assemblage. As Mol

observes in *The Body Multiple*, "attending to the multiplicity of reality is also an act" (Mol, 2002, p. 6). In her ethnography of a Dutch hospital, Mol investigates how atherosclerosis is done, practiced, and enacted across different sites of care (Mol, 2002). In the Department of Pathology, the disease appears as an amputated leg under the microscope; for clinicians, it is experienced through the touch of hardened arteries or the measurement of blood pressure; for the patient, it manifests as pain while walking and the anxiety of restricted movement. Each actor enacts the disease differently through their own practices, instruments, and bodily engagements, producing distinct yet coexisting realities that cannot be reduced to a single, unified truth. Similarly, in the case of remote access fraud, the event is enacted through multiple logics at once: the victim's belief in legitimate assistance, the institution's perception of authorized activity, and the fraudster's orchestration of deception. These realities overlap but never fully align, revealing that cyber financial crime, like the diseased body in Mol's account, is a multiple object realized differently through the practices that bring it into being.

Email Money Transfer Interception

My next example of access control compromise is email money transfer interception. Email money transfer is a money transfer service frequently used by Canadian consumers, where consumers can send and receive money by sending emails or text messages to contacts. Email money transfer interceptions happen when a fraudster diverts a legitimate email money transfer to the fraudster's email account and then deposits the money that does not belong to them. Email money transfer interception can also happen when the victim's email account access is compromised (Interac, 2023). When cybercriminals have access to a victim's email account, the victim may not be able to receive the money transfer notification and the payment may be intercepted.

The realities in email money transfer interception incidents are multiple yet partially connected. Different realities coexist and relate without achieving full coherence; various enactments overlap but never completely merge (Law, 2004; Mol, 2002; Strathern, 2004). For the sender, the transaction appears successful: the system confirms delivery with a notification that the transfer has been sent. For the receiver, the money never arrives, as it has been intercepted before deposit. For the financial institution, transaction logs display that the sender's account was debited while the receiver's account was never credited. These realities are partially connected through shared artifacts—the intercepted transfer, the transaction record, and the notification system—yet they embody different versions of the same event as experienced and interpreted by distinct human and non-human actors.

As Law argues, studying multiplicity requires "messy" methods—approaches that attend to partial connections rather than seeking closure or singular explanations (Law, 2004). The overlapping realities of an email money transfer interception are held together by these partial connections: the same event is enacted across multiple sites and systems, each sustaining its own logic of truth and verification. Following Strathern's notion of partial connections, which influenced both Law and Mol, multiplicity is understood as the coexistence of realities that are linked but not unified, contradictory yet interdependent (Law, 2002; Mol, 2002; Strathern, 2004). Though the sender's, receiver's, and institution's perspectives conflict, they remain connected through the shared infrastructures, data traces, and communicative protocols that make the transfer possible. Multiplicity, in this sense, recognizes that different realities do not collapse into one another but remain in tension—coordinated yet divergent, linked yet irreducible.

To summarize, the examples of remote access compromise and email money transfer interception demonstrate how access control operates as a multiplicity, a field of coexisting and

partially connected realities enacted by heterogeneous human and non-human actors. Authorization, in these contexts, is not a fixed condition but a relational and performative achievement, one continually negotiated across technological infrastructures, institutional protocols, and user practices. What appears as a secure login or a successful transaction in one reality may simultaneously constitute a breach or deception in another. These events reveal the limits of static conceptions of security and highlight how fraud and innovation evolve together within the same assemblage: misuse generates adaptation, and protection gives rise to new vulnerabilities. Thus, access control cannot be understood as a singular defense mechanism but as an evolving multiplicity where authorization, trust, and fraud are not opposites but interdependent forces shaping the ongoing dynamics of the cyber financial crime assemblage.

6.3 One Incident, Many Realities: Enacting Victimization

Žukauskaitė identifies three conditions through which Deleuze defines multiplicity (Žukauskaitė, 2020). First, multiplicities are indeterminable in advance: they have no fixed identity or essence prior to the relations that compose them and can only be understood through ongoing differentiation. As Deleuze writes, they are “neither sensible form nor conceptual signification, nor, therefore, any assignable function” (Deleuze, 1994, p. 183). Second, multiplicities consist of intrinsic differential relations described as “reciprocal relations” that generate singularities and intensities, forming “continuous and dynamic, non-localisable ideal connections” whose elements are “actually incarnated in a variety of terms and forms” (p. 183). Third, multiplicities articulate the movement from the virtual to the actual; they are virtual structures infused with potential that unfold and materialize through particular historical, social, and material configurations, becoming “from the condition of a problem to the cases of solution”

(p. 183). To sum up, multiplicity enacts realities without prior identity, consisting of continuously varying relations that carry the intensive energy of becoming, moving potentials from the virtual to the actual.

Echoing Deleuze's three conditions of multiplicity, the cyber financial crime assemblage emerges through interrelated relations and energetic processes of becoming, without any predetermined or stable configuration of identity. In this section, I illustrate how cyber financial crime victimization operates as an enacted multiplicity, where realities are continually reconfigured through diverse practices and interpretations. Specifically, I focus on service agreement violations to analyze situations in which consumers or unauthorized third parties, whether intentionally or unintentionally, exploit available banking systems.

Examples in this section include individuals selling their bank cards without realizing they have become money mules; cases of family or friendly fraud where relatives or friends exploit trust to drain victims' accounts; customers who deliberately plan credit card bust-out schemes, ultimately victimizing financial institutions through intentional default and deception; and scam victims who believe they are actioning the correct steps in identified scenarios but have unknowingly participated in a fraudulent scheme. Such incidents give rise to multiple, coexisting versions of reality that are, in turn, legal, procedural, experiential, and affective. Each version enacts the event differently, revealing that victimization is not a fixed state but an ongoing process performed through institutional rules, technological infrastructures, and user practices.

Every instance of financial service violation is unique: it unfolds without pre-given conditions of the bank accounts, without static templates of user behaviour, and within institutional relationships that continuously evolve as banking practices and profitability logics shift. Each violation alters the assemblage's configuration, introducing new potentials, relations,

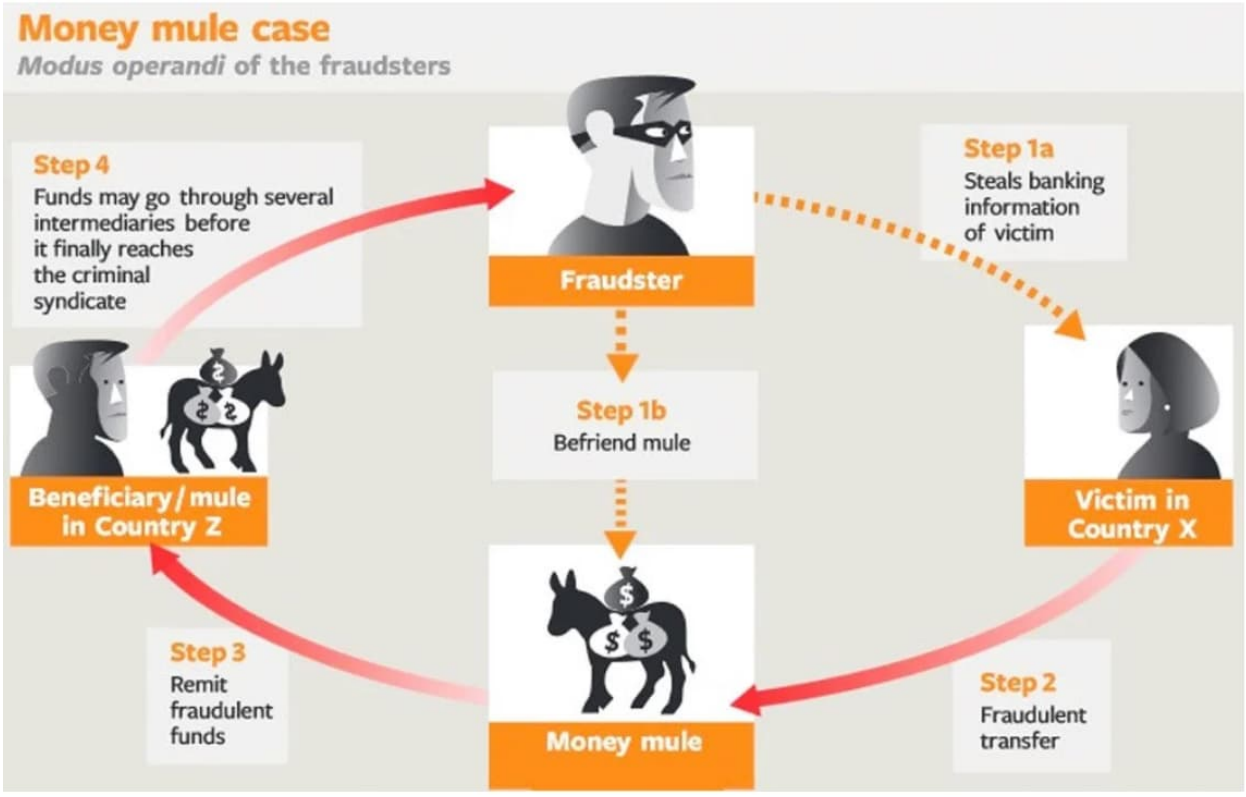
and capacities for change within the ecosystem of cyber financial crime (Deleuze, 1994). The evolving enactments illustrate that the cyber financial crime assemblage operates as a complex multiplicity that is irreducible to any single narrative, cause, or truth.

When consumers open accounts with financial institutions, they need to sign the service agreement drafted by that institution. In these financial service agreements, consumers are asked to keep their PINs confidential, safeguard their bank card details, report lost or stolen cards promptly, and review banking statements periodically to identify suspicious transactions (BMO, 2023a; CIBC, 2019; RBC, 2021; Scotiabank, 2020; TD Bank, 2023b). Consumers are held liable for their own activities and authorized transactions, including but not limited to using bank cards and PINs to access financial services, providing credentials to merchants, using bank cards to complete contactless payment transactions, failing to notify the financial institution about lost credentials, voluntarily allowing third parties to access financial services, making fraudulent deposits, misusing credit products, abusing a Funds Availability Policy after a cheque is deposited, and failing to co-operate fully in an investigation of a fraud incident (BMO, 2023a; CIBC, 2019; RBC, 2021; Scotiabank, 2020; TD Bank, 2023b). From reviewing the financial service agreements issued by the Big Five banks in Canada, it is traceable that some consumers or unauthorized third parties may intentionally or unintentionally exploit available financial services or systems by violating financial service agreements. The violation of financial service agreements, whether intentional or unintentional, generates multiple realities, as the customer's understanding of their actions and the financial institution's interpretation of those same actions often diverge.

Card Transfers and Money Mules

The first example of a financial service agreement violation involves the sale or transfer of bank cards for use as money mule accounts (Europol, 2021). Victims may hand over their cards intentionally, often in exchange for quick cash, or unintentionally through deception, coercion, or misunderstanding. Once in possession of these accounts, malicious actors use them to receive, launder, and move illicit funds, performing a range of criminal activities such as depositing stolen money, withdrawing cash, or routing payments to obscure their origins (see Figure 6).

Figure 6. Illustration of Money Mule Cases



Note. From "Money Mules: How Scammers Exploit Job Seekers to Launder Money," by WhatIsMyIPAddress.com, (n.d.). https://whatismyipaddress.com/money-mule

Other forms of service agreement violations that may occur once accounts are compromised include submitting false chargeback claims by disputing legitimate transactions as fraudulent, coordinating merchant fraud with complicit vendors, abusing cheque-clearing windows to inflate account balances through cheque kiting, and producing falsified documentation to obtain fraudulent mortgages (Canada Mortgage and Housing Corporation, 2018; Chargeback Gurus, 2021b; Chargebacks911, 2023; Dludla, 2021). Each of these actions blurs the boundaries between victimization and perpetration, exposing both account holders and financial institutions to legal, financial, and reputational harm.

At the level of everyday practice, when individuals sell or share their bank cards for quick cash, they often do so without fully understanding the downstream consequences. From their perspective, the action may appear limited to granting another person access to a card. What remains invisible is the broader set of activities that subsequently unfold—activities that become legible only within the financial institution's operational reality, where unauthorized transactions, suspicious fund flows, and policy violations are identified.

From an institutional perspective, the same incident is interpreted differently, as illustrated by Interviewee #LX4K-Z3DK:

> In those cases, I would not say yes, because in both situations the customer is a victim—either of a scam or of fraud. The individual committing the fraud is usually elsewhere. The receiving account may be a mule account, either with TD or another financial institution, or the funds may have been transferred out of the country, which is often the case. As a result, the actual perpetrator is rarely held accountable. (Interviewee #LX4K-Z3DK)

These divergent interpretations reveal the multiplicity of a single incident. Victimization is not a fixed or singular condition but is enacted through interdependent relations among users, financial institutions, intermediaries, and transnational infrastructures. The incident acquires different meanings across these settings, demonstrating how cyber financial crime is constituted through multiple, coexisting realities rather than as a discrete event.

Family fraud refers to situations in which a family member or close friend gains access to an individual's financial services and conducts unauthorized transactions. When consumers obtain bank cards and sign financial service agreements, they agree to keep their PINs and credentials confidential and never share them with third parties. However, in cases of family fraud, consumers often breach this condition by sharing access with those they know, love, and trust. In one case reviewed by the Ombudsman for Banking Services and Investments (OBSI), a consumer discovered multiple unauthorized transactions across several accounts, including a personal chequing account, investment portfolios, and a credit card, all conducted by a family member without his consent (Ombudsman for Banking Services and Investments, 2020). Although the victim did not authorize these transactions, the OBSI found that the bank was not liable, as the customer had voluntarily shared his credentials, meaning the transactions were considered authorized under the service agreement.

This case exemplifies how a single incident can enact multiple, coexisting realities. From the victim's perspective, the experience is one of betrayal and financial loss: funds were taken without meaningful consent. From the financial institution's perspective, however, the same transactions appear legitimate, as authentication protocols were followed and identity validation was successful. Within the cyber financial crime assemblage, these realities do not cancel each other out. Instead, they coexist and partially connect: the transfer is simultaneously "authorized"

and “unauthorized,” the victim both deceived and implicated, and the loss both personal and procedural. Cyber financial victimization is thus enacted through multiplicity, where contradictory versions of events overlap rather than resolve into a single truth.

This multiplicity becomes even more pronounced in cases involving emotionally charged social engineering. As Interviewee #AS9X-JSNM explains:

> Your granddaughter had an accident and you need to send money right away because she’s in the hospital. That kind of scams are very intuitive. They fall into it, and it’s normal. (Interviewee #AS9X-JSNM)

Such scenarios further complicate institutional interpretations of authorization and responsibility, as emotional urgency reshapes how consent, intent, and vulnerability are enacted in practice. Recognizing multiplicity within assemblages is therefore crucial for developing governance strategies that can adapt over time. Avoiding simplification through static or umbrella-style policies allows financial institutions to address cyber financial crime through multiple, context-specific lenses, offering more nuanced forms of customer protection that reflect the layered realities through which victimization unfolds. Law and Singleton discuss how multiple realities coexist and how heterogeneous elements enact different versions of those realities. In their case study of the British government’s response to the 2001 foot-and-mouth disease epidemic, they explore how policy might have differed if multiplicity had been recognized (Law & Singleton, 2014). The government’s approach—mass slaughter and movement restrictions—treated the disease as a singular, stable entity, overlooking the diverse human and non-human actors that enacted it in different ways. The farms, laboratories, government agencies, datasets, and livestock mobilities each participated in producing distinct realities of the disease. On farms, the disease represented a lived and economic reality tied to

animal care, livelihoods, and local knowledge. In laboratories, it became a virological object, existing as samples, test results, and models. Within government agencies, it was an administrative and regulatory problem, expressed through policy categories, risk thresholds, and control measures. In datasets and mobility networks, it appeared as patterns of spread shaped by animal movements and trade routes. These were not simply different perspectives on the same thing, but different practical enactments that produced partially overlapping versions of what the disease was, shaping which forms of intervention seemed necessary or legitimate. Law and Singleton argue that policy cannot be fully understood without tracing these heterogeneous relations. They speculate that if policymakers had acknowledged multiplicity—allowing for multiple enactments of the disease—they might have pursued more locally adaptive, context-sensitive, and less standardized responses.

The multiplicity thinking model enables the development of more adaptive policy approaches while providing a framework to trace the relations between human and non-human actors and to question underlying assumptions. Because multiplicity attends to relations without assigning pre-existing identities, it allows overlooked or invisible actors within an assemblage to be recognized. In the cyber financial crime assemblage, for instance, consumers are not the only victims; financial institutions themselves can become victims when misusers exploit infrastructural vulnerabilities or breach financial service agreements. The following example of credit card bust-outs illustrates this dynamic, showing how deception and compliance can coexist within the same system, and how institutional mechanisms of trust and creditworthiness can themselves become sites of exploitation and victimization.

Credit Card Bust Out

A credit card bust-out fraud is a long-term scheme in which fraudsters deliberately build and maintain strong credit profiles for months or even years before maxing out all available credit lines and disappearing (Chargebacks911, 2022). Within the Canadian financial ecosystem, access to credit, loans, and borrowing capacity is largely determined by an individual's credit score and their demonstrated patterns of borrowing and repayment. Financial institutions, trusting these behavioural indicators, extend greater credit limits to customers who appear to manage debt responsibly. However, some users exploit this trust by artificially constructing a false record of good financial behaviour (e.g., making timely payments, increasing limits, and cultivating the illusion of reliability) until the moment they withdraw or charge the maximum available credit with no intention of repayment.

In this case, multiple realities are enacted within the same cyber financial crime assemblage. From the perspective of the financial institution, the customer appears to be a reliable borrower, one who complies with service agreements and demonstrates consistent repayment behaviour. From the perspective of the fraudulent user, however, this same credit relationship is mobilized as a strategic resource, gradually exploited through calculated spending and ultimately culminating in deliberate default. At the same time, credit reporting platforms enact yet another reality: a credit profile that appears stable and trustworthy until it suddenly deteriorates. As late payments accumulate, the credit score declines sharply, reclassifying the account from creditworthy to delinquent.

From an operational standpoint, industry practitioners note that financial institutions deploy a range of detection mechanisms to identify, prevent, and manage credit card bust-out

fraud. Yet distinguishing between genuine, well-intentioned customer behaviour and fraudulent activity remains challenging. As one practitioner explains:

> For credit card bust-out fraud, it's very difficult—sometimes frustrating. We introduced some automation about six months ago, so now one of the first things I do each morning is review regular anomalies. (Interviewee #BAWZ-SXX7)

Despite these controls, practitioners also emphasize that fraudsters often exploit informational gaps across systems and time. As another interviewee observes:

> But obviously, people are taking advantage of the missing pieces of information. (Interviewee #AR26-4DEE)

The credit card application and usage process embodies coexisting and contradictory realities: one grounded in institutional trust, procedural compliance, and algorithmic assessment, and another rooted in deception, manipulation, and strategic misuse. These realities unfold simultaneously within the assemblage, illustrating how credit card bust-out fraud is not the result of a singular failure but emerges through the misalignment of temporal, informational, and institutional perspectives.

Additionally, this example illustrates how multiplicity operates through the enactment of credibility, trust, and control, revealing that systems built on predictive assessment and behavioural regularity are multiple and vulnerable. The boundary between legitimate financial participation and fraudulent behaviour remains fluid and relational. The multiplicity is continuously reorganizing through the interactions of users, institutions, and technological infrastructures.

Agreement Violation

Next, I expand the discussion of scams within the context of financial service agreement violations to illustrate how multiple realities coexist and complicate the management of cyber financial crime incidents. Scams are particularly revealing because victims often remain unaware that their actions have violated the terms of their financial service agreements. My illustrated example is the abuse of the Funds Availability Policy in a job scam where the victim deposited a fraudulent employment cheque and was instructed to transfer money out of their account before the cheque had cleared. The cheque clearing process typically takes several business days, but many victims are unaware of this delay. Cybercriminals exploit this gap, manipulating victims who believe the visible increase in their account balance indicates that the cheque is legitimate (Johnson, 2021). In such cases, the bank advances funds to the customer for convenience before the cheque is officially verified. When the cheque is later identified as counterfeit, the victim discovers that the transferred money was never real.

This scenario exemplifies a Funds Availability Policy violation, where the victim unknowingly acts before the cheque has fully cleared. The multiplicity of this incident lies in the contradictory yet coexisting realities it produces. From the bank's perspective, the policy is designed to provide convenience, via temporary access to deposited funds to enhance customer experience. From the victim's perspective, however, the increased account balance signifies that the cheque has cleared, enacting a false sense of security and legitimacy. The system, in its design, carries an intention of efficiency, while the victim enacts that efficiency as validation. The fraudster, in turn, exploits this temporal gap or knowledge gap as an opportunity for deception. Thus, the incident represents how multiple realities of authorization and legitimacy overlap: the bank's procedural truth, the victim's experiential truth, and the fraudster's

manipulative truth are all partially connected within the same assemblage of financial trust, time, and technology.

Multiplicity is multiple, but it is not measurable by quantity; rather, it is temporal, spatial, and intensive, defined by degrees of force, variation, and energy (Briassoulis, 2017; Law, 2004; Mol, 2002). Multiplicity can expand and contract, encompassing temporal variations that continuously transform the assemblage over time (Mol, 2002). In the case of cheque deposits, as the cheque moves through its multi-day clearing process, realities stretch and shift. What appears as available funds to the victim is simultaneously a provisional credit to the bank and a potential liability in the financial institution's accounting process. These overlapping realities are enacted simultaneously across sites—the customer's interface, the bank's clearing system, and the interbank verification network—thus demonstrating how multiplicity unfolds through temporally distributed processes of becoming.

As Deleuze and Guattari describe, multiplicity moves from the virtual to the actual through potential forces, where continuous transformations occur through processes of recombination, variation, and becoming (Deleuze & Guattari, 1987). Reality, in this sense, is not static but continually produced through the unfolding of relational potentials. Building on this, Mol's notion of ontological politics highlights that realities are not singular or given but are enacted at specific sites, and the location of decision-making determines which version of reality becomes stabilized (Mol, 1999). Each site—whether institutional, technical, or professional—reshapes what is taken to be real and, consequently, reconfigures the ontological politics surrounding a phenomenon.

In the context of the cheque clearing process, the financial institution operates as the site of ontological decision-making, determining whether a transaction constitutes a violation of the

financial service agreement. Because institutions are responsible for assessing financial losses and investigating fraud, they hold the authority to define the nature of the cheque—whether legitimate, fraudulent, or misused. This mirrors Mol's example in medicine, where the presence of anaemia is not defined by the patient's experience of dizziness but by laboratory measurements of haemoglobin levels (Mol, 1999). In both cases, knowledge and authority are situated, and the site that holds epistemic power determines which version of reality prevails and how accountability, legitimacy, and risk are subsequently organized.

Additionally, the violation of financial service agreements places financial institutions in a difficult position, where they must continually navigate the financial and reputational consequences of customer actions. Procedural guidance for fraud investigators typically emphasizes minimizing monetary losses and mitigating reputational harm, yet these goals are not always achievable, particularly when customers fail to follow preventative instructions. As several industry practitioners explained, while banks may impose account restrictions or implement safeguards in response to risky behaviour, violations of financial service agreements, particularly in the form of scams, can still occur when customers insist on proceeding with questionable transactions despite warnings or restrictions.

Victims often act within fabricated realities, believing in non-existent jobs or fictitious romantic relationships. These realities are deeply affective and convincing, leading victims to trust the fraudsters more than the legitimate institutions attempting to protect them. When victims do not disclose the full situations they are facing, the financial institution remains unaware of the lived reality driving the transactions. Fraud investigators may speculate on the type of scam involved, drawing on behavioural cues and transaction patterns, but even with investigation and persuasion, intervention becomes nearly impossible if the customer chooses to

act within their own version of reality. In such cases, the multiplicity of realities—the victim's trust, the fraudster's manipulation, and the institution's procedural logic—creates a field of partial connections where prevention and protection become profoundly difficult to enact.

The following two interview excerpts illustrate how industry practitioners also face challenges when customers disregard fraud education and system-generated alerts, choosing instead to proceed with transactions that ultimately result in fraud losses. These examples reveal the limits of institutional intervention within the cyber financial crime assemblage: despite layered safeguards—fraud warnings, authentication prompts, and educational messaging—customers' actions can reconfigure the intended protections. For practitioners, this creates a tension between institutional responsibility and user decisions, highlighting how the enactment of security is not solely technological but relational in the complex multiplicity.

> In terms of client intentional service agreement violation, we can place restrictions on the accounts, but there's no guarantee that the consumer won't do it in other ways, right? To conduct more fraud. If it all goes to scale, we can educate and educate as much as we want. But sometimes, especially in a romance scam, the customer will still proceed regardless of what we tell them, right? (Interviewee #E5M8-TZRB)

> So I guess I might be a little biased on this, but like we do see a lot of times where people, for example, are very educated or knowledgeable, fall victim to a romance scam, right? And they give away hundreds of thousands. I've had incidents where I've had to literally go out of my way and risk my job to stop them from giving money to the fraudster. Right? And these kinds of scenarios where they just really fell deep into the scam. Like, there's only so much control that the bank has. So I feel that in most cases

where the customer should know better, it's not the responsibility of the bank, right? (Interviewee #2YNV-3L4Y)

The quotes from Interviewee #E5M8-TZRB and Interviewee #2YNV-3L4Y illustrate how responsibility and control are distributed unevenly across the assemblage: even when protective measures exist, the enactment of security remains contingent on the choices, understandings, and interactions of both human and non-human actors. As interviewees noted, many industry practitioners believe that responsibility ultimately rests with the victim, rather than with financial institutions. This reflects a prevailing institutional logic in which authorization equals consent, regardless of the social or emotional context in which that authorization is produced.

Unfortunately, in practice, victims may bypass the protections that banks design to safeguard them, insisting on sending money to scammers despite warnings or intervention attempts. In doing so, scam victims enact their own version of cyber financial crime, one where trust, fear, or persuasion temporarily override procedural control. This example shows how multiple realities of responsibility coexist within the assemblage—legal, procedural, emotional, and technological—each shaping how security, fault, and victimhood are understood and performed.

As Law outlines, the study of multiplicity begins with attention to practice (Law, 2004). First, one must attend to what is being done, such as the empirical details of how relations are materially and discursively assembled in specific sites. Second, one must abandon the assumption that there exists a singular, stable reality independent of practice and instead ask how such a world is continually enacted through practice and made to hold together. Third, one must consider how these processes work to erase their own conditions of production, transforming

situated practices into restructured realities. Fourth, one must recognize that there is no escape from practice. Finally, one must look for the gaps, tensions, and contradictions between practices and the realities they produce, as differences always emerge in these intricacies (Law, 2004, p. 157–158).

Building on Law's attention to practice and enactment, these insights can be traced within the domain of cyber financial crime prevention. An approach informed by multiplicity directs analysis toward how fraud prevention and fraud education are accomplished in practice: how warnings are generated, circulated, interpreted, and acted upon by heterogeneous human and non-human actors. The effectiveness of fraud prevention, as described by practitioners, is not solely determined by the design of the system or the bank's communication. Instead, it depends on how various stakeholders respond. Fraud prevention systems do not operate as isolated technical solutions; they function within a broader context that includes institutional actors, customers, and digital infrastructures. First, institutional communication generates warnings intended to guide action across this configuration. Then these warnings enter practice where they are interpreted and enacted in ways that do not necessarily align: customers may understand alerts differently than anticipated, frontline staff may rely on experiential judgment that sits uneasily alongside standardized protocols, and digital infrastructures may intervene through automated blocks, delays, or system thresholds that redirect decisions. Finally, these situated interpretations and enactments do not simply mediate the warning but actively reorganize how authorization, responsibility, and protection are distributed in each encounter. Fraud prevention outcomes therefore emerge through the coordination—and miscoordination—of these heterogeneous practices, where security is enacted and its limits become visible.

Bank Investigator Impersonation

The realities become even more entangled when a bank investigator is impersonated, blurring the boundaries between legitimacy and deception and making the different versions of truth increasingly difficult to distinguish. According to CBC News, a woman from Hilden, N.S. was involved in a telephone investigator scam where she lost $15,000 (Mulligan, 2019). The woman received a call from an unknown caller and thought it was a bank investigator scam, then the scammer urged the woman to hang up the phone and dial the number on the back of her debit card. When she did, the scammer answered the phone and eventually scammed $15,000 out of her bank account.

This example illustrates how non-human actors can intensify the entanglement between fraud alerts and investigator scams. *TD Stories*—TD Bank's corporate storytelling platform—describes how fraudsters use call-spoofing tools and landline technologies to make a call appear to originate from a legitimate company or financial institution, and advises customers to hang up and independently contact their bank to verify the situation (TD Stories, 2019). However, in some landline systems the connection is not immediately terminated when the victim "hangs up." Fraudsters exploit this brief delay, remaining on the line and intercepting the victim's attempt to place a verification call. When victims attempt to call their financial institution back, they may remain unknowingly connected to the fraudster. The fraud then escalates when an individual posing as a bank representative pretends to answer the call, presenting themselves as a legitimate institutional representative. Believing that they are cooperating with a bank-led investigation, victims may comply with instructions to transfer funds, thereby unintentionally facilitating the fraud. Industry practitioners report that this form of impersonation-based fraud is increasingly prevalent. As one investigator explains:

> What we're seeing now is a rise in investigator scams. These are situations where customers receive unsolicited phone calls and are given a false pretense—that they need to assist with an investigation or take urgent action. (Interviewee #NF8T-GHAB)

This shift highlights how authority, urgency, and institutional trust are actively mobilized within the cyber financial crime assemblage, reshaping how consent and cooperation are enacted in practice. From the victim's perspective, the individual from Hilden, Nova Scotia, reported in CBC News correctly suspected a potential scam and took what appeared to be the appropriate precaution by hanging up and calling the legitimate bank number printed on the back of her debit card. However, the fraudster had manipulated the landline connection and intercepted the call, allowing the deception to continue under the guise of the legitimate institution. The victim's awareness therefore did not terminate the interaction but prompted a tactical escalation in which control was maintained through the communication infrastructure itself. From the financial institution's standpoint, the resulting transactions appeared fully authorized, with no visible indication that the customer was being manipulated. Technologies such as call spoofing and line interception tools introduce additional layers of multiplicity within the cyber financial crime assemblage, producing overlapping and contradictory realities across technological, procedural, and experiential sites. As scam techniques and technologies continue to evolve, these coexisting realities are repeatedly enacted and reconfigured, making the boundary between legitimate activity and deception increasingly difficult to discern. From an institutional perspective, this ambiguity is particularly pronounced in situations where customers voluntarily disclose confidential information. One industry practitioner described this as a critical point of vulnerability:

> When clients give up their confidential information, that's where banks face the biggest challenge. We try very hard to educate clients not to share this information, but once they do, it becomes the most vulnerable point for both the client and the bank—because at that stage, there is very little the bank can do. (Interviewee #R5PL-5ST9)

This observation underscores how responsibility, control, and vulnerability are unevenly distributed within the cyber financial crime assemblage. Even as financial institutions invest in preventive education and technical safeguards, evolving scam practices continue to exploit moments where institutional protections give way to user action, further complicating efforts to clearly distinguish deception from legitimate participation.

Malicious actors are also aware of these (mis)user-driven innovations and continually adapt their scams to exploit them, including deceiving customers into sharing their OTPs. In bank impersonation scams, fraudsters often possess enough personal and transactional information to convincingly pose as legitimate bank representatives, leading victims to genuinely believe that their financial institution initiated the interaction. Within the victim's reality, the act of sharing an OTP is a gesture of cooperation and trust; within the institution's reality, it constitutes a breach of security protocol. Consequently, when victims unknowingly provide their OTPs to unauthorized users, they are often classified as misusers because they have violated the financial service agreement, resulting in denied reimbursement claims. This incident further illustrates how multiple, conflicting realities of authorization, trust, and fault coexist within the cyber financial crime assemblage.

In conclusion, this section argues that a single cyber financial crime incident can generate multiple and contradictory realities of victimization, revealing the multiplicity inherent in how such events are enacted and understood. From the financial institution's perspective, a service

agreement violation signifies customer liability; from the victim's standpoint, it is an experience of deception and harm; and for the fraudster, it represents successful manipulation. These human and non-human actors—the victim, the institution, the fraudster, digital platforms, and algorithms—form an assemblage held together by (mis)uses, each producing a distinct but interconnected version of reality. In response, financial institutions have developed new strategies as forms of (mis)user-driven innovation, recognizing that traditional protections like passwords are no longer sufficient. Yet this innovation is itself multiple: as institutions introduce new defences, misusers simultaneously adapt and reconfigure these measures to exploit emerging vulnerabilities. Fraud alerts, one-time passcodes, and authentication systems thus become sites where innovation, misuse, and adaptation coexist, reflecting the ongoing multiplicity of the cyber financial assemblage, a dynamic system in which human trust, institutional rules, and technological infrastructures continually interact to produce new risks, responses, and realities of security and exploitation.

6.4 The Work of Blame: Mobilizing Faults and Multiplying Accountabilities

In STS, the concept of mobilizing objects highlights the role of non-human actors within the heterogeneous networks that compose scientific, technological, and social practices. These objects are not passive tools but active mediators that circulate across contexts, shaping meanings, relations, and outcomes. The notion of *mobilizing* refers to how entities move and transform across different sites, functioning as intermediaries that convey, reinterpret, or modify information, responsibilities, and relationships within a network (Callon & Rabeharisoa, 2003; Irwin, 2008; Law & Callon, 1992). Seen through the lens of multiplicity, mobilizing objects do not enact a single, stable function; rather, they participate in the coexistence of multiple realities,

as their meanings, roles, and effects shift as they navigate through diverse sociotechnical arrangements. In this dissertation, I use the concept of mobilizing objects to examine how loss accountabilities, as non-human actors, perform and reconfigure multiple versions of responsibility within the cyber financial crime assemblage, mediating between institutional, regulatory, and experiential realities of fraud, liability, and victimization.

Callon's analysis of the electric vehicle project shows that technological innovation develops through processes of translation in which artifacts, state policies, industrial infrastructures, and human actors work to define problems, assign roles, and align one another within a shared configuration (Callon, 1986). Stabilization occurs when these translations hold—when actors accept the identities and responsibilities attributed to them—producing a temporary order that appears coherent, even though it remains contingent and open to change. Translation also involves displacement, as actors speak and act on behalf of others, redefining interests while sidelining alternative possibilities; moments of breakdown make these claims visible and reveal that coherence depends on continued negotiation. This logic clarifies dynamics within the Canadian financial ecosystem, where policies, technical systems, organizational procedures, and everyday professional practices shape what counts as risk, loss, responsibility, and protection. Fraud detection tools classify transactions, compliance protocols set thresholds, and frontline staff interpret alerts in interaction with customers; together these practices distribute accountability and make some losses visible while obscuring others. Cyber financial crime therefore takes shape through these shifting alignments between technical designs, institutional priorities, and policy interventions, where security and loss emerge as effects of translations that temporarily stabilize particular versions of threat and institutional action.

Seen through this understanding of translation and provisional stabilization, and through the lens of multiplicity, cyber financial crime technologies, policies, and operational decisions can be understood as mobilizing objects. They work to stabilize particular versions of responsibility and risk by aligning actors, defining thresholds, and attributing agency; at the same time, these very stabilizations reconfigure the field of action, opening new spaces of vulnerability, displacement, and contestation. What appears as protection in one alignment may generate exposure in another, as the ordering of security simultaneously redistributes uncertainty and loss.

In this section, I outline the three most common outcomes of how faults and accountabilities are distributed in fraud claims within the cyber financial crime assemblage. First, I examine how the Zero Liability policy, though designed to protect consumers, remains contingent and open to multiple interpretations, as financial institutions strategically mobilize its terms to shift losses onto victims under certain conditions. Second, I illustrate how institutions can leverage their situated knowledge to re-mobilize fault away from valuable customers, offering goodwill reimbursements to preserve profitable or long-standing relationships, even when customers have technically violated service agreements. Finally, I analyze how banks may choose to end relationships with repeat victims as a preventive measure aimed at limiting future fraud-related exposure. This form of exclusion illustrates how the assignment of responsibility functions productively, reorganizing relations of risk and protection rather than simply determining fault. From the perspective of multiplicity, such decisions do not remove risk from the system but redistribute it across different actors and settings. Institutional safeguards may coincide with increased vulnerability for customers as they transition to other financial arrangements or service environments. At the same time, distinctions between “legitimate

customer" and "higher-risk account" are continuously enacted through policy criteria, system classifications, and professional judgment. The cyber financial crime assemblage therefore remains dynamic, as actors, risks, and accountabilities are shifted and reconfigured, showing how efforts to stabilize security in one domain can reshape conditions of uncertainty in others.

Zero Liability Policies and Protections

To begin with, most financial institutions implement Zero Liability policies to protect customers from financial losses resulting from unauthorized transactions, i.e., transactions that occur without the account holder's knowledge or consent. Under this policy, loss accountability falls on the financial institution, which must reimburse the customer when such transactions take place. The intent behind Zero Liability is not only protective but also strategic: it aims to build consumer trust and confidence in digital banking technologies, encouraging adoption by assuring users that their funds are secure even in unfamiliar digital environments.

However, when cyber financial crime occurs, the boundaries of liability become blurred. The conditions of reimbursement are often tied to behavioural and contractual expectations, such as compliance with service agreements or adherence to security protocols. According to the Financial Consumer Agency of Canada (FCAC), consumers can be liable for fraud losses if they use easy-to-guess numbers for their PINs (such as date of birth or telephone number), reveal their PIN to someone else (including a family member), have their PIN written down in proximity to the bank card, fail to take the necessary steps to protect their PIN, or fail to report lost or stolen cards in the amount of time specified in the service agreement (Financial Consumer Agency of Canada, 2018). Additionally, if consumers refuse to cooperate in an investigation of unauthorized use or make fraudulent deposits using bank accounts, consumers may also be liable for any fraud losses.

FCAC fraud loss liability rules often contradict the Zero Liability consumer protection policies, producing multiple, coexisting realities that financial institutions can interpret and enact differently. When financial institutions market their digital products and services, they often emphasize the Zero Liability policy to build consumer trust and encourage digital adoption by assuring customers that they are protected from unauthorized transactions. However, when fraud actually occurs, the fine print of adjudication guidelines, particularly those aligned with the FCAC, quickly surfaces. While the Zero Liability framework suggests that customers should not bear losses from unauthorized transactions, the FCAC's rules introduce situational conditions such as consumer behaviour, negligence, or contractual breaches that allow institutions to redefine what counts as unauthorized.

Within the Canadian financial ecosystem, institutions hold privileged access to extensive transaction data, authentication logs, and behavioural analytics, enabling them to unilaterally determine whether a transaction was authorized. The asymmetry of knowledge and interpretive power allows financial institutions to mobilize policies strategically, enacting accountability in ways that align with their operational and reputational interests. For instance, using digital technology investigation tools and transaction record platforms, financial institutions in Canada can have sufficient resources to collect digital evidence against technology misusers. Using information such as device ID, IP address, login credentials, internet service providers, operating systems, customer profiles, and transaction histories, financial institutions can easily create a customer profile to assess the loss accountability of a cyber financial crime incident.

In addition, fraud adjudicators collaborate closely with Predictive Analytics and Transaction (PAT) platforms, integrating algorithmic insights to evaluate case risk. These insights can directly influence reimbursement decisions. For example, when a transaction has not

been flagged as high risk by the system, adjudicators are often more inclined to believe that it was initiated by the customer, leading to a higher likelihood of claim denial. This outcome reflects the production rules embedded within the platform, which define what counts as unusual activity based on parameters such as recognized devices, consistent IP addresses, and familiar transaction patterns.

The PAT platform also organizes data on key factors such as transaction type, amount disputed, frequency of fraud attempts, and possible involvement of malicious technological actors, thus enabling adjudicators to align human judgment with machine-calculated risk. Yet not all claims represent clear-cut cases of fraud: some consumers deliberately exploit the process by falsely disputing authorized transactions, while others are victims of scams who willingly authorized transactions under deception.

As Callon and Law argue, objects do not merely reflect the world—they perform it (Callon, 1986; Law, 2004). The PAT platform, through its algorithms, interfaces, and classification rules, continually enacts accountabilities, shaping how human adjudicators interpret and act upon each case. In this sense, the platform's automated operations and data structures participate in the co-production of knowledge and decision-making, transforming abstract behaviours into actionable judgments, ultimately enacting a particular version of reality. The fraud detection process, therefore, is not simply a technical procedure but a multiplicity of human and non-human performances. These overlapping realities of algorithmic assessments, institutional protocols, and human interpretations further complicate adjudication, revealing the multiplicity through which fraud, intent, and legitimacy are simultaneously enacted and contested within the cyber financial crime assemblage.

Multiplicity of Reimbursement Realities

At the time of writing this dissertation, Canadian financial institutions typically do not reimburse claims related to scams. According to service agreements by major Canadian financial institutions, most of the banks are not reimbursing claims if customers willingly authorized the transactions themselves (BMO, 2023a; CIBC, 2023; RBC, 2018; Scotiabank, 2023; TD Bank, 2023a). As a result, industry practitioners are more inclined to mobilize the loss accountabilities on the scam victims' sides, as they have authorized the transactions. The Zero Liability policy protects customers against financial losses from unauthorized transactions. However, if a customer initially authorizes a transaction and later reports it as fraudulent due to being scammed, industry practitioners are likely to consider these losses as the customer's responsibility based on FCAC rules. This differentiation helps maintain the integrity of the policy while addressing fraudulent claims.

Interviewee #MBC5-GZ8U shares that it is hard for the bank to protect the customer if the customer decides to carry out offline transactions, such as physically going into a branch and withdrawing cash and giving it to the scammer. Authentication and enhanced fraud protection can only be useful when the customer is not proactively initiating the transaction. If the victim initiates the transactions themselves, there is nothing much the financial institutions can do:

> We can try to prevent other […] fraudsters from entering your account, where we have control we can ID stuff but if it's you willing to go, you know, physically go to the branch, take out your money and then send it off to someone. [It will be hard for the bank to protect you]. (Interviewee #MBC5-GZ8U)
>
> And then for wires really, because our customers, especially for personal banking customers, they are actually going into the branch to make that transaction. And so we do

> tell like, our tellers, to educate them before helping them to make the transaction, right? But sometimes clients are like customers, they get stubborn and they don't want to hear about it, right? They think that they think that we warn them every time and it's just too much. (Interviewee #AR26-4DEE)

Both Interviewee #MBC5-GZ8U and Interviewee #AR26-4DEE emphasized that financial institutions employ multiple communication strategies and channels to warn customers about emerging scam trends and to intervene before money is transferred to fraudsters. However, as both practitioners noted, victims sometimes ignore or dismiss these warnings, convinced by persuasive fraud narratives or emotional manipulation. This limits the institution's ability to prevent cyber financial crimes, particularly when customers authorize transactions using valid identification and pass all authentication measures. Once a transaction is authorized, the system marks it as legitimate, even if it was executed under deception.

This situation exposes a critical tension in the cyber financial assemblage: while security infrastructures are designed to detect unauthorized access, they struggle to account for authorized deception, where human trust, affect, and persuasion override technological safeguards. Canadian financial institutions acknowledge their responsibility to inform customers about the risks associated with certain types of transactions, such as sending money to a country they have never sent to before or borrowing funds to transfer overseas. However, when customers insist on proceeding with such transactions, Canadian financial institutions often believe that they have fulfilled their duty by informing the customers of the risks and consequently mobilize the loss accountabilities to the victims:

> We made changes to like, the OTP message received via SMS or via phone call advising that they don't share those, and will never ask for this code and never share it but we still find [this type of victimization] over and over again. (Interviewee #E5M8-TZRB)

Interviewee #E5M8-TZRB refers to scam victims as a "reputational risk" when the customer is not willing to accept that they were a victim of a scam:

> Scams [victims] are a reputational risk, because this individual is not willing to accept the fact that they're a victim of a scam. So they will continue to deplete funds […] There's no way to stop the activity. (Interviewee #E5M8-TZRB)

In these cases, the Zero Liability policy becomes contingent and negotiated rather than absolute, revealing how such policies operate as mobilizing objects that shape accountability, redistribute risk, and enact multiple realities of protection and blame within the broader cyber financial crime assemblage. From the perspective of financial institutions, when they are unable to prevent victims from transferring money to scammers—particularly in cases where the customer willingly authorizes the transaction—they mobilize the financial service agreement to redefine the boundaries of liability. This contractual framework is used to justify that the Zero Liability policy no longer applies, effectively shifting fault onto the customer and positioning the victim as responsible for their own losses.

A similar dynamic appears in Yates et al.'s study of hydro-ontological contestation in British Columbia, where water is enacted through divergent ontological realities (Yates et al., 2017). Effectively, water becomes political: drinking water is prioritized through public health infrastructures; environmental regulators approach it through technocratic treatment regimes; while for Indigenous communities, water is understood through the *En'owkin* principle and as *siwlkw*—a living being, a lifeblood. These differing enactments do not simply represent

alternative perspectives on the same object; they generate distinct political projects, governance practices, and ethical obligations. Multiplicity therefore results in competing yet overlapping modes of action, as each reality of water calls for different interventions, authorities, and criteria for what counts as protection, harm, or responsibility. These ontological differences shape who is recognized as a legitimate decision-maker, what forms of evidence are considered authoritative, and which risks are considered urgent. As a result, political conflict does not arise only from disagreement but from the coexistence of partially connected realities that organize action in fundamentally different ways.

Likewise, within the assemblage of cyber financial crime, institutional practices enact a particular version of reality organized around procedural compliance, evidentiary thresholds, and contractual interpretation, while customers' lived experiences of coercion or deception may not align neatly with these categories. As in the hydro-ontological case, these are not simply differing viewpoints but enactments that carry distinct practical consequences, shaping how responsibility, protection, and loss are defined and addressed. This redistribution of responsibility shows that policy instruments and operational procedures do not merely respond to events but participate in producing the conditions through which events are recognized, evaluated, and acted upon. Multiple, co-existing realities therefore emerge through these processes, each organizing authority, accountability, and intervention in different ways.

(Mis)user-Driven Innovation: Knowledge and Re-Mobilization of Fault

The next boundary object I examine is the situated knowledge that financial institutions acquire during fraud investigations and how it enables the re-mobilization of fault away from certain customers. This knowledge allows institutions to make discretionary judgments about accountability, often resulting in goodwill reimbursements for customers deemed financially or

strategically valuable. Even when these customers have technically violated service agreements, their accountabilities are diminished because their long-term profitability, asset holdings, or borrowing potential outweigh the cost of reimbursement. In such cases, situated knowledge functions as a mobilizing object, guiding how institutions selectively interpret evidence and redistribute blame and in turn demonstrating that accountability within the cyber financial crime assemblage is not fixed but relational, negotiated, and contingent upon institutional interests. This form of knowledge—context-specific, institutionally embedded, and asymmetrically distributed—plays a decisive role in shaping how authorization and loss accountability are determined.

Drawing on Haraway's concept of situated knowledge, this institutional epistemology is not neutral but positioned (Haraway, 1988). Its value and authority are grounded in specific technological, regulatory, and organizational contexts. As Code emphasizes, knowing is inseparable from the conditions and power structures that make it possible; knowledge is legitimate not by its universality but by its embeddedness in particular situations (Code, 2006). Similarly, Irwin notes that knowledge cannot be detached from its development or application: it is always contingent, contextual, and co-constructed (Irwin, 2008). In this sense, financial institutions' situated knowledge functions as a mobilizing force within the cyber financial crime assemblage, shaping how realities of fraud, authorization, and accountability are enacted, stabilized, and contested.

Using situated knowledge, Canadian financial institutions can mobilize the loss accountability of cyber financial crime. A part of "knowing" is also knowing how to "work the system," in other words, how to make consumers acknowledge their misconduct and how to shape their victimization experiences based on each case scenario (Irwin, 2008). Even though

Canadian financial institutions do not sell products similar to the Protected Card Insurance sold in Peru to mitigate fraud losses, Canadian financial institutions have the institutional power to reshape the loss accountabilities of cyber financial crime using unique knowledge that is not available to outsiders.

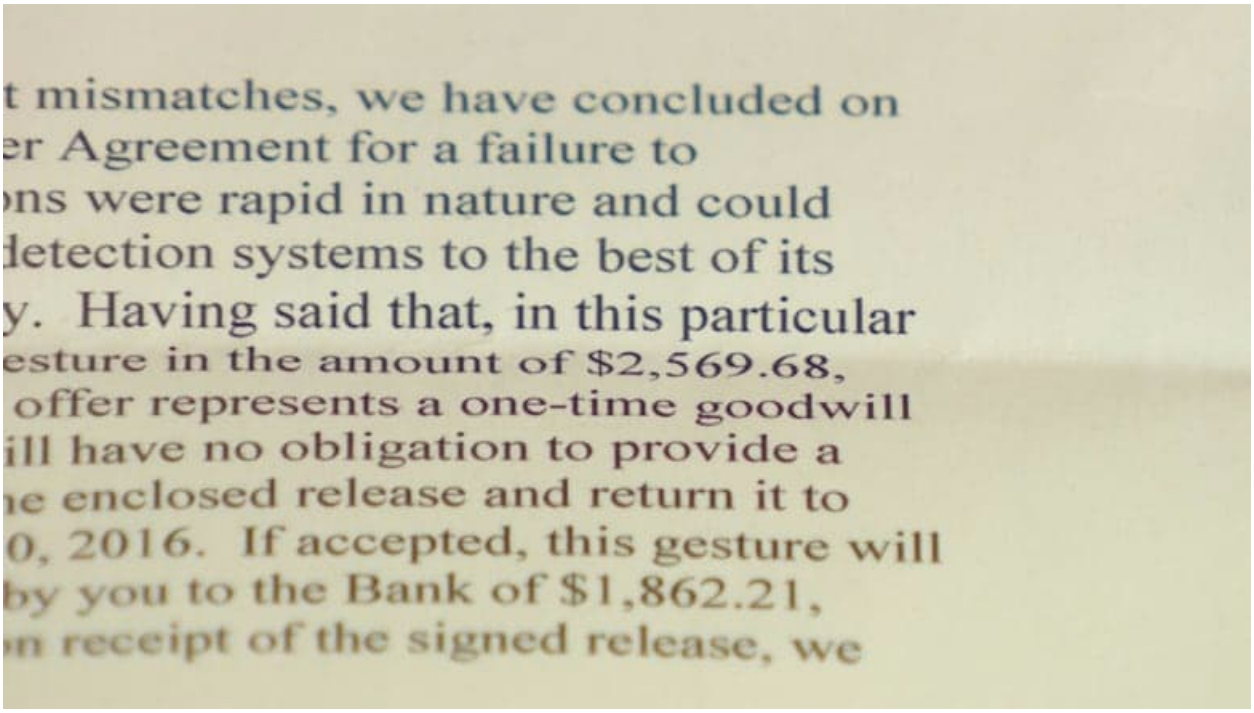
For example, mobilizing loss accountabilities can also be contingent on individual cases. Some industry practitioners might give a "goodwill" reimbursement to first-time offenders for educational purposes depending on the situation. Many cyber financial crime victims truly do not understand how and why the incident happened, especially when they are scammed into committing certain cyber financial crimes.

> We do take that into consideration […] clients' opinion does matter to us. After all, the financial institution is trying to lead in client experience. What we do is we try to balance […]. And then we do ask for some kind of proof. Right? Like if you're looking for a job and got scammed […] we do ask for documentation. Hey, could you send us info when and what kind information was shared? (Interviewee #WYUV-P7LK)

Scam cases are paid out on an exception basis as goodwill acts (Figure 7). Canadian financial institutions may choose to fully reimburse or partially reimburse customers, especially those that appear in the media (Johnson, 2021; Ombudsman for Banking Services and Investments, 2020).

> Some interview participants agreed that the banks sometimes do pay out for goodwill:
>
> If we were to consider goodwill, for goodwill, we need to consider external risk factors. Same thing if we were to consider reaching out to legal or [compliance department] it would be due to external risk factors. (Interviewee #E5M8-TZRB)

Figure 7. An Example of Goodwill Fraud Claim Reimbursement



Note. Screenshot from "TD Bank Customer Frustrated with Fraud Investigation Leaving Him Owing Thousands," by B. Brach, 2017, October 10, *CBC News.* https://www.cbc.ca/news/canada/british-columbia/td-customer-fraud-unhappy-1.4341899.

Some interviewees from credit unions or smaller financial institutions said they may reimburse claims in order to maintain a good member relationship, because they consider the victims to be members of their organizations rather than customers.

> I mean, at [credit union], we were fairly liberal on what we reimbursed versus what we didn't. There wasn't a lot of claims that we denied. But if we did it was, it was because we could clearly see you know, what has what had happened and, and it was it was fairly obvious that you know, that customer was negligent in what they did in causing the loss. And usually not only that, but they didn't take steps fast enough to help mitigate any further loss either. (Interviewee #Undisclosed)

Comparatively speaking, investigators and adjudicators of fraud claims from the Big Five banks are stricter when it comes to reimbursing customers. One of the key differences here is that Big Five banks see their customers as consumers, and they have the discretion to end the relationships as needed; however, credit union investigators and adjudicators try their best to maintain good membership relationships and not to jeopardize their members' best interests.

> But if a client is continually not protecting themselves and are misusing it […] the bank is still a private organization and will have the free choice to enter or exit a relationship with a client. (Interviewee #76MW-WT9E)

> There's obviously like [...] certain rotten apples in the basket, right? By restraining and restricting, for example, we're restricting a portfolio that has conducted client intentional fraud […] if there's no evidence of […] the customer being a victim of a scam, or being coerced or deceived, those portfolios could be restricted and exited. (Interviewee #3NGU-8XTJ)

In these goodwill gestures, financial institutions may choose to reimburse victims as a means of retaining valuable customer relationships, even when the evidence suggests possible customer liability. Here, the multiplicity of accountabilities becomes visible. Drawing on their situated knowledge, financial institutions may determine that a customer has fallen victim to a scam and technically violated the financial service agreement, which would normally lead to the decline of a fraud claim. However, when broader relational factors are considered, such as a long-standing relationship, significant financial assets, or profitable borrowing activities, financial institutions may re-mobilize fault away from the customer, framing reimbursement as an act of goodwill. In other words, financial institutions possess sufficient situated knowledge to

strategically “work the system” (Irwin, 2008), shaping investigative outcomes in ways that align with their preferred realities and institutional perceptions of truth.

This selective enactment of accountability illustrates how loss allocation is not predetermined but continually negotiated, contingent upon institutional priorities, relational dynamics, and contextual interpretations. Barad’s theory of agential realism in *Meeting the Universe Halfway* provides a useful lens for understanding this process (Barad, 2007). Barad conceptualizes *intra-action* as the ongoing dynamism through which relations of matter, meaning, and practice are continually configured and reconfigured. According to Barad, reality does not pre-exist but emerges through entangled performances of human and non-human agencies.

In the context of cyber financial crime adjudication, technological evidence such as data analytics, transaction modes, and behavioural profiles interacts with institutional and political practices to produce multiple realities of accountability. For the customer, the reimbursement may appear as an unexpected act of empathy, unaware that it reflects a strategic realignment of institutional priorities rather than a reversal of liability. For the financial institution, it is a tactical reconfiguration of responsibility, aligning moral gestures with operational and reputational interests to preserve customer trust and retain high-value clients. Through these intra-actions, accountability becomes multiple: simultaneously, it is moral when framed as fairness to the victim; it is procedural when governed by adjudication rules; and it is economic when shaped by cost–benefit considerations. Financial institutions’ capacity to mobilize data, policies, and technical expertise enables them to stabilize particular versions of events—versions that often reinforce institutional authority while marginalizing alternative interpretations offered by victims or external regulators.

Intent, Misuses, and Behaviours

Another crucial component of the cyber financial crime adjudication process involves determining whether a consumer exhibits fraudulent intent or is attempting to misuse reimbursement policies. When a customer submits multiple claims within a short timeframe and the claim frequency appears abnormally high, adjudicators often conduct additional assessments of intent and may ultimately decline reimbursement. Using device history, transaction patterns, merchant data, and geolocation information, adjudicators can sometimes identify clear indications of malicious or opportunistic behaviour. This evaluative practice illustrates the multiplicity inherent in the cyber financial crime assemblage: adjudication outcomes are shaped not by a single universal rule but by the interplay of historical records, algorithmic indicators, and contextual interpretations. A customer's prior claims history, for example, influences how subsequent cases are understood. Those with a clean record are more likely to have claims approved, while repeat claimants may face heightened scrutiny. These contingent and relational judgments show that accountability is enacted differently across each case, reflecting multiple, overlapping realities of fraud, intent, and legitimacy within the adjudication process.

Furthermore, even when adjudicators identify fraudulent activity within a claim, not all disputed transactions receive full reimbursement. Customers sometimes submit both legitimate and unauthorized transactions within a given period because unfamiliar or unclear entries make it difficult for them to distinguish genuine activity from fraud. In such cases, adjudicators engage in a collaborative process with consumers to clarify the details and gather further evidence. For example, if both fraudulent and legitimate transactions are detected within the same claim, adjudicators may contact the customer to verify which ones were authorized. Consumers are often asked to recall their activities on the transaction dates, as some legitimate purchases may

appear unfamiliar due to merchants' names (e.g., corporate or parent company names rather than store names). Adjudicators also analyze the mode of transaction: for example, if fraudulent activity occurred online through a malicious website, in-person purchases at a regular grocery store during the same period are likely genuine but mistakenly included. Through these exchanges, human adjudicators and customers co-construct the claim's narrative, distinguishing between legitimate and illegitimate transactions. In most cases, this collaborative clarification leads to partial reimbursement, where only verified fraudulent charges are compensated. This process illustrates how legitimacy and authorization are relationally mobilized within the cyber financial crime assemblage, revealing that fraud adjudication is not purely procedural but an ongoing negotiation shaped by memory, interpretation, and situated judgment.

Losses, Accountabilities, and Risks

As illustrated in the above discussion, financial institutions can strategically shift accountabilities away from customers under certain conditions such as when they wish to preserve valuable client relationships or avoid media or legal escalation, when they find no evidence of product misuse, or when customers mistakenly include authorized transactions but cooperate in correcting them. These practices demonstrate that fault within the cyber financial crime assemblage is inherently multiple. There is no fixed or universal rule that determines who is at fault or who should bear responsibility for financial losses. Instead, accountability emerges as a contingent and negotiated outcome, shaped by institutional priorities, situational contexts, and relational dynamics between customers, technologies, and adjudicators. Each case enacts a different configuration of truth and responsibility, revealing how the meanings of fraud, legitimacy, and liability are fluid, contextual, and multiply produced within the evolving assemblage of cyber financial crime.

However, this flexibility in accountability allocation does not imply that financial institutions tolerate repeat offenders or individuals who deliberately abuse financial services. While discretion allows institutions to re-mobilize fault in certain contexts, repeated or intentional misuse often leads to stricter interventions, such as claim denials, heightened monitoring, or even account termination.

My final example illustrates how financial institutions may choose to terminate relationships with repeat victims as a preventive measure to reduce future exposure to fraud-related losses. This practice reflects a shift from reactive loss management to proactive risk containment, where victims are reclassified as potential liabilities rather than customers in need of protection. By closing accounts or restricting services, institutions effectively redefine the boundaries of responsibility and trust, thereby transforming victims into risk objects.

Financial institutions can end the banking relationship with a customer (exiting a customer) at any time if the exploitation behaviours are aggressive or signs of abusing financial services persist after previous fraud education. Essentially, financial institutions do care about customer experience and ensure customers' accounts are thoroughly reviewed before making any restriction decisions. If customers take advantage of such a courtesy, however, financial institutions can discontinue the financial services. Interviewees #76MW-WT9E and #WYUV-P7LK both indicated that financial institutions may grant a one-time exception. However, if fraud involving the same user occurs a second or third time, the institution may terminate its banking relationship with that user:

> Three strikes and you're out. [...] I've worked in multiple previous financial institutions before this one. [...] there was a lot of the concepts around you get one free kind of one goodwill grace. (Interviewee #76MW-WT9E)

> And, again, we did not […] exit clients just based on one particular incident, okay. We do, you know, take those things into account. […] we give them a fair notice: hey, I did not do that. Good. We hope that you don't do it again. And then if they kind of do second time and third time I think then that's when you kind of get booted out because it's also a reputational risk as well. (Interviewee #WYUV-P7LK)

To industry practitioners, repeated victimization is rarely interpreted as an indicator that customers require more fraud education or that financial products and services need enhancement to prevent exploitation. Instead, such customers—those who have repeatedly violated financial service agreements—are often viewed as individuals who have exhausted institutional goodwill and may continue to abuse reimbursement policies. Within this framing, these customers represent both financial and reputational risks to the institution.

Consequently, the most effective strategy to mitigate institutional exposure is often to terminate the banking relationship altogether, thereby removing the perceived source of vulnerability. This practice exemplifies what Mol describes as multiplicity's ontological politics, in other words, the process through which one version of reality is privileged over others (Mol, 1999, 2002). Mol argues that reality is not pre-given or singular but enacted through practices. What counts as real emerges from the coordinated activities of knowing, measuring, and intervening. Yet, these enactments are never neutral: decisions about how to act, who may act, and what counts as legitimate knowledge shape which versions of reality are stabilized and which are excluded. In her study of the patient–laboratory–disease entanglement, Mol argues that medical practices produce multiple coexisting realities of a single condition, but institutional and professional hierarchies determine which version becomes dominant.

Similarly, in the context of cyber financial crime, financial institutions' decisions about which realities to privilege—for example, framing a customer as a liability rather than a victim—constitute inherently political acts. These decisions shape not only how fraud is understood and governed but also whose experience of reality is acknowledged and whose is dismissed within the assemblage. In the multiplicity of the customer exit scenario, when a financial institution chooses to terminate a client relationship, it enacts a specific version of reality in which the customer becomes a risk object, embodying potential financial and reputational harm. This act of redefinition is both politically and economically productive, allowing the institution to assert control, stabilize its preferred reality of security and efficiency, and mitigate exposure to future fraud losses. Although the customer exit decisions may compromise customer experience, they stabilize an institutional reality that prioritizes operational control, reputational integrity, and financial protection within the cyber financial crime assemblage.

Yet, in doing so, financial institutions silence alternative realities, namely, those of vulnerability, victimhood, and systemic asymmetry, thus revealing how ontological politics operates as a mechanism through which power, accountability, and legitimacy are continually reorganized within the cyber financial crime assemblage. By mobilizing situated knowledge, working the system to redistribute fault, and selectively enacting accountability, financial institutions maintain a delicate balance between risk management and customer relations, preserving their authority while managing reputational exposure. Through these practices, institutions repeatedly negotiate and redraw the boundaries of trust, legitimacy, and tolerance, illustrating that accountability within the assemblage is neither fixed nor evenly distributed but context-dependent and strategically bounded by institutional interests and regulatory constraints.

6.5 Conclusion

This chapter examines one of the defining characteristics of the assemblage, multiplicity. The concept captures the layered heterogeneity of human and non-human actors as multiple participating artefacts, the overlapping and contradictory realities they produce, and the shifting processes of becoming through which configurations of practice, meaning, and power are continuously reassembled.

Through three empirical cases, this chapter explored the different dimensions of multiplicity within the cyber financial crime assemblage.

The first case focused on the multiple enactments of authorization, where both human and non-human actors define legitimacy through their own situated logics, generating divergent realities that emerge from spontaneous and relational decisions. The second case traced how victimization is framed and experienced differently across institutional, technical, and personal domains, resulting in plural and sometimes conflicting enactments of victimhood. The third case examined responsibility and accountability as dynamic and negotiated processes, demonstrating how blame, liability, and protection shift across institutional practices and sociotechnical arrangements. Taken together, these analyses illustrate that a cyber financial crime assemblage is not a singular event or object but a multiplicity in motion—a distributed process where realities, relations, and accountabilities are continually enacted, contested, and remade.

Chapter 7 - Affectivity: Intensities, Forces, and Desires

7.1 Introduction

> "AFFECT/AFFECTION. Neither word denotes a personal feeling (sentiment in Deleuze and Guattari). L'affect (Spinoza's affectus) is an ability to affect and be affected. It is a prepersonal intensity corresponding to the passage from one experiential state of the body to another and implying an augmentation or diminution in that body's capacity to act." (Massumi, 1996)

The above passage appears in the *Notes on the Translation and Acknowledgements* section of *A Thousand Plateaus*, translated by Brian Massumi. Massumi interprets Deleuze and Guattari's use of the term *affect* as symbolizing a relational capacity to act and to be acted upon. According to Deleuze and Guattari, the intensity of the affect may increase or decrease according to the body's ontological movements (Deleuze & Guattari, 1987). Although Deleuze and Guattari were among the first to situate affect within assemblage thinking, the concept—also described as *affectio*—has a much longer cultural and philosophical lineage.

In *Before Emotion: The Language of Feeling, 400–1800*, Copeland traces the genealogy of the term affective through classical Latin rhetoric, focusing on *affectio* and *affectus*, terms that described the movements of feeling within the soul. Similarly, the Greek concept of *pathos* represents the passions or emotional states that move or act upon the subject. These early forms of affect concern the governance of emotion, emphasizing its role in persuasion, moral disposition, and virtue (Copeland, 2019). In ancient and medieval thought, the classical roots of the term affective largely align with the notion of feeling—a sense of emotion that reveals how the body and soul are susceptible to external influences, a meaning that remains prevalent in modern psychology.

Early modern philosopher Baruch Spinoza, however, reconceptualized affectus to describe the body's capacity for transformation. For Spinoza, affects emerge from encounters and experiences that alter a body's power to act: "affects push and pull us in different directions, determining our actions and behaviour, sometimes overwhelming us. Affects are also known as passions, because we are passive to the things that affect us" (Lord, 2010). In this view, affect is no longer an emotional feeling but a shift in capacity, a dynamic transformation of the body's potential to act and to be acted upon.

Spinoza's interpretation of affectus provided the philosophical foundation later taken up by Deleuze and Guattari, who extended the term into the ontological and relational dynamics of assemblages. For Deleuze and Guattari, affect does not refer to an emotional state of feeling but to a relational force of becoming: the capacity through which bodies, both human and non-human, enter into composition and transformation (Deleuze & Guattari, 1987). The affective field grants heterogeneous elements the power to interact, resonate, and transform one another within a multiplicity. This ontological movement generates varying capacities for an assemblage to disassemble and reassemble, producing forces of change that may be either absorbed into existing configurations or resisted by them.

In this chapter, I draw on Deleuze and Guattari's concept of the affective to describe the cyber financial assemblage and to illustrate how the field of becoming interacts with forces of change. The affective dimension reveals how human and non-human elements possess the urge, desire, and drive to configure and reconfigure the assemblage's existing formations. By tracing how these elements affect and are affected by one another, I argue that the cyber financial assemblage exhibits an ontological movement that generates intensities shaping the processes of account compromise, fraud detection and investigation, and reimbursement. These affective

forces are not merely reactive but constitutive, as they animate the assemblage's continual transformation and its capacity to negotiate stability and disruption.

7.2 The Urge to Exploit: Compromises, Tools, and Intrusions

Unauthorized users exploit consumers' financial information and bank accounts through a range of malicious tools and technological intrusions. These compromises manifest in multiple forms, most notably credential compromise and identity compromise. In this section, I examine these two forms of cyber financial crime to illustrate that unauthorized users, malicious software, and intrusive technologies are not merely constitutive components of the cyber financial crime assemblage. Rather, they are affective elements animated by relational dynamics, moving to intrude, to harm, and to evade within shifting configurations of opportunity and constraint. I then turn to the examples of unsecured loans and email money transfer limit increases to illustrate how business initiatives intended to enhance customer experience can evolve into (mis)user-driven innovations, enabling unauthorized users to further exploit digital banking technologies and services. Across these examples, I argue that this drive or urge functions as an affective force that binds the heterogeneous elements of the assemblage, generating both its coherence and its capacity for transformation (Deleuze & Guattari, 1987). Affectivity operates as the force of change, the energy that enables reconfiguration, and the source from which innovations emerge.

Credential Compromise

The first example is credential compromise, a form of exploitation involving the unauthorized acquisition of consumers' authentication information, such as credit or debit card numbers, residential addresses, and dates of birth. Credential compromise enables further intrusions into banking services and platforms, often resulting in credit card fraud, debit card

fraud, and other forms of transactional exploitation. Exploitation of banking services or systems using compromised credentials is usually constrained by the limited information available, as cybercriminals often do not have enough information to fully impersonate the victim. For example, they may be able to conduct fraudulent credit card transactions by possessing credit card numbers, credit card expiry dates, credit card CVVs, cardholder names, and billing addresses, but they may not have other information such as government photo identifications to further exploit the banking services or financial platforms.

In credential compromise incidents, cybercriminals may not necessarily need to directly interact with victims. They can obtain compromised credentials through cybersecurity incidents such as database breaches or botnet attacks (Capital One, 2022; Cross et al., 2019). Even if consumers diligently protect their sensitive financial information or actively avoid exposing their psychological weaknesses to malicious actors, they still face the risk of data compromise through service providers, both online and offline, through scams or through fraud. I asked interview participants how credential compromise impacts consumers in the world of cyber financial crime:

> All it takes is a card number and the expiry date back in 2010. I believe [that is the case] earlier when the mandate for EMV to move to chip technology on the credit card. That's fraud in the face-to-face environment. But what we see there was a shift in the fraud into the internet space. And I think the volume even bigger because the fraudster finds different ways …so there's a huge financial impact. (Interviewee #CVN3-7UBK)

As explained in the previous chapters, cybercriminals can leverage technological means such as botnets or web-based exploit kits to take advantage of online merchants or online

payment systems. The stolen data can also be traded in the illicit online marketplace such as the Dark Web.

> I feel like there's there's a lot of probability and how long until you're the next victim of fraud. There's suddenly breaches that happen. And there's so many, there's so much information that share in the dark web and online with customers data, that sometimes personally, I feel like it's so hard. (Interviewee #76MW-WT9E)

Interviewee #76MW-WT9E notes that the illicit trading of sensitive financial data in underground online marketplaces is difficult for financial institutions to manage. Unauthorized actors possess an urge to exploit financial infrastructures through compromised accounts, and this urge becomes a force that reshapes the cyber financial crime assemblage. Deleuze and Guattari describe affect as a potential or force of becoming that arises through encounters (Deleuze & Guattari, 1987). Within these interactions, compromised credentials, financial platforms, and customers' sensitive information continually modify the assemblage. Driven by affective forces, this urge is not static; it circulates between components, generating internal intensities that reconfigure their relations and, in doing so, transform the assemblage itself.

Malins, a critical drug researcher, draws on Deleuze and Guattari to argue that desire, rather than pleasure, is a more useful concept for understanding how relations, bodies, and power connect (Malins, 2017). Pleasure is limited because it refers to a specific feeling or experience. Desire, in contrast, is productive: it is a force that moves through relationships, enabling attachments, shaping actions, and sustaining connections. Assemblages therefore function through these flows of desire, which include not only enjoyment but also fear, obligation, hope, dependency, and care.

This distinction helps explain cyber financial crime in contexts such as relationship abuse, elder abuse, and domestic violence. Financial exploitation here is often tied to affective bonds rather than the pursuit of pleasure. Trust, intimacy, fear of conflict, or the desire to maintain the relationship can make harmful financial decisions appear necessary or reasonable from within the situation. Fraud in these contexts is therefore not only technical or cognitive but affective, as desire shapes how people act, how risk is perceived, and how responsibility is later interpreted. This dynamic is visible in forms of unauthorized transactions linked to relationship abuse, including elder abuse and domestic violence, where access to victims' credentials emerges through relational conditions rather than technical breach alone (Cross et al., 2018; Ma & McKinnon, 2022). Victims may share their credentials knowingly or unknowingly, willingly or under coercion, enabling malicious actors to appropriate these credentials and subsequently engage in further intrusions. Human vulnerabilities such as loneliness, anxiety, distress, insecurity, and fear of authority create affective atmospheres that render targeted individuals more susceptible to cyber financial exploitation. These emotional and sensory states are not merely psychological; they are productive forces that can affect and be affected, actively reshaping the relations and capacities within the assemblage.

For instance, a grandson who assists his grandmother with grocery shopping may later record her credit card details and use them for online purchases without her consent. In this case, the grandmother may have authorized the initial grocery transaction, yet once her credentials are compromised, subsequent transactions occur beyond her control. The grandmother's physical limitations and reliance on assistance for everyday tasks become part of a broader relational and affective configuration, one shaped by trust, dependence, and vulnerability. These affective and sensory conditions, including the embodied experience of aging, the need for care, and the

uneven distribution of digital literacy, co-produce the relational dynamics through which exploitation becomes possible. Within this assemblage, vulnerability itself becomes a productive force, one that can be affected and can affect, thereby reshaping how agency, trust, and control are enacted in the cyber financial crime assemblage.

In addition, physical security risks such as lost or stolen bank cards can compromise access to digital payment systems. In Canada, many debit and credit cards support contactless payment through technologies such as Visa payWave™, MasterCard Tap & Go™, and Interac Flash™, where digital credentials are embedded directly in the payment function (Canadian Bankers Association, 2021). When a card is lost, access to these payment capacities is displaced along with it. Although contactless systems include transaction limits, the design of fast, low-friction payments allows multiple purchases to occur in quick succession before intervention takes place. These repeated transactions create a tempo of activity that moves through payment infrastructures, detection systems, and institutional response processes.

Affectivity in this context does not refer to individual intentions or motivations. Instead, it describes the action-oriented environment generated by the payment system itself—its speed, ease, and permissiveness—which shapes what actions become possible and how events unfold. Contactless design reduces pauses, checks, and deliberation, allowing transactions to move quickly and with minimal friction. This produces a situational momentum in which actions can accumulate before they are fully registered by users or institutions. The system's architecture therefore creates a field of circulation where transactions, alerts, and responses are set into motion, each triggering further adjustments across platforms and actors. Affectivity here lies in this capacity of the environment to orient movement, accelerate sequences, and distribute pressures, making certain pathways of action more likely while narrowing others.

When compromised credentials are used to initiate transactions, banks and consumers may or may not detect the activity, depending on algorithmic alerts and individualized fraud monitoring systems. Consumers in these situations are typically responding to earlier data-compromise events rather than intentionally facilitating misuse. The exploitation that follows can be understood as affective, not in the sense of individual intent but as movement within a field of relations. Once credentials circulate beyond their original context, transactions unfold within an environment structured by speed, automation, thresholds, and response protocols. Affect, as Deleuze and Guattari conceptualize it, operates as the dynamic of desire within an assemblage—a force of becoming that exceeds individual actors and emerges through encounters among human and non-human elements (Deleuze & Guattari, 1987). It is a capacity for affecting and being affected, a circulation of intensities that moves across infrastructures, systems, and bodies. As Parr notes, these affective processes can become "enveloped by affection," translating into perceptions, decisions, and institutional responses (Parr, 2010, p. 12). Credential exploitation, therefore, is not only a technical breach but an affective event that sets sequences of transaction, detection, and adaptation into motion, reorganizing relations within the cyber financial crime assemblage.

Identity Compromise

Compared to credential compromise, identity compromise represents a more advanced form of fraud in which cybercriminals possess sufficient information to impersonate victims and exploit financial systems or services under their identities. The key distinction lies in the scope of information obtained: while credential compromise typically involves isolated data elements such as login credentials or account numbers, identity compromise entails a more comprehensive acquisition of personal information. In such cases, malicious actors can successfully pass identity

authentication processes—whether these are initiated by human agents or automated systems—thus allowing them to execute financial transactions or register for new banking services, all without the victim's awareness.

Examples of identity compromise include the compromise of digital banking credentials, compromise of verbal passwords or PINs for telephone banking authentication, biometric authentication compromise (fraudulent biometric authentication enrolment or biometrics data theft), fraudulent identification documents, in-person branch or phone channel impersonation, or any personal credentials used to access any banking services or banking rewards programs.

Technological vulnerabilities, human vulnerabilities, physical security risks, and insider threats can all lead to identity compromise. It is worth noting that although acts of identity compromise eventually target the financial industry for financial gains, not all identity incidents are originally triggered by service dealings in the financial service industry. Data breaches that happen in other industries or business sectors may also impact the security of consumers' identities.

One example of this type of data breach is the recent Shields Healthcare Group data breach (UpGuard, 2023). According to CBS News, the US Department of Health and Human Services Office for Civil Rights has confirmed that the Shields Healthcare Group data breach affected over two million people (CBS News, 2022). Sensitive personal information such as names, Social Security numbers, addresses, insurance information, and medical treatment information was exposed in this incident (CBS News, 2022). In cases like these, identity theft victims may suffer indirectly from other data breaches happening outside of the financial industry, but the cybercriminals eventually target financial institutions for material gains.

Fraudsters who are able to produce fraudulent identification cards or documents can also easily take over victims' accounts when they present the fraudulent identification to banks.

> Especially in cases of account takeovers, it's very common that once the fraudster knows a lot of your information and has taken over your account, they can do it again. So they already know all your information. They know your date of birth. They know your tracking number and all these things. So it's just a matter of how savvy we'll be knowing that, hey, this client was a victim before. Let's see if this is a fraud. So it's really tough. (Interviewee #76MW-WT9E)

The above examples of identity compromise show how non-human elements such as personal data, financial credentials, fabricated identification, and falsified authorization function as heterogeneous components that are both productive and affective. As Interviewee #76MW-WT9E explains, critical information capable of undermining digital identity can circulate with relative ease across different platforms and actors. Within this assemblage, human and non-human elements do not possess intentions but capacities to enter into relations, interact, and generate effects (Parr, 2010). The potential for exploitation arises from these relational conditions, as connections between data, infrastructures, and users enable new sequences of action. These affective dynamics are not reducible to technology or psychology; they describe the capacities of the assemblage itself to shape how relations form, how vulnerabilities emerge, and how configurations are continually reworked (Deleuze & Guattari, 1987).

(Mis)user-driven Innovation: Unsecured Loans

The two common types of compromises—credential compromise and identity compromise—demonstrate how human and non-human elements within an assemblage can be affective. My next two examples concern (mis)user-driven innovations, one involving unsecured

loans and the other the increase of email money transfer limits. Both cases illustrate how financial institutions continually evolve customer strategies to meet diverse needs and enhance satisfaction, while malicious actors simultaneously adapt their own tactics to exploit institutional infrastructures and circumvent protection and detection mechanisms for financial gain.

The first (mis)user-driven example concerns a type of unsecured loan. Unsecured loans are credit products developed by financial institutions that allow customers to borrow money without collateral. To mitigate repayment risks, institutions typically assess applicants' credit profiles to determine eligibility. These assessments are designed to minimize the likelihood of default, such as not repaying the borrowed money; however, as one interviewee explained, malicious actors often exploit these processes. According to Interviewee #LX4K-Z3DK, their team recently experienced a large-scale fraud attack targeting an unsecured loan product, revealing how the service was misused by misusers who manipulated the credit platform for illicit gain.

> For [a type of unsecured] loans launched last year, they took care of all the [technology design] aspects, except the part where if fraud happens, how will the recovery happen, because indemnity never used to recover loans. Never had to, because we never did that, right? But all of a sudden, a big wave came, and we lost millions of dollars under the loan [product].
>
> So this was a platform where people can apply for loans on the website using the [banking] credentials. Money gets deposited into any account they want… fraudsters found out about that particular loop, so they started applying with fake information or, you know, stolen information of the customer. And a lot of money got deposited in [bank], [bank], [bank], [bank] everywhere. So they entirely misuse the product. And by

> the time we found out, now that program is stopped, so our entire work that we did to build this product is gone now because they had to stop it. So that's how they actually completely shifted that process for us. (Interviewee #LX4K-Z3DK)

The example shared by Interviewee #LX4K-Z3DK illustrates how (mis)user-driven innovations can generate affective intensities that travel through a financial institution's technologies, policies, and strategic orientations. The unsecured loan cyberattack produced an immediate affective response—an institutional sense of urgency, anxiety, and vigilance—that compelled reconfiguration of detection, investigation, and recovery practices. Through these affective encounters between human and non-human elements, involving fraud teams, digital infrastructures, algorithms, and policy instruments, the assemblage was reorganized. Ultimately, the institution suspended the unsecured loan program to mitigate ongoing exploitation.

The decision to suspend the project was not solely a technical or managerial adjustment but an affective re-alignment, where the force of intrusion and the institutional drive for stability co-produced a new configuration of the cyber financial crime assemblage. Assemblages are affective in the sense that they enable movements, allowing relations to stretch, contract, or mutate in response to intensities that pass through them.

Deleuze's threefold ontology of event, virtual, and actual clarifies how such movements unfold (Deleuze & Guattari, 1987). For Deleuze, the virtual comprises a field of capacities and potentials; when a new, affective force enters the assemblage, these virtual tendencies become activated. The virtual then generates new actualities. Through lines of flight, virtual potentials that lie outside the apparently unified object are drawn into its interior, transforming its coherence and reconfiguring its trajectory (Deleuze & Guattari, 1987). In this way, the intrusion

does not simply interrupt the project; it creates an opening through which new organizational behaviours, risk sensitivities, and institutional priorities emerge.

Grove and Pugh demonstrate a similar dynamic in participatory development, where affectivity provides the force that enables communities to resist purely top-down structures (Grove & Pugh, 2015). They argue that biopolitics is not only imposed through fixed governance infrastructure but is actively shaped through affective participation. For example, workshops, meetings, and local negotiations generate intensities that can redirect development trajectories by amplifying certain voices.

These insights travel productively into the cyber financial crime context, as fraud management processes are similarly shaped by affective participation. Customer complaints, fraud investigation, financial losses, accounting reports, internal meetings, cross-departmental escalations, and stakeholder consultations become affective sites where institutional anxieties, professional judgments, regulatory pressures, and technological uncertainties circulate.

Rather than stabilizing the assemblage, these affective moments can reorient it, producing shifts in investigative priorities, recalibrations of risk thresholds, or even the suspension of a digital initiative. In both fields, affectivity is not secondary to decision-making; it is the relational force through which institutional actors transform the assemblage's ongoing movement.

(Mis)user-driven Innovation: Email Money Transfer Limit

In cases of (mis)user-driven innovation, it is often challenging to balance technological advancement, customer experience, and the risks of cyber financial crime. The following example demonstrates how exploitations within the cyber financial crime assemblage carry affective urges to intrude upon and reconfigure new products, strategies, and policies designed to enhance financial services. Interviewee #76MW-WT9E shared that during the COVID-19

pandemic, several Canadian financial institutions increased transaction limits for email money transfers to enable customers to complete higher-value self-serve transactions without visiting branches. This initiative reflected the institutions' shared desire to simplify banking processes and improve customer convenience. Yet this same desire also produced new affective openings—points of intensity and vulnerability—through which malicious actors could exploit the expanded transactional capacities and reconfigure the assemblage in unanticipated ways.

> I've noticed where clients want certain features, or ease of access for certain features, whether it's sending email money transfers […], adding a new, higher limit for EMT. I know with COVID, some big banks are sending virtual cards. Clients wanted to sign up and didn't want to go out into the branch. So having that ease of access for time sometimes needs impact on the fraud side because there's less checks and security checks on those pieces of assets. (Interviewee #76MW-WT9E)

Convenience and customer preference are not always without cost. Interviewee #2YNV-3L4Y explains that many customers expressed a desire for higher email money transfer limits, allowing them to send larger sums through digital banking platforms. However, this preference placed financial institutions in a complex position: responding to customers' affective desire for convenience and autonomy simultaneously exposed new vulnerabilities within the system. If a customer's credentials were to be compromised, the financial institution may need to face financial losses. In this sense, the drive for convenience—an affective force shaping both user demand and institutional innovation—becomes entangled with the assemblage's potential for exploitation and transformation.

> EMT […] limits because people always want to send more. And then obviously, it's the pros and the cons. Okay, you send more than potentially the bank is opening up itself to greater liability. If something goes wrong […] if it falls within the terms and agreements then the bank is possibly liable to. (Interviewee #2YNV-3L4Y)

The quote from Interviewee #2YNV-3L4Y illustrates how different components within the cyber financial crime assemblage are affective and continually affected by one another. Cyber financial crime assemblages are in constant flux as new desires, needs, and innovations enter and reconfigure them. Technological developments intended to enhance customer experience can simultaneously generate new sites of vulnerability, enabling (mis)users to appropriate technologies and policies in unintended ways and produce unforeseen consequences. Non-human elements such as technologies, objects, data infrastructures, and even statements, ideas, and regulatory logics possess the capacity to act, affecting and being affected by the assemblage's dynamics. In credential and identity compromise, (mis)users intentionally target victims' credentials, identity information, or system access points for financial gain. Rather than existing in isolation, human and non-human elements coexist within a dynamic and interdependent field, where their relations continually constitute the assemblage's formation and transformation. As Interviewee #T35Y-LX3F remarked, users who embrace new technologies and desire the convenience they offer must also be prepared to encounter the accompanying risks and challenges:

> I think technology advancement is very important. But I definitely think with the technology or technology advancement, there's always higher risk that's associated with it, right? We see these advancements are put in place to essentially make our lives easier, kind of help us out. But then, I mean, with the things I guess, made more convenient and easier for us, it also introduces more risk or higher risks.
>
> I feel like certain technology advancements shouldn't really be pushed for everyone necessarily. There are still you know, the smallest population of people who prefer to do things more manually in terms of you know, maybe stepping into a branch and actually speaking to someone about activity, there should be the option and if there are, which, in most cases there is, people prefer the more technological aspect of, you know, the convenience. They need to be ready to accept the risks that come with it, and also just be able to educate themselves. […] So I think with technology for those who are ready to, I guess, accept that type of convenience, they also need to be ready to kind of educate themselves as well. (Interviewee #T35Y-LX3F)

Interviewee #T35Y-LX3F's observation demonstrates that users exhibit varying degrees of desire to engage with digital banking services and technologies. Humans within assemblages are not merely agents of influence; they are also shaped by the network of relations they form with other elements. Intentions and interests, as Mol suggests, mediate how users enact technologies and make decisions within these relational configurations (Mol, 2010). Consequently, Canadian financial institutions may face greater challenges in mobilizing customers who display lower levels of interest or confidence in digital financial services.

Financial institutions continuously evolve their customer strategies, digital products, and financial solutions to retain clients and meet evolving banking needs. Greater convenience, faster

responsiveness, streamlined interactions, and increased digitalization have become dominant themes in financial product development among Canadian institutions in recent years. These digital products and services embody a desire to enhance customer experience and expand sales potential. Yet, technological and policy transformations also reshape the terrain of cyber financial crime and affect the operations of fraud management departments. Each time a new digital solution is integrated into online or mobile banking platforms, it reconfigures the assemblage by introducing new affective relations and potential vulnerabilities.

Financial institutions' fraud prevention strategies and detection mechanisms are continually affected by the forces of exploitation and must adapt by evolving their response strategies, whether through building more robust controls, recalibrating customer authentication processes, or even discontinuing new products that have become (mis)user-driven innovations. What is designed as convenience or innovation for users simultaneously opens new points of intensity where exploitation may occur, revealing how every technological advancement carries the potential to be both productive and disruptive.

These ongoing adjustments are not purely procedural or technical but affective in nature. They embody the tensions, desires, and anxieties that circulate between institutions, users, and technologies, forces that animate the cyber financial crime assemblage and give it its capacity for continual transformation. In this sense, innovation and exploitation coexist as interdependent affects, shaping how the assemblage evolves, reorganizes, and sustains its dynamic equilibrium. For Deleuze, affectivity is a productive force: every element holds the capacity to affect and be affected, generating continuous movement rather than stable form (Deleuze & Guattari, 1987). Seeing the cyber financial crime assemblage through affectivity reveals how fear, trust, and

desire circulate across its heterogeneous elements and how these circulations shape the shifting movements of power, value, and legitimacy.

7.3 The Desire to Capture: Platforms, Logics, and Decisions

Deleuze sees affect as a dynamic of desire that actively shapes meaning and relations, generating intensity and movement. According to Parr, this movement produces varied effects—sensorial, abstract, physical, and temporal (Parr, 2010). Affect is neither given nor passive; it is continually autonomous and productive. The concept of affectivity is powerful in STS because it draws attention to the pre-personal and pre-representational forces that move through sociotechnical systems before they become articulated as products, policies, or classifications (Barrett, 2013; Buser, 2014). In this section, I examine how platforms, algorithmic logics, and investigation decisions are enacted. The movements of these elements are not merely technical or procedural; they emerge from shifting intensities and tendencies that shape how actions are taken, how risks are assessed, and how fraud is captured.

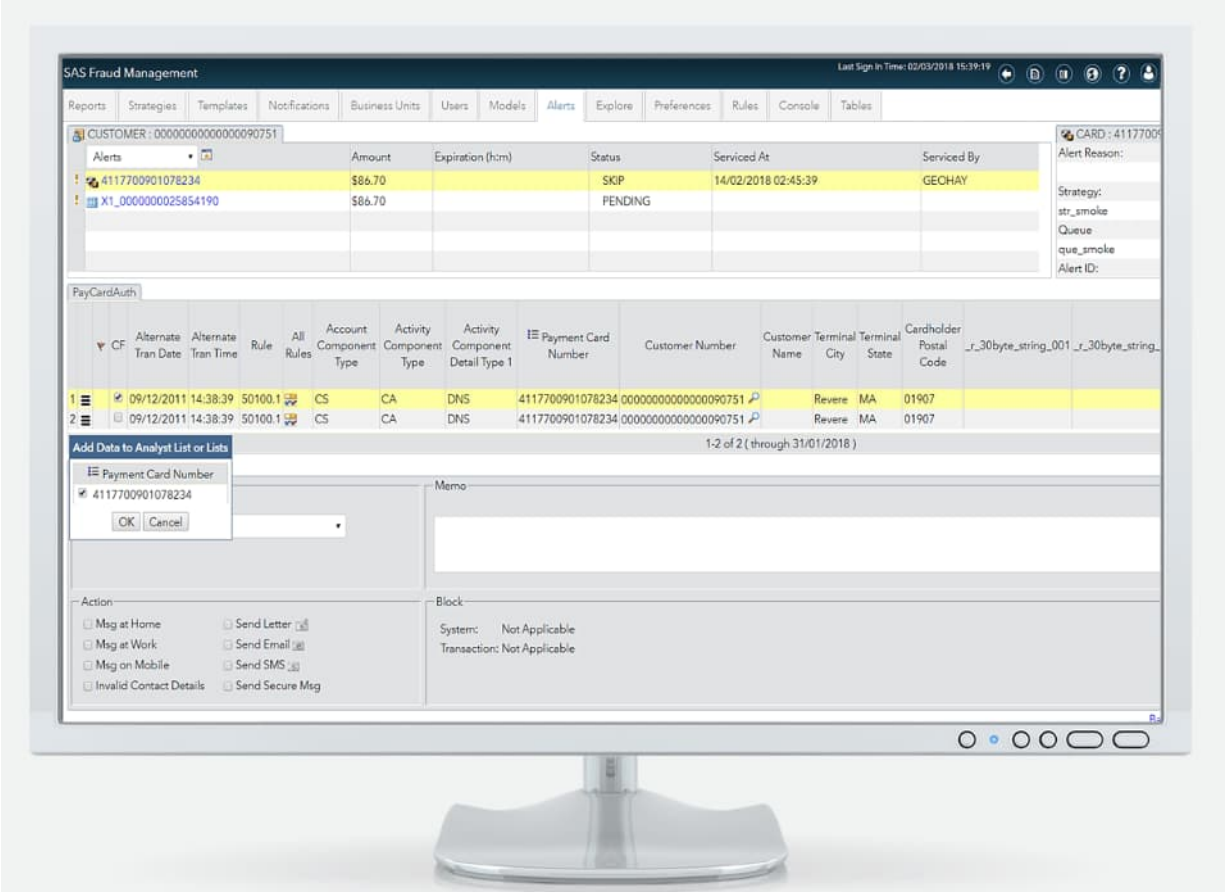
The Detection Analytics

Investigation starts with detecting suspicious activities. Suspicious activities and high-risk transactions may be discovered by fraud detection algorithms embedded in financial institutions' information systems. According to the Association of Certified Fraud Examiners (ACFE), continuous monitoring of real-time transactions and proactive data analysis proves to be one of the most effective controls for fraud (Association of Certified Fraud Examiners, 2014). There are multiple Predictive Analytics Technologies (PAT) vendors offering real-time fraud detection solutions in Canada. According to Hafiz et al., popular PAT vendors include Falcon

Fraud Manager by Fair Isaac Corporation (FICO), IBM SPSS Modeler, SAS Fraud Management, Cyber Source Decision Manager, and ACI Proactive Risk Manager (Hafiz et al., 2016).

PAT solution vendors provide services and platforms that allow for detecting cyber financial crime in real time and prevent fraud losses at the onset of cyber financial crime (Maruatona et al., 2012). Typically, PAT platforms indicate consumers' profile information, including their names, addresses, date of birth, account numbers, and recent transactions or activities (Figure 8). PAT platforms will also show the alerted transactions (usually highlighted in the interface) and indicate the nature of the transaction as well as the possible reasons behind the alert triggers.

Figure 8. Sample Cyber Financial Crime Investigation Platform: SAS Fraud Management



Note. From "How to Choose Fraud Detection Software: Features, Characteristics, Key Providers," by AltexSoft, 2018. https://www.altexsoft.com/blog/business/how-to-choose-fraud-detection-software-features-characteristics-key-providers/

PAT platforms usually manage suspected fraud cases at the account level, meaning each alerted case is dedicated to one consumer's profile, rather than having multiple consumers reviewed at the same time. One interviewee makes a similar observation on PAT's functionalities:

> The analytics team basically looks into the trends and tries to develop more automation, automated tools, rules, which you know, can block certain kind of transactions…which are basically falling into the pattern […] something which has already been confirmed as fraud. (Interviewee #R5PL-5ST9)

Cases are alerted in PAT platforms because the cases are deemed high risk, as determined by fraud detection algorithms. PAT solution vendors work with financial institutions to design different fraud detection algorithms through predictive analytics processes (Hafiz et al., 2016). Hafiz et al. explain that predictive analytics processes answer questions like "What will happen" and usually involve five analytical processes: business problem definition, data acquisition and preparation, data analysis and model development, predictive model deployment, and monitoring model performance (Hafiz et al., 2016, p.1).

In the context of cyber financial crime, most transaction data are produced by consumers themselves as they conduct banking activities. Real-time transactions are accumulated on a user's account, and the account level information is used to detect suspicious banking patterns. Financial institutions typically work with technology vendors to store and manage real-time

transaction data. This procedure illustrates the first two critical processes: business problem definition and data acquisition and preparation.

The third process, data analysis and model development techniques, however, varies distinctively team by team and bank by bank. Every bank, every analytics team, and even every analyst uses different statistical models to manage their fraud detection portfolios. When exploitation occurs, Canadian financial institutions are simultaneously affected and activated, generating incentives to develop new risk management technologies, strategies, and policies in response.

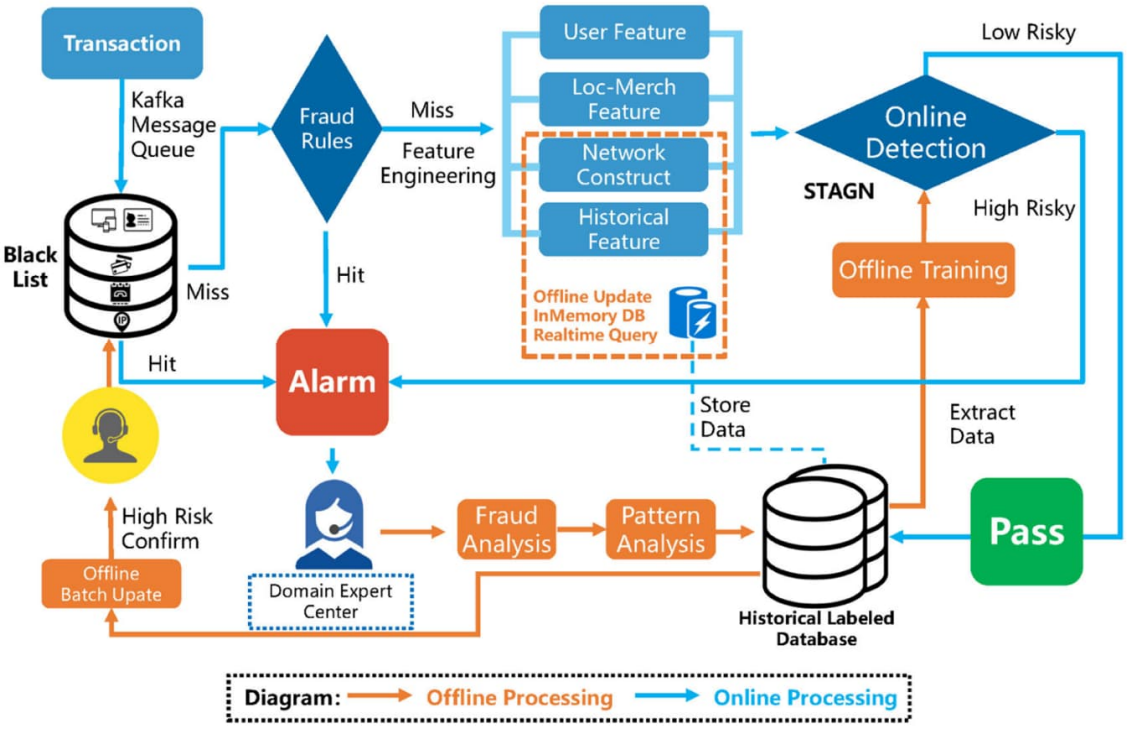
> What I do first thing in the morning, what I do, first thing when I wake up, I will run the script, see the false positive ratio, see the merchant ID, and I run my macro […] then to see the fraud trend, I will use [a fraud detection software] to see what's going on there and determine what needs to be acted on. (Interviewee #BAWZ-SXX7)

Interviewee #BAWZ-SXX7 is a strategist responsible for developing computational algorithms that detect suspicious transactions. Strategists and analysts in fraud analytics teams work with a continuum of tools, from statistical models to machine-learning techniques, to surface anomalies and shifting patterns of exploitation. When real-time transactions appear in customers' accounts, platforms display the activity while algorithms run live in the background, scanning for criteria that may constitute a red flag according to fraud detection specifications and rule logics. The fraud strategist evaluates these outputs, assesses whether the decision aligns with institutional guidelines, and sequentially deploys additional logics to capture emerging suspicious behaviours. This field of play is a field of becoming, enacting what Deleuze and Guattari describe as a force field of emergence in which affect arises through encounters and circulates across the assemblage (Deleuze & Guattari, 1987). In this dynamic interplay, human

and non-human elements affect and are affected: platforms sense variation, algorithms modulate thresholds, strategists interpret intensities, and institutional guidelines shift in response. Together they constitute an affective assemblage in which detection is not simply procedural but continually reconfigured through the relations and forces that move across it.

Through these affective modulations, technologies not only enact detection but continually reconfigure how the assemblage becomes alert to exploitation. Fraud-detection algorithms rely on a data feedback loop built from confirmed fraud events: fraud detection→blacklist→alerts if another profile transaction triggers blacklist (Cheng et al., 2020). Other factors such as consumer patterns, transaction and merchant location, consumer address, and historical features are all indicators to be processed through modeling such as decision trees, regression, neural networks, and boosting in order to determine the legitimacy of the transaction (Cheng et al., 2020; Domashova & Zabelina, 2021). Figure 9 presents an example of an online and real-time fraud detection system.

Figure 9. Determining Transaction Legitimacy through Fraud Analytics



Note. From "Graph Neural Network for Fraud Detection via Spatial-Temporal Attention" by Cheng et al., 2020, *IEEE Transactions on Knowledge and Data Engineering*. Copyright 2019 by IEEE Transactions on Knowledge and Data Engineering.

Logics and Decisions

A data feedback loop helps with the accuracy of the predictive model, and through reinforced learning, the performance of the predictive model can be improved. Accurate capture of fraud is crucial in the fraud detection industry because blocking a legitimate transaction can create consumer inconvenience and frustration. For example, according to MasterCard spokesman Bernhard Mors, up to 80% of declined transactions in 2015 were in fact legitimate when credit card holders travelled abroad (Queen, 2015, as cited in Hafiz et al., 2016).

If the transaction was legitimate, the fraud algorithm then over-blocked a legitimate transaction; if the transaction was fraudulent but the fraud algorithm failed to detect it, then the fraud algorithm missed a fraud incident.

Industry practitioners often use the terms false positive and false negative to describe the accuracy of algorithms. A false positive alert is an incorrect decline of a legitimate transaction, whereas a false negative alert can result in the false acceptance of a fraudulent transaction (Hafiz et al., 2016). According to Interviewee #LRPS-55Y3, balancing between overblock and fraud miss is critical in the fraud business because of customer experience:

> So, the easiest thing for agents would be if they could just block everything because that means that we wouldn't have any risks. But I think [about] the importance of a good balance between overblock and fraud miss. At the end of the day, we are a financial institution. So we do have to think about the customer's journey in the sense that it impacts other things again.
>
> Foot traffic to branches, customers were called into other call centres. So as much as it would be easy to block everything, we do want to encourage that agents do their due diligence to investigate properly to minimize that negative impact. Not just to customers but to their partners as well. (Interviewee #LRPS-55Y3)

Interviewee #LRPS-55Y3 illustrates a difficult decision that financial institutions routinely face. Overblocking all suspicious transactions introduces heavy branch traffic and surges in call-centre volume. For lower-dollar transactions, even when they appear suspicious, the fraud-detection logics may allow them to proceed while continuing to monitor for emerging patterns of exploitation. As the interviewee explains, the institutional costs of negatively affecting customers may be too high when the potential loss is minor. If an institution blocks an

account too frequently simply to prevent a possible fraud, customers are forced to repeatedly visit branches, verify their identity, or re-authenticate their accounts, generating frustration and eroding trust.

Seen through affectivity, this balancing act is shaped not by purely rational assessments but by circulating intensities such as risk sensitivity, institutional tolerance, customer frustration, reputational anxiety, and anticipated operational burdens. These pre-cognitive and pre-representational forces modulate how blocking thresholds are set, how exceptions are made, and how the assemblage senses when to intervene or hold back. Deleuze argues that affect exists prior to conscious thought, interpretation, or meaning-making, and before language, symbolization, or conceptual framing (Deleuze & Guattari, 1987). This means affectivity is not a psychological state, does not hold opinions, does not convey meaning, is not fixed or containable, and does not operate within any moral register. Rather than expressing emotion or intention, affect is a capacity—a force that modulates tendencies and possibilities as they emerge (DeLanda, 2006). It circulates across technologies, infrastructures, and human–non-human relations, distributing the conditions through which actions are sensed, responses are triggered, and assemblages shift.

Moving through detection platforms, financial institution representatives, policy guidelines, and institutional practices, these affective forces shape when an institution hesitates, when it intervenes, and how it interprets the “felt weight” of low-value risk or high-risk activities. Although algorithmic logics are designed to identify fraud, the desires and intensities circulating within the assemblage do not carry predetermined value. They constitute a force of becoming, one open to possibilities, contingencies, and unpredictabilities. Every transaction is singular, while the dollar amount differs, the customer profile differs, and the transaction pattern

differs. Nothing can be pre-labelled or neatly pre-boxed. The affective force of decision-making moves through these desires and uncertainties, continually balancing operational demands, risk sensitivities, and institutional comfort as the cyber financial assemblage configures and reconfigures itself in practice. In this sense, the decision to interrupt or permit a suspicious transaction becomes an affective negotiation, where shifting comfort levels, fraud-loss tolerance, and expectations of customer reaction collectively recalibrate institutional responses within the cyber financial assemblage.

Behavioural analytics is another newer technological approach to understand consumer patterns and detect fraud. Behavioural analytics refers to tracking technology users' behavioural data and using machine learning to understand and anticipate predictable patterns at a granular level (Chargeback Gurus, 2021d; Horan, 2018). Behavioural analytics allows algorithms to be triggered if the digital behavioural pattern does not necessarily align with a user's typical pattern. For example, if the consumer usually transfers money from a savings account to pay bills, but suddenly the consumer is transferring money from a credit card account to pay a new bill payee, the transaction pattern may be listed as suspicious. If the financial institution uses an accelerometer, consumers' tap gestures (light and steady versus strong and shaky) can be used as an indicator to determine if the consumer is under distress (Ma et al., 2022). Behavioural profiles are constantly updated with each new transaction and individual behaviour. Figure 10 presents a sample of profile category maintenance techniques that are critical for establishing an effective fraud detection algorithm.

Figure 10. Maintaining Behavioural Profiles for Accurate Fraud Detection

Transaction profiles	Behavioral Machine Learning profiles for each consumer's financial and non-financial activity. Updated in real-time with each transaction, across all channels.
Collaborative profiles	Improves risk sensitivity by identifying behaviors that differ from typical behaviors within individuals' peer groups.
Behavior sorted lists	Deep learning behavioral analytics that identify and rank recurrent activities that are unique to each individual, such as favorite merchants, ATMs or destination accounts, in order to significantly reduce false positives.
Merchant profiles	Aggregated transactions at merchant-level to form behavioral metrics for a more comprehensive view of risk.
Multi-layered self-calibrating profiles	Detects behavioral outliers in real time even with limited or no data to train the model and automatically adjusts to accommodate new behavioral patterns. Advanced instances use deep learning to further improve pattern recognition.
User-defined profiles	Flexible, custom-defined profiles for entities such as devices or IP addresses.
Global intelligent profiles	Real-time adaptive risk ranking to monitor and respond to the riskiest profiles for improved fraud assessment.

Note. From "Fraud Detection: Applying Behavioral Analytics," by T. J. Horan, 2018, *FICO Decisions Blog*. https://www.fico.com/blogs/fraud-detection-applying-behavioural-analytics

In most financial institutions, fraud departments have dedicated analytics teams equipped with fraud analysts and fraud strategists who create rules to alert on suspicious activities. Production rules—or business rules management systems—can be well-illustrated with the phrase "If Condition then Action." Production rules models usually involve pairs of conditions and corresponding actions (Ma et al., 2022). Data analysts working at financial institutions can design dynamic fraud detection algorithms that can be integrated with production rules, including device monitoring, biometrics evaluation, and behavioural pattern analytics. For example, when device ID is inconsistent with historical records, remote access is detected, or

when session length is longer than normal, rules can be triggered to prompt next step actions (Ma et al., 2022).

As Interviewee #YKLR-V6US explains, algorithms and strategies are never purely technical; they are shaped by affective forces circulating within the assemblage. Risk sensitivity, institutional tolerance, regulatory pressure, and the anticipation of customer impact all modulate how models are calibrated, how thresholds are set, and how detection logics evolve. As a result, fraud-analytics work is both computational and affective, emerging from the interplay of data, technological capacities, and the intensities that guide institutional judgment:

> You know, [fraud analytics can do these analysis] does this person normally deposit big checks, or do they normally send out big transfers people they've never met before? Oh, they don't. Okay, well, then let's not let that happen without doing something (such as fraud review) right. (Interviewee #YKLR-V6US)

Interviewee #YKLR-V6US describes how creators of technological artifacts inscribe particular desires, goals, and orientations into the systems they build. In detection work, these inscriptions shape how technologies sense and respond to exploitation within the cyber financial crime assemblage. By mobilizing algorithmic thresholds, pattern-recognition models, and rule-based logics, non-human actors participate directly in capturing exploitation—with desire, with energy, and with a force of becoming (Massumi, 2021). This process is also inherently affective: the capacities embedded in these technologies, in other words, what they are designed to notice, tolerate, or escalate, are shaped by circulating intensities such as institutional risk appetite, anticipated customer response, and shifting regulatory pressure. Massumi describes Deleuze's notion of affectivity as webbed in relations, emphasizing that affect cannot be possessed but unfolds between bodies (Massumi, 2021). Relational affectivity is a movement within the

assemblage, not a static linkage. This means that platforms, detection logics, and institutional decisions are enacted simultaneously through shifting intensities, generating endless possibilities as the assemblage senses, interprets, and responds to exploitation in real time (Massumi, 2021).

Digital banking is filled with major data challenges, including boundary-less digital payments, real-time consumer engagement, innovative transformational platforms, continuous digital banking services, ongoing human–machine collaborations, and so on (Prosa Mx, 2021). According to a presentation by one of the leading PAT platforms, to better balance consumer experiences, credit risks, compliance and regulatory requirements, insider risks, and the occurrences of financial crime, contextual intelligence can be a viable approach (see Figure 11) (Prosa Mx, 2021).

Figure 11. Convergence of Fraud Detection Algorithms



Note. From “Fraud Detection Algorithms: Contextual Profiling and Orchestration” [Video], by Prosa Mx, 2021, *YouTube.*

https://www.youtube.com/watch?v=Ys7yrIzg2t4&ab_channel=ProsaMx

In this convergence of fraud detection algorithms, it is illustrated that validating a profile in a contextual setting can be helpful in accurately detecting fraud. For example, using verification strategies to validate consumer identity, confirming identity documentation and biometrics enrolment, assessing the consistency of the consumer's existing and new devices, evaluating application fraud risk, adopting enhanced authentication methods, ensuring regulatory requirements are met, continuously monitoring transaction history, and using network scoring to organize the consumer's behavioural patterns—all of these can be productive in fraud detection and in generating alerts when anomalies are detected.

When alerts are triggered, there are typically four possible outcomes (CIBC, n.d.-b; RBC, n.d.; TD Bank, n.d.-b):

1. Block and Review: In this situation, the transaction is temporarily blocked due to suspected fraud. If determined to be a false positive alert upon investigation, the case will be released, and the transaction will be put through.
2. Decline and Review: In this situation, the alerted transaction is declined due to high risk. If determined upon investigation to be a false positive, the case will be released, and the transaction will be required to be re-initiated by consumers.
3. Pending and Review: In this situation, the transaction causes an alert but there is no blocking or declining action. The transaction remains pending for investigation. Typically, these types of transactions have a service window time—for example, some bill payments may take several business days to complete the transaction, or some money transfer services may take a few hours to a few days. If determined upon investigation to be a false positive alert, the case will be released, and the transaction will be put through without any additional action required.

4. Alert and Review: In this situation, the transaction causes an alert due to suspicious activities, but transactions are typically completed by the time of the alert. These cases will be further investigated to determine risk. If determined to be a false positive alert upon investigation, the case will be closed; if the activity is suspicious, the account may be suspended to prevent further losses.

The four possible outcomes triggered after an alert illustrate how fraud-detection mechanisms embedded within Canadian financial institutions mobilize both human and non-human elements toward the shared desire to capture suspicious activity. Just as Deleuze described affect as "verbs becoming events—naming affects as perceivable forces, actions, and activities" (Parr, 2010, p. 13), these detection and capture processes signal the assemblage's active transformations. Each outcome is an event in which platforms, algorithms, analysts, and institutional guidelines collectively affect and are affected, continually shifting how the assemblage senses, interprets, and responds to exploitation.

(Mis)user-Driven Innovation: Artificial Intelligence

The desire to capture is not a static field; its affectivity continually reshapes the energies and intensities circulating within the assemblage as forms of cyber financial crime evolve. As exploitation techniques shift, the convergence of fraud detection mechanisms responds by reconfiguring its capacities, effectively adapting thresholds, recalibrating models, and generating new modes of sensing. This adaptive movement reflects an affective responsiveness where the assemblage is compelled to innovate in order to meet emerging threats. Recently, this has included the growing use of artificial intelligence to detect and counter increasingly sophisticated patterns of fraud, demonstrating how affective forces propel the assemblage toward continual (mis)user-driven innovation.

Based on my qualitative data, industry practitioners tend to have positive sentiments towards using technologies to detect the suspicious activities. For instance, Interviewee #3NGU-8XTJ recommends using artificial intelligence to locate fraud patterns:

> I strongly recommend getting […] artificial intelligence, you know, some sort of system robotics to pretty much interpret patterns and you know, create rules, strategies to you know, predict and mimic fraud patterns and prevent them from happening. So, investment in automation, artificial intelligence strategies would be one of the best ways to improve the ecosystem, and huge in physical asset point of view education, keeping teams updated on new fraud trends, what's happening across the world, not just in the bank. (Interviewee #3NGU-8XTJ)

As per Interviewee #3NGU-8XTJ, using Artificial Intelligence (AI) to detect high-risk patterns allows the automation of fraud pattern detection. Without human intervention, the non-human actor (the AI-empowered detection system) has the desire to detect and stop fraud. Because of the machine learning processes embedded within, the system can automatically self-learn the newest fraud trend and therefore be productive in addressing the risks stemming from the risky activities.

Callon explains how when scientific and technological initiatives become integrated into society, there are four moments embedded in the translation process: problematization, interessement, enrolment, and mobilization (Callon, 1998). Callon describes the process of stabilizing scallop population in St. Brieuc Bay, France, using the translation process. Researchers identified the problem of the declining scallop populations and worked with local fishermen to ensure the competing interests of this project were minimized. Upon securing commitments, researchers then worked with fishermen and changed their fishing practices.

Finally, the process of mobilization ensured all actors, including non-human ones like the scallops, actively participated and fulfilled their roles, effectively stabilizing the population as planned. This example highlights the negotiated and interconnected nature of scientific and environmental management efforts, illustrating how human and non-human actors collaboratively contribute to ecological interventions.

The four moments embedded in Callon's translation process can also be used to analyze the (mis)user-driven innovations emerging around the adoption of AI within the cyber financial crime assemblage. Drawing on Callon's model of scientific and technological initiative translation, I examine how Canadian financial institutions can productively integrate AI as a response strategy to new fraud trends (Callon, 1998). This analysis is informed by my own professional experience in developing strategies and policies to address emerging forms of misuse.

The first moment, problematization, involves identifying a pressing issue within the shifting landscape of cyber financial crime and determining which entities—the fraud strategists, the fraud-management technologies, and the organizational infrastructures—are positioned to address it. Problematization typically arises when institutions detect new fraud patterns or observe measurable losses associated with emerging misuse.

The second moment, interessement, centres on constructing the alliances required to address the problem while displacing competing priorities that may divert resources. At this stage, securing funding and internal support becomes critical. Within Canadian financial institutions, this includes acquiring investment for research and development, building AI infrastructure, recruiting technical expertise, and establishing procedural frameworks that enable AI deployment within regulated environments.

The third moment, enrolment, involves further negotiation and stabilization of roles among human and non-human actors. In this phase, responsibilities and expectations become explicitly defined. Within the financial institutions, strategists, operations teams, IT developers, audit and compliance units, and supporting departments such as finance, accounting, and administration all engage in negotiation to ensure the AI initiative can be enacted in practice. Technologies themselves—algorithms, detection engines, data pipelines—are enrolled as actors that must align with institutional requirements and regulatory constraints.

The final moment, mobilization, ensures that the actors designated to speak and act on behalf of broader groups effectively represent them. Successful mobilization aligns heterogeneous interests into a coherent project that can adapt, scale, and respond as intended. In the context of AI adoption, mobilization ensures that fraud management strategies, technological capacities, and organizational practices move collectively toward reducing exploitation. Through this sequence, AI becomes not only a technical solution but an affective and relational innovation. Its adoption is shaped by circulating intensities such as risk appetite, institutional anticipation of future attack vectors, regulatory pressure, and organizational desire for operational efficiency, illustrating how (mis)user-driven innovation unfolds as both a technological and affective transformation within the cyber financial assemblage.

To summarize, the desire to capture functions as an affective field within the cyber financial crime assemblage. Human and non-human actors generate intensities that continually reconfigure detection logics, institutional practices, and technological capacities. These elements affect and are affected by shifting forms of misuse, producing an environment where responses emerge through ongoing encounters rather than predetermined plans. In this movement, (mis)user-driven innovation becomes central: fraudsters' creative exploitations force institutions

to recalibrate models, adjust thresholds, and redesign rule engines, while institutions repurpose tools and adopt emerging technologies such as AI to sense and counter new threats. These processes are affective because they operate through circulating pressures such as loss events, customer harm, reputational risk, operational strain, and regulatory expectations which modulate how technological decisions are made and how innovations become possible. The adoption of AI as a (mis)user-driven innovation, for example, depends on institutional appetite, resource availability, and tolerance for uncertainty, demonstrating how affect shapes the direction and feasibility of technological development. The cyber financial crime assemblage is therefore not static but continually shifting, shaped by affective forces that compel adaptation, improvisation, and reinvention. The desire to capture moves through these dynamics, remaking how the assemblage becomes alert, responsive, and able to act in the face of evolving patterns of exploitation.

7.4 The Drive to Settle: Automated Processes for Investigation and Reimbursement

Detection of suspicious activity is usually only the first step in the fraud management process. As cyber financial crime grows more complex, investigations must account for multiple components, including loss assessment and reimbursement. For customers, the priority is understanding what happened and receiving appropriate compensation. In Canada, not all cases are adjudicated by humans; many are investigated and reimbursed through automated systems that evaluate loss, apply rules, and issue credits. This section illustrates how technologies and automated processes shape investigation and settlement by reimbursing customers efficiently while mediating institutional risk. These automated processes are also affective: they shape the

composition of the cyber financial crime assemblage and are themselves reshaped by shifting fraud patterns, operational pressures, institutional risk sensitivities, and the movements of human and non-human actors.

The drive to settle activates what Deleuze describes as a productive force—an ongoing generation of new configurations, capacities, and relations rather than a fixed or final structure (Deleuze & Guattari, 1987). Social assemblages possess their own objective existence and causal capacities, shaping both the components within them and those around them, each at their own pace and scale (DeLanda, 2006). Automated processes are not isolated procedures that simply move cases through computational codes; rather, they are affective components situated within the assemblage, enacting relations and interpreting different versions of reality. Through these enactments, they generate decisions that ultimately shape how financial institutions respond to threats, claims, and customer complaints within the cyber financial crime assemblage.

Automating Investigation

I first discuss the automated investigation processes in the cyber financial crime assemblage. As mentioned above, when an alert is triggered, the system typically produces one of four outcomes: (1) block and review, (2) decline and review, (3) pending and review, or (4) alert and review. Although these decisions provide an initial assessment, confirming legitimacy ultimately requires financial institution representatives to contact customers directly. To understand what happens after a cyber financial crime occurs and how investigation and settlement proceed, I asked interview participants to describe the sequence of actions that typically follow and how cases move through the institutional processes of verification, loss assessment, and reimbursement:

> I work… as an analyst for the claims [department] where we handle digital, in-branch [impersonation] and phone channel claims where the customer has confirmed fraud, or was a victim of scam. And we kind of analyze those things and decide if this claim has to be paid or not. (Interviewee #Undisclosed)
>
> The second option is to report… online fraud, alerting on suspicious unauthorized account activities, which is the fraud claim. (Interviewee #3NGU-8XTJ)

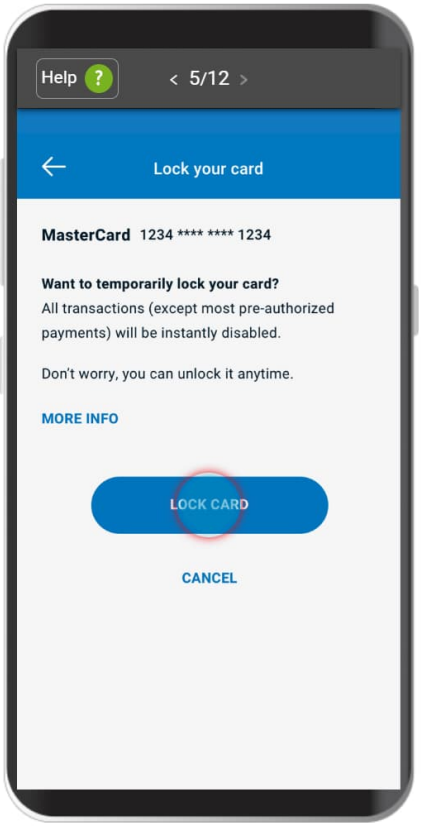
Canadian financial institutions rely on automated processes to support fraud investigations by using technologies that initiate verification and gather customer input. Institutions may send text messages requesting confirmation of recent transactions, allowing customers to reply directly to validate or report them as fraudulent. Automated phone calls from toll-free numbers may also ask customers to verify activity. In some cases, institutions email customers about suspicious transactions, prompting them to contact the bank for further review (CIBC, n.d.-a; RBC, n.d.; TD Bank, n.d.-a).

Some financial institutions also have mobile banking application push notification options available. In the event of an unexpected withdrawal or deposit, the mobile banking application can send a push notification to the consumer advising them of the unusual transactions (RBC, n.d.). Consumers can also configure their alert options, such as via push notification, email, and text message.

Technology-based investigation is cost-efficient because it removes the need for a human investigator to review every case. Once an alert is triggered, the process initiates automatically, and consumers can use digital channels to confirm or report the activity with minimal delay. Some institutions also allow customers to lock their cards temporarily through online or mobile

banking, providing an immediate layer of protection and reducing potential fraud losses before direct contact with the bank is established (see Figure 12).

Figure 12. Lock Card Function on Mobile Application



Note. A screenshot of a tutorial animation illustrating the lock card function on the mobile banking application. From "Lock/unlock your credit card," by BMO, (n.d.-a). https://bmodemos.com/en/course/start/public-lock-unlock-your-credit-card-mobile/emulator-lock-unlock-your-credit-card-mobile/emulator

> Technology could definitely make things more efficient. Definitely make things quicker and potentially cheaper and potentially, again, just overall more efficient. But that's not going to capture 100% of everything, that human interaction and that sort of human intervention, I should say, will definitely always be required in my eyes. Just given the fact that a machine is only as smart as you make it. (Interviewee #B7FQ-RANC)

In this statement, Interviewee #B7FQ-RANC mentions that the "machine is only as smart as you make it." Automated systems are programmed to follow predefined rules and processes, which might not always accommodate unusual or exceptional cases. This can result in investigation errors or operation oversights if the automation process is unable to adapt to unique scenarios that fall outside its configured parameters. Interviewee #CVN3-7UBK raises a similar concern related to this system failure:

> The downside [of automation] is that if a logic is broken, we're not talking about 25 agents, one made an error it's that one agent's [work] will be impacted. If that logic is broken, it's broken for every [investigation/adjudication] process under that same scenario, right? (Interviewee #CVN3-7UBK)

Although automating investigation can free operational capacity by handling simple, repetitive tasks while human agents focus on more complex cases, errors within automated systems can become self-replicating. When a mistake enters the workflow, the system reproduces it at scale, turning a single misjudgment into a patterned, repeated outcome. These disruptions show how automated investigations are not static tools but affective actors whose capacities to notice, respond, and protect are continually shaped—and reshaped—by the movements of human and non-human forces within the cyber financial crime assemblage.

Additionally, while technology-based investigation can be productive and improve consumer experience, it also introduces operational risks. If cybercriminals gain unauthorized access to a mobile banking application, they can alter fraud alert settings or lock and unlock cards. In cases of SIM-porting fraud, text-message verification becomes ineffective because alerts are rerouted to numbers controlled by the criminal. Likewise, if verification calls are redirected to fraudulent numbers and confirmed by the attacker, consumers lose visibility over the alerted activity. In these scenarios, the automated investigation fails, exposing the limits and vulnerabilities of technology-driven verification.

One challenge of using automated investigation, according to interview participants, is the absence of a "human touch." Automation may investigate a case and resolve a complaint efficiently, but customers may still feel uncertain or insufficiently supported after experiencing fraud. As Interviewee #AWXJ-54VW explains, consumers often need human interaction following an adjudication to feel reassured that their concerns have been properly acknowledged and addressed by the financial institution.

> I think automation is beneficial for reducing the amount of hours spent with certain activities within our business. But I think the human touch, maybe there's a department that is just customer appreciation or understanding, and they just say, hey, really sorry that this has happened. What we did is we reimburse you, as you can see from […]. Do you have any questions or any concerns going forward or is anything I can help you with? (Interviewee #AWXJ-54VW)

This need for human reassurance also reflects the affective dimensions of reimbursement. Automated systems operate through business rules and operation policies, but the experience of fraud generates intensities—anxiety, vulnerability, and the desire for recognition—that move

across customers, staff, and technologies. These forces are not emotions in a psychological sense but relational capacities through which bodies affect and are affected, activating what Deleuze and Guattari describe as a force of becoming (Deleuze & Guattari, 1987). When automation cannot absorb or respond to these intensities, human adjudicators enter the process to acknowledge harm, restore trust, and recalibrate the assemblage's relations. In this way, affectivity shapes reimbursement: customer uncertainty, institutional sensitivity to reputational risk, and the technological limits of automated systems all modulate when automation is sufficient and when human intervention becomes necessary. The assemblage responds not only to data and rules but to the relational movements of reassurance, credibility, and care that guide how cases are resolved and how the assemblage reassembles after disruption.

Interviewee #AWXJ-54VW further expands on the opportunity of contacting customers after fraud happened—they believe it is a good opportunity to restore the relationship and institutional trust. Interviewee #AWXJ-54VW suggests if rules and regulations permit, such human connection contact can turn into a sales opportunity, such as selling a line of credit or other bank products.

> And just that human touch because that human touch could potentially help mend fences a lot quicker, because we're either getting a visual person either through like a video call or an audio through a phone call. And that also could potentially be an opportunity to branch into other bank products could be a mortgage could be a line of credit for us buying a car for their son or daughter. It could be anything. I think that human touch it's going to be although we're getting to guess a community and a world of disconnection, and everybody's on their phone, and no one's really paying attention to anybody. When

you get that human connection it's gold. It's not even gold. It's platinum. (Interviewee #AWXJ-54VW)

Müller and Schurr's (2016) work further exemplifies how these affective dynamics operate by showing that assemblages are composed of both material and immaterial forces that are simultaneously productive. In their analysis of the surrogacy and reproductive industry, they argue that contractual arrangements, biological processes, legal infrastructures, and economic transactions intertwine with expectations, anxieties, hopes, and vulnerabilities. These heterogeneous elements do not simply coexist; they actively affect one another through relational intensities that generate new capacities and outcomes. Applying this insight to cyber financial crime reimbursement reveals that technological infrastructures, automated rules, customer interactions, and institutional guidelines are likewise animated by affective forces. Material components such as automation scripts, verification systems, and digital evidence intersect with immaterial currents like trust, uncertainty, institutional responsibility, and customer expectations. Together, they produce a field where reimbursement is not only a technical process but a productive process shaped by forces that transform the assemblage itself.

Automating Reimbursement

Next, I discuss automated reimbursement processes. The use of technology to reimburse claims is not unique to Canadian financial institutions; it is a widespread practice across multiple sectors. Medical insurance providers employ automated systems to assess and reimburse claims (Fathy & Donahue, 2016; Segal et al., 2002). Car insurance companies rely on automated claim evaluation tools to process payouts efficiently (Bader et al., 2018; Patil et al., 2017). Travel expense reimbursement systems similarly automate assessment and approval (Bartman-Gatt, 1990).

Some cyber financial crimes cannot be processed by automated systems because their complexity involves numerous interdependent human and non-human actors. These cases require human adjudicators who can interpret context, assess intent, and determine loss with nuance beyond what automated rules can capture. However, for simpler fraud claims, automated adjudication is both possible and efficient. Technology-based reimbursement can process straightforward cases quickly, increase overall productivity, and reduce long-term operational costs for financial institutions.

In recent years, extensive research has been done on automation processes in the banking industry (Madakam et al., 2019; Romao et al., 2019; Villar & Khan, 2021; Vishnu et al., 2017). The rising interest in automating business processes is mainly motivated by operational costs and by the goal of reducing manual administrative work. During the COVID-19 pandemic, the development of business automation processes in the banking industry was further developed.

The pandemic has affected business continuity plans in various ways. For industries that rely heavily on global employment outsourcing sectors, workforce capacity and capabilities worldwide have been significantly impacted by widespread lockdowns, particularly in China and India (Kajjumba et al., 2020). Employees requiring sick leave or taking unscheduled time off to care for ill family members have also taken a heavy toll on productivity (Kumar et al., 2020).

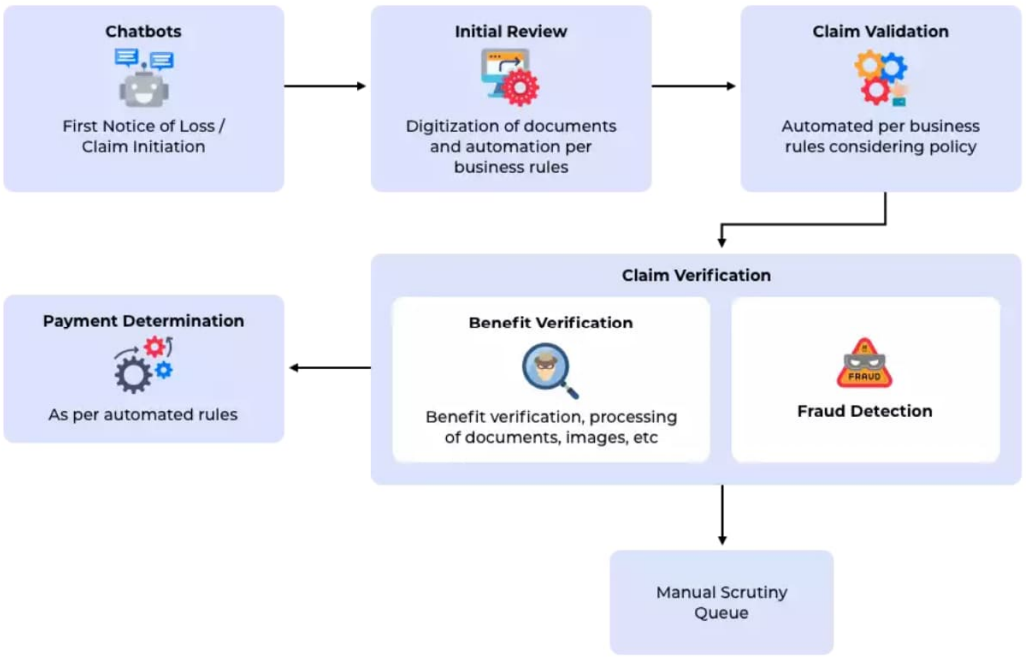
It is not surprising, then, that Robotic Process Automation (RPA) has been on the rise throughout the COVID-19 pandemic. RPA refers to a set of technologies which enable the automation of routine activities previously performed by humans (Madakam et al., 2019). The mechanism maximizes operational efficiency, improves workforce productivity, and maintains industry compliance. Use cases in the financial service industry include credit application

processing, fraud detection, fraud claims adjudication, and contact centre optimization (Romao et al., 2019; Villar & Khan, 2021).

As Madakam et al. explain, there are many other technologies working at the background level to ensure RPA can be incorporated into the business operation process seamlessly, including artificial intelligence, machine learning, deep learning, data analytics, and HR analytics (Madakam et al., 2019). RPA uses a computer, or what is sometimes called a virtualized Full-Time Equivalent (FTE) or a robot, rather than a person to manipulate existing application software. RPA can function in the same way that an employee in a regular business process executes a task.

Canadian financial institutions also use RPA in their technology-based adjudication processes. These systems process digitized documents, apply the institution's adjudication policies, and generate claims decisions according to the predefined rules and criteria (see Figure 13).

Figure 13. An Example of the Technology Adjudication Process



Note. From "Automated claims processing: Using RPA and machine learning to manage insurance claims," by M. Synytsia, 2021, *AltexSoft.* https://www.altexsoft.com/blog/automated-claims-processing/

When consumers submit fraud claims, technology-based adjudication may be triggered. Certain simple cases can be processed entirely by RPA, such as card-not-present credit card fraud or lost/stolen card incidents where contactless payments were misused. In these situations, RPA reviews business rules and institutional policies to make adjudication decisions quickly and consistently. The swift turnaround improves customer satisfaction by minimizing the waiting period for reimbursement:

> And the purpose of RPA is to ensure that we're always delivering on our customer expectations. Because we live in a world where we see sudden fraud attacks and all of that and customer has to wait for have to wait for their refunds because when they're entitled to it. (Interviewee #CVN3-7UBK)
>
> One of the […] key recommendations would be automation: simplifying the process and getting rid of a lot of hand and manual work […] fraud trends they always change […] humans are always looking at growing, so fraudsters will always think about different ways to fraud the bank. We need to keep on planning for future capacity and also […] the additional volumes to deal with. (Interviewee #3NGU-8XTJ)

The affective nature of reimbursement is also evident in how the system responds to RPA failure. When RPA cannot reach a decision based on available business rules, the case is automatically removed from automation and routed to human adjudicators. As Interviewee #CVN3-7UBK explains, multiple parameters can influence whether RPA succeeds or fails, and a case may shift back and forth, receiving partial human review before re-entering the automated

queue for further adjudication. This process is relational: what human adjudicators input into the case reshapes how RPA interprets the next steps, demonstrating how human and non-human actors continually affect and modify one another within the reimbursement assemblage.

> Many parameters that could modify the outcome. It's kicked out of the process, Agent intervene and we can loop it back into RPA. We're not losing it completely for the efficiency. (Interviewee #CVN3-7UBK)

(Mis)user-Driven Innovation: Reflecting RPA in Action

My role as a Manager of Strategic Initiatives has allowed me to observe how RPA has already transformed the financial service industry. The pandemic stimulated an urgent need for RPA development to prevent financial services from being interrupted by shutdowns. At the same time, we can see how RPA, as a non-human agent, also shapes adjudication outcomes. As both an STS scholar and an industry practitioner, my academic and professional training sensitizes me to the tension between efficiency gains and technoscientific risk. While RPA promises operational speed and cost reduction, it also introduces forms of opacity within what is often described in STS as a "black box"—a system whose internal operations are rendered invisible or taken for granted (Pasquale, 2015; Winner, 1993). This raises critical questions: How does RPA adjudicate cases within the black box of decision-making processes? And are the outcomes produced through these automated systems applied consistently and fairly across cases?

Winner advocates challenging the black box by opening up the process and the technology (Winner, 1993). Examining the inner workings and implications of investigative technologies can reveal that organizational actors—including institutions, designers, and users—often rely on these systems without substantial understanding or critical engagement (Winner,

1993). Winner encourages learning about technology, whether it be a research and development laboratory, a farm, an electrical power plant, a communication centre, an airport, an automated theme park, or other locations. The understanding of technology is contextual, influenced by the specific locations, the technical apparatus in use, and the social processes in which it is embedded. To grasp technology's role and its broader societal impact, broad yet detailed knowledge about both the processes and the technologies involved is necessary for critical reflection. By tracing the human and non-human actors situated within the black box, it becomes easier to identify the connections, relationships, and interactions that form and dissolve the cyber financial crime assemblage, and to see how affective forces become productive within it.

RPA follows pre-determined criteria when processing cases and lacks the analytical capacity to consider situations that fall outside established decision grids. These socially constructed criteria function both as a black box and as a form of closure. In STS, closure refers to the process through which debates in science and technology are settled, leading to the stabilization and widespread acceptance of a particular technology or practice (Pinch & Bijker, 1984). This concept is essential for understanding how technological artifacts and scientific judgments come to be treated as taken-for-granted within institutional and societal contexts. The pre-determined criteria used in adjudication are rarely contested at the moment of their creation, and become even more difficult to challenge once embedded in RPA systems, as the technological black box renders the process inherently opaque to outsiders. Moreover, these criteria carry their own affective force: they channel institutional desires for efficiency, consistency, and risk reduction, shaping how cases are sorted, how liabilities are inferred, and how decisions are enacted. In this way, affectivity becomes part of the closure, stabilizing the

system not through neutrality but through the circulation of institutional priorities and pressures within the RPA apparatus.

RPA may also automate injustices. Cases that human adjudicators once approved or declined may now receive different outcomes because RPAs execute operational tasks in a checklist-like manner, without the situational sensitivity that human judgment provides. Customers may be grouped and labelled through risk scores derived from demographic and financial behaviours, and RPAs may enact business decisions based on these metrics (Villar & Khan, 2021). These classifications are not neutral; they carry affective intensities that channel institutional desires for efficiency, risk minimization, and control, shaping how users are sorted and treated. RPA systems can also be exploited when malicious actors target their decision rules; by feeding fraudulent training data into the system, attackers may steer affective and computational logics toward favourable outcomes (Kosi, 2019).

Jasanoff raises the following key questions: who claims to know? In answer to whose questions? On what authority? With what evidence? Subject to what oversight or opportunity for criticism? With what openings for countervailing views to express themselves? And with what mechanisms of closure in case of disagreement? (Jasanoff, 2017)

With these guiding questions in mind, I have mobilized STS knowledge at my workplace by deploying a series of RPA policy enhancement campaigns for fraud claims using RPA adjudication. The first is to address who claims to know. Instead of having external automation engineers determine RPA rules, I interviewed different frontline adjudicators who have previously adjudicated cases manually and garnered feedback on how to improve RPA logic by incorporating human decision knowledge into the automated adjudication process. If the case

cannot be adjudicated using prescribed criteria, it is routed back to human adjudicator processing instead of making an automated decision based on assumptions.

Even when adjudication decisions are made by human agents, outcomes are not necessarily consistent. The boundary of criminality in cyber financial crime remains fluid, and decision-making is often shaped by individual adjudicators' interpretations of specific case circumstances rather than by strictly uniform rules. As one practitioner explains, variations in customer profiles and claim contexts complicate these assessments:

> There are different types of customers and different types of claims. Some customers are truly victims of fraud and are made whole. In other situations, claims may be declined. Some customers are living pay cheque to pay cheque; there may be indicators of fraud, but they may not have had any direct involvement. (Interviewee #Undisclosed)

Interviewee #Undisclosed further notes that adjudicators may exercise discretion in such cases. For example, when customers experiencing financial hardship are involved in a scam, adjudicators may interpret the situation differently, which can result in a declined claim despite the absence of clear malicious intent. At the same time, practitioners may adopt temporary or conditional measures to mitigate immediate harm. Industry practitioners like Interviewee #Undisclosed might consider temporarily keeping the money on the profile for the customer and taking it out again when they are paid, and then educating them not to do it again. As the interviewee describes:

> I think we've done in the past where we've kept profit on credit, knowing that, you know, in these situations, put the money upfront […] we need to educate customers on how the process works. (Interviewee #Undisclosed)

These quotations illustrate how human adjudication introduces flexibility but also variability into cyber financial crime governance. Decisions emerge through situated judgment, balancing evidentiary assessments, customer circumstances, and institutional practices, rather than through the application of fixed or universally consistent criteria. Unfortunately, these situations and business rules cannot be easily built into automation logics. Adjudication processes are affective and affected by different adjudication rules. The black box of RPA adjudication is not a unilateral data-input and data-output process.

To ensure transparency, our team has worked with the bank's marketing department to deploy a fraud education website so that users are fully aware of how fraud happened and what criteria are used to adjudicate suspected fraud. For operational oversight, we proactively retain all process maps for external audit review and provide ample opportunities for criticism. We encourage external auditors to use customer feedback as a baseline to assess whether the bank has taken appropriate action in addressing concerns in each situation. Interviewee #CVN3-7UBK shares how industry practitioners can stay reflexive when designing RPA processes.

> What RPA can do for us makes us look at our old process. What can we do? We use in that mindset because RPA is doing the same thing slightly different and what we learned from RPA when certain tasks cannot be done exactly the same way the alternative solution became an efficiency solution in their business when we had to do it ourselves. (Interviewee #CVN3-7UBK)

Throughout this project, I have learned that recognizing technoscientific risks introduced by RPA helps a team accurately identify issues and concerns. STS key concepts have become a guiding roadmap for me to effectively strategize about how to lead a team in deploying policies that can improve public trust. For instance, Winner's *Upon Opening the Black Box and Finding*

it Empty: Social Constructivism and the Philosophy of Technology and Callon's *The Sociology of an Actor-Network: The Case of the Electric Vehicle* provide further elaboration on the concept of black-boxing (Callon, 1986; Winner, 1993). RPAs are often treated as black boxes because they conceal complexities, and users of these technologies rarely inquire about what is inside. The unopened black boxes may hide important normative issues, such as why and how certain RPA decisions were made. When designing RPA, I consider how customers might react to the RPA's decisions and how the bank can take responsibility for innovative practices.

I have also identified several challenges. For example, RPA may discourage operational improvement initiatives. Even when risks are recognized, institutions may delay process enhancements when modifications become complex and costly. Automation requires additional time, financial investment, and technical expertise to reconfigure, and these pressures generate affective hesitations—organizational impulses to defer, avoid, or minimize disruption. Such affective dynamics can create barriers to maintaining public trust.

Affectivity does not always generate new innovations; at times, affective forces introduce hesitation that slows or halts the development of a product or service, pushing the assemblage in alternative directions. Deleuze and Guattari describe a similar dynamic in the nomadic war machine, where hesitation exists over how to treat conquered territory—whether to return it to open space or allow a State apparatus to take hold—and this hesitation enables the State to capture the war machine and turn it against the nomads (Deleuze & Guattari, 1987). This affective hesitation reveals how indecision can shift trajectories, enabling new forms of control or reorganization. Likewise, as actors in the cyber financial crime assemblage enact their concerns and uncertainties, affective pressures reorient priorities. As different actors enact their concerns, uncertainties, or risk sensitivities, the assemblage reorients itself through these

affective pressures, thereby redirecting resources, altering priorities, or abandoning certain initiatives altogether.

As Wynne details, the concept of public mistrust began to garner more attention in recent decades after the infamous 1986 Chernobyl disaster and the 1996 mad cow disease epidemic regulatory failure in the UK (Wynne, 1992, 2007). At the beginning of the twenty-first century, widespread moves to restore public trust in science started to emerge. One of the strategies to increase trust is to increase democratic participation during the knowledge creation process (Christou, 2018; Gillespie, 2006; Irwin, 2008; Roth et al., 2003).

STS scholars have advocated for the reorganization of existing relations among decision-makers, experts, and citizens in the management of technology in order to systematically assess risks, avoid miscommunications and mixed messages, and rebuild public trust (Abraham & Sheppard, 1997; Arimoto & Sato, 2012; Funk, 2017; Jasanoff, 2003). By developing a two-way public dialogue with science initiatives and fostering the co-creation of democratic knowledge, public mistrust can be significantly reduced, therefore increasing user confidence when engaging with emerging digital technologies.

However, developing two-way public dialogue can be challenging. Technoscientific knowledge depends on specialized training, practice, and accumulated experience. A fraud investigator, for example, requires years of embodied learning to recognize digital traces of fraud, and a fraud detection strategist must master coding and analytic techniques to build effective detection models. Cyber financial crime professionals cannot generate or interpret such knowledge without prior expertise. Because technoscientific production is shaped by heterogeneous human and non-human actors (tools, platforms, datasets, and protocols), it carries affective intensities that further distance it from lay understanding. These sociotechnical and

affective layers make technoscientific knowledge difficult to access and not easily comprehensible to the broader public.

Currently, users of digital products and services must adapt to technological systems if they wish to benefit from the convenience those systems offer, even when the underlying processes remain opaque to them—or when those processes may embed biases or produce unequal outcomes (Pasquale, 2015). In such cases, technology can function not merely as a neutral tool but as a decision-making mechanism whose criteria are inaccessible and contestable. Responsibility for ensuring fairness and equality in product design, process flows, and decision trees therefore rests largely with the technoscientific actors who design, implement, and govern these systems, making algorithmic justice an institutional obligation rather than an individual user responsibility.

Although I have not yet found a viable way to cultivate two-way public dialogue about cyber financial crime, articulating these concerns remains essential. The development and adoption of RPA intensify the affective dynamics of trust and distrust circulating around automated decision-making. For institutional actors, automated processes evoke desires for speed, consistency, and operational relief; yet these same processes can generate frustration, vulnerability, and skepticism among users when automation produces decision injustice, opens new avenues for exploitation, or delays needed procedural reforms. If RPA continues to expand, its affective consequences—shaping confidence, fear, reassurance, hesitation, and frustration—become central to understanding its social impact. In a post-pandemic landscape increasingly reliant on automation, these affective tensions demand sustained attention and collective reflection.

7.5 Conclusion

Intensities, forces, and desires animate the cyber financial crime assemblage. Affectivity, as a key characteristic of this assemblage, enables it to operate as a field of becoming, continually reconfiguring itself through the urges, drives, and capacities of both human and non-human actors. To examine how the assemblage is affective, I first analyze the dominant modes of exploitation—credential compromise and identity compromise—and show how these processes carry their own impulses to intrude, overtake, and illegitimately possess. Exploitation is not a passive sequence waiting to be triggered; malicious software, illicit tools, and exploitation kits are affective in that they generate productive outcomes aimed at compromising victims' financial assets. I also discuss two (mis)user-driven innovations, unsecured loans and e-transfer limit thresholds, to illustrate how financial products evolve as exploitation evolves. The field is charged with potential: financial institutions create products, exploitation affectively unfolds, and institutions respond by recalibrating offerings and strategies. These ontological movements generate the intensities that shape the assemblage.

I then examine how financial institutions respond more directly. The platforms, logics, and decisions within institutions are affective as they embody continual desires: to detect fraud, to settle claims, and to deliver improved customer experiences. Detection analytics, algorithmic platforms, adjudication logics, and decision systems are all designed to achieve greater convergence and efficiency in fraud detection. Artificial intelligence, emerging as a (mis)user-driven innovation, becomes a constitutive force within the assemblage and further animates its movement.

The final section analyzes the affective drive to settle. Automated processes operate continuously as forces that reshape customer resolution pathways. Automated investigation and

reimbursement accelerate workflows and expedite compensation, reducing the need for manual adjudication. I also reflect on the adoption of robotic process automation (RPA) within a project context where I collaborated on refining adjudication policies. By tracing how decisions are made, by whom, and through which sociotechnical arrangements, I show how the cyber financial crime assemblage is continually affected and reorganized by heterogeneous actors, each contributing to the dynamic intensities that sustain its becoming.

To summarize, exploitation techniques, institutional responses, analytical platforms, and automated settlement processes all operate through intensities and desires that draw actors into new relations and propel the assemblage forward. What appears as technical or procedural is, in fact, charged with impulses to intrude, protect, optimize, or resolve. These affective movements shape how exploitation emerges, how institutions recalibrate their strategies, and how technologies evolve in response. In this assemblage, stability is not achieved by fixed data inputs or mundane operation procedures, but through the restless energies and drives that circulate between human and non-human actors. Affectivity thus functions as the energy that sustains the assemblage's metabolism, ensuring that the cyber financial crime assemblage remains a field of constant adaptation and transformation.

Chapter 8 - Fluidity: Reconfigurations and Relations of Exteriority

8.1 Introduction

Relations of exteriority (*relations d'extériorité*) is a core concept in assemblage thinking, first articulated by Deleuze and Guattari and later systematized by DeLanda (Deleuze & Guattari, 1987; DeLanda, 2006). For Deleuze and Guattari, an assemblage is composed of heterogeneous elements whose connections are autonomous, contingent, and open to continual reconfiguration (Deleuze & Guattari, 1987). Components are not fused into a unified whole but remain detachable, substitutable, and capable of entering new relations. DeLanda develops this insight by defining relations of exteriority as the condition under which a component can be removed from one assemblage and inserted into another, acquiring different interactions and capacities in the process (DeLanda, 2006). This understanding rejects the structuralist view of internal and fixed relations, treating socio-material formations instead as situated compositions held together by shifting practices and dynamic, contingent connections. Continuous reconfiguration arises because the relations that bind components are external to the parts themselves. Manuel DeLanda builds on this logic by arguing that assemblages persist through the ongoing re-composition of these external linkages, allowing components to enter, exit, or transform their roles without undermining the assemblage's overall coherence.

STS scholars such as Latour, Law, and Mol extend the notion of relations of exteriority by showing how objects and actors hold together through fluid, shifting connections rather than fixed structures (Latour, 1993b; Law, 2002; Mol, 2002). Latour emphasizes that actors move through networks while retaining enough identity and capacity to participate in new relations (Latour, 1993b). Law introduces the idea of fluid space, where objects persist by adapting and transforming rather than by maintaining stable, tightly bounded forms (Law, 2002). Mol argues

that objects are enacted differently across practices, with their coherence sustained through flexible, overlapping transformations rather than rigid boundaries (Mol, 2002). Together, these perspectives illustrate how sociotechnical entities endure through ongoing variation, partial connections, and adaptive realignments.

In this chapter, I explain fluidity through relations of exteriority within the cyber financial crime assemblage. Relations of exteriority indicate that elements are not fully defined by the roles they occupy in one arrangement; they retain capacities that allow them to detach, recombine, and participate in new configurations (DeLanda, 2006). Fluidity, therefore, emerges from the mobility of relations themselves. First, I examine contested liabilities by analyzing how Canadian financial institutions distinguish and manage fraudulent versus disputed transactions, showing that accountability is not fixed but produced through changing alignments among customers, frontline staff, fraud analysts, transaction data, internal policies, and evidentiary standards. These elements can be connected differently across cases, redistributing responsibility. Second, I explore the fluid boundaries of criminality, demonstrating how an individual may be enacted as either victim or perpetrator depending on how documentary traces, risk models, and institutional narratives are assembled in a particular situation. Subject positions emerge from these temporary relational configurations. Third, I analyze how investigation and reimbursement processes themselves are fluid, with guidelines that can bend or be selectively relaxed to mitigate potential reputational risks or accommodate affective pressures. Finally, I consider the use of contractual services in Canadian financial institutions as an example of labour functioning as an exterior component—detachable and reinsertable—that allows institutions to expand or contract investigative capacity in response to surges in cyber financial crime while redistributing cost, expertise, and risk across organizational boundaries.

8.2 Fraud or Disputes: The Contested Liabilities

In this section, I analyze two categories of reported transactions that within Canadian financial institutions constitute two different types of claims: fraudulent transactions and disputed transactions. Fraudulent transactions are generally treated as unauthorized, in other words, as cases where the customer asserts that they neither conducted nor consented to the transaction. These fraudulent cases activate fraud protocols, risk models, and regulatory obligations that position the customer as a potential victim of external exploitation, credential compromise, or account takeover. Disputed transactions, by contrast, are generally classified as authorized but contested. In these situations, customers typically interacted with the merchant or service provider but later challenge the charge either because they are dissatisfied with the amount, the quality of the goods or services received, or the merchant's fulfillment practices.

Differentiating Fraudulent and Disputed Transactions

Latour's work in ANT offers a useful lens for understanding how classifications in cyber financial crime do not merely describe events but actively generate the pathways through which those events unfold. Categories are not static containers but performative mediators that mobilize some actors, documents, devices, and procedures (Latour, 1993b, 2005). Labels such as fraud, dispute, or authorized transaction set different chains of action in motion, shaping institutional responses and decisions. By tracing how these labels are produced, the human and non-human actors involved, such as technologies, investigators, victims, and documents, come into view. Classification thus operates not as an after-the-fact judgment but as a fluid interpretive practice that configures who may act, what counts as credible evidence, and how responsibility is distributed across the network.

The distinction between fraudulent and disputed transactions is crucial because it organizes the investigative pathways, evidentiary standards, liability assignments, and reimbursement thresholds within Canadian financial institutions. When a case is treated as a fraudulent and unauthorized transaction, the likelihood of reimbursement is generally higher, since liability is presumed to fall on external actors rather than the customer. Disputed transactions, by contrast, are more likely to place responsibility on consumers, given that they initially consented to the merchant or service, even if they later contest the legitimacy or outcome of the charge. How consumers describe their cases, how they frame the sequence of events, and how institutions interpret and classify these reports all become indicators of how liability is continually negotiated within the cyber financial crime assemblage. The contestation is fluid: a case may drift between categories depending on new evidence, shifting institutional sensitivities, or changes in how narratives are interpreted. This fluidity demonstrates that categorization is not a neutral, technical exercise but a situated practice shaped by institutional judgment, customer narratives, and the unstable boundaries between fraud, error, dissatisfaction, and exploitation in the broader cyber financial assemblage.

In the following section, I first outline how consumers typically report suspicious or unfamiliar transactions to Canadian financial institutions and how these cases proceed through the initial intake process. This includes the opportunities customers have to articulate their concerns, provide supporting evidence, and narrate the circumstances surrounding the transaction. I examine how these reports are subsequently categorized by institutional representatives such as frontline representatives, back office analysts, and automated systems, where both human and non-human actors play decisive roles in shaping how liability is assigned. Each stage of this trajectory can redirect the case onto a different investigative pathway,

revealing how even small variations in customer narratives, evidence, or system prompts can lead to diverging outcomes. I then examine enhanced authentication as an example of (mis)user-driven innovation to show how institutions adapt their evidentiary practices in response to emerging forms of cyber financial exploitation. These shifting pathways illustrate the fluidity of reimbursement decisions, where liability is not pre-determined but enacted through a series of contingent encounters, interpretive judgments, and procedural checkpoints within the cyber financial assemblage.

To start with, consumers typically become aware of suspicious activity through technology-driven alerts or routine account monitoring. Many Canadian financial institutions employ automated detection and investigation mechanisms that flag unusual patterns—such as atypical spending, foreign transactions, or activity outside the customer's behavioural profile—and immediately trigger fraud alert notifications. When a consumer receives such an alert and reviews the transaction, they may determine that it is unauthorized and proceed to notify the financial institution. Suspicious activity may also be discovered independently, such as when customers review their recent transaction history or examine their monthly banking statements. As most Canadian financial institutions have migrated toward electronic statement delivery, consumers increasingly rely on digital interfaces to monitor their accounts. Online banking platforms, mobile applications, biometric logins, push notifications, and even smart-watch banking features allow customers to identify unfamiliar transactions with ease. Through this combination of automated detection and consumer-initiated review, suspicious transactions enter the institutional intake process, setting into motion the assemblage of assessments, categorizations, and decision pathways that follow.

Upon identifying suspicious activity, consumers typically contact their financial institution to file a claim. This initial contact may occur through several channels: calling the telephone banking line, visiting a branch, or using digital tools integrated into online and mobile banking platforms (Scotiabank, n.d.-b; TD Bank, n.d.-a). Depending on the institution and the customer's preferred mode of communication, these cases are handled by phone-channel agents, in-branch retail banking representatives, or virtual service workers who interact directly with consumers and initiate the intake process.

Banks also enable customers to submit both fraud claims and non-fraud disputes through self-serve technology services, allowing claim initiation through mobile apps, online portals, or guided digital forms. Despite the expansion of digital self-serve reporting, a human agent is still required to review the case and determine the next steps. As Interviewee #R5PL-5ST9 explains, once the customer alerts the institution to suspicious transactions, the institution would assess the report populated in the fraud detection platform, verify key details, and take protective actions on the account, such as blocking cards, disabling access, or initiating additional authentication procedures:

> You know, [the fraud detection platform] might just leave the account at certain point by placing a block, you know, sending out a message to the client your account has been blocked because of some suspicious activity, but then its client might not call us right away. We might have to you know, look into the account before that. And we … need to do [the fraud detection/prevention technology] because [the activities] are also very time sensitive. (Interviewee #R5PL-5ST9)

This hybrid model illustrates how both human and technological actors jointly shape the early stages of the investigation process, with digital tools enabling rapid reporting while human

agents interpret the claims, apply institutional guidelines, and initiate the pathways that ultimately influence liability outcomes. Interviewee #R5PL-5ST9 also shares that upon completing the preliminary investigation, human agents could manually reverse transactions when possible to prevent further financial losses:

> We can reverse transactions; we can take certain actions within a certain time period. If we only wait for the clients to get back to us, you know if we'll only have one team which will be taking the fraud reports or you know, any kind of fraud inquiries from our clients, then it might cause even bigger losses because we will lose the opportunity where we can get the money back by reversing the activities like bill payments or Interac money transfers. (Interviewee #R5PL-5ST9)

Fraud claims are typically understood as claims relating to unauthorized transactions, whereas non-fraud disputes are usually triggered by disagreements between merchants and consumers. Financial institution actors then need to determine the nature of the complaint and decide whether to file a fraud claim or a non-fraud dispute. If a consumer has previously signed up for free trial offers and the subscription charges begin as the free trial period ends, for example, that is considered a non-fraud dispute rather than a fraud claim:

> If they have no knowledge of the transaction, never dealt with the merchant or if they tend to the merchant in the past, but there is there is violation by the merchant where they start using the customer's card for purchases not associated or for billing. I should say, our settlement not associated with any services or correlation of past services for that customer. (Interviewee #CVN3-7UBK)

Guideline Fluidity, Decision Inconsistencies

The distinction between fraud and dispute is often subtle, and many consumers are not fully aware of the difference. However, the way a consumer narrates the incident, presents supporting evidence, and responds to institutional prompts can determine how the case is initially classified. Once categorized, the claim is routed into a specific workflow, and this procedural pathway significantly shapes the subsequent investigation and reimbursement outcome. In some Canadian financial institutions, preliminary screening mechanisms are used to determine whether a claim should be treated as fraud or as a non-fraud dispute. This screening may involve structured questionnaires administered either by human actors—such as call centre agents or branch representatives—or by non-human actors, including virtual fraud claim tools or chatbots. These early classification processes play a decisive role in how the case proceeds and how responsibility is ultimately allocated.

Furthermore, these questionnaires typically involve an investigation into the customer's prior dealings with the merchant. If the customer has interacted with the merchant before, such as through having made previous purchases, having an account with the service provider, or having authorized a recurring payment, additional investigation is required to determine whether the case should be treated as a disputed transaction.

Establishing intent is a central part of this assessment. When the customer acknowledges that they initiated the transaction but disagrees with the amount charged, the quality of the service, or the merchant's fulfillment practices, the case is usually routed as a disputed transaction. By contrast, if the customer asserts that the transaction was entirely unauthorized—in other words, if they claim they have no knowledge of the merchant, the service, or the

circumstances under which the charge occurred—the institution is more likely to categorize the case as a fraudulent transaction.

This categorization shapes not only the investigative pathway but also the liability framework, evidentiary expectations, and reimbursement prospects that follow. The preliminary screening enables financial institutions to determine which procedures, verification steps, and documentary requirements are needed for the next stage of assessment. Non-fraud disputes and fraud claims diverge significantly once this initial determination is made. Non-fraud disputes follow an operational process grounded in the chargeback system, in which the financial institution contacts the merchant's acquiring bank and requests that the merchant provide evidence or re-issue credit to the consumer's account (Chargeback Gurus, 2021c). By contrast, fraud claims typically require more extensive investigation and adjudication, involving the review of authentication logs, device data, behavioural indicators, and customer statements. These cases often trigger account protections, risk-scoring adjustments, and internal fraud operations reviews. Therefore, the case categorization process becomes a pivotal moment that sets claims onto distinct institutional tracks, each carrying different expectations, timelines, and potential outcomes for consumers (see Figure 14).

Figure 14. Differences Between Fraud and Dispute



Note. Adapted from "Fraud vs. Dispute: What's the Difference?" by MSU Federal Credit Union, 2017. https://www.msufcu.org/fin40/story/1036/

In this sense, customers co-construct the narrative of their claims, directly shaping whether an incident is classified as fraud or a non-fraud dispute. This shared authorship parallels de Laet and Mol's analysis of the Zimbabwe Bush Pump, a technology that succeeds through distributed ownership rather than fixed design (De Laet & Mol, 2000). Despite scarce resources and uneven technical expertise, communities kept the pump functioning by installing, repairing,

and modifying it with whatever tools and materials were available, producing multiple local versions that diverged from engineers' original specifications. This distributed ownership demonstrates the fluidity of the assemblage: no single actor—engineers, government, or community—fully controls the pump. Likewise, liability in fraud and non-fraud disputes is fluid, continually contested and reconfigured through shifting evidence, evolving narratives, and situated judgments.

As many Canadian financial institutions do not publicly disclose the precise criteria they use to differentiate fraud from dispute, I draw on a definition provided by the U.S. institution MSU Federal Credit Union to illustrate the operational distinction. This example illustrates the fine line between the two categories and highlights how consumers may experience very different institutional responses depending on where their case is routed. Because the boundary between fraud and dispute is fluid, consumers often encounter variation in adjudication and reimbursement outcomes.

This fluidity in adjudication can produce inconsistencies, as institutional guidelines shift in response to emerging exploitative tactics, operational pressures, and evolving interpretations of consumer intent. Some customers acting with malicious intent may exploit ambiguities in these guidelines by filing a disputed transaction as a fraudulent one in order to obtain reimbursement from the bank. In such cases, a customer dissatisfied with a product or service might claim never to have authorized the transaction at all, thereby misrepresenting a merchant dispute as external compromise. This creates a financial burden for the institution, as no fraud, intrusion, or account compromise actually occurred. At the same time, the reverse scenario is also possible: a genuinely fraudulent transaction may be misclassified as a merchant dispute because the customer has had prior dealings with the service provider, or because the available

evidence appears consistent with an authorized transaction. Such wrongful adjudication can delay reimbursement and shift liability onto victims, resulting in loss of funds and a breakdown of confidence and trust in the financial institution.

Although Canadian financial institutions make ongoing efforts to align operational practices and protect stakeholder interests, the process remains complex. Institutions continue to invest in refining definitions of fraudulent transactions so that genuine victims can be properly identified and compensated, while individuals involved in merchant or service disputes are directed toward appropriate chargeback or merchant-resolution processes. Central to this differentiation is the capacity to determine whether a consumer authorized or intended the transaction, an assessment that increasingly relies on enhanced authentication processes.

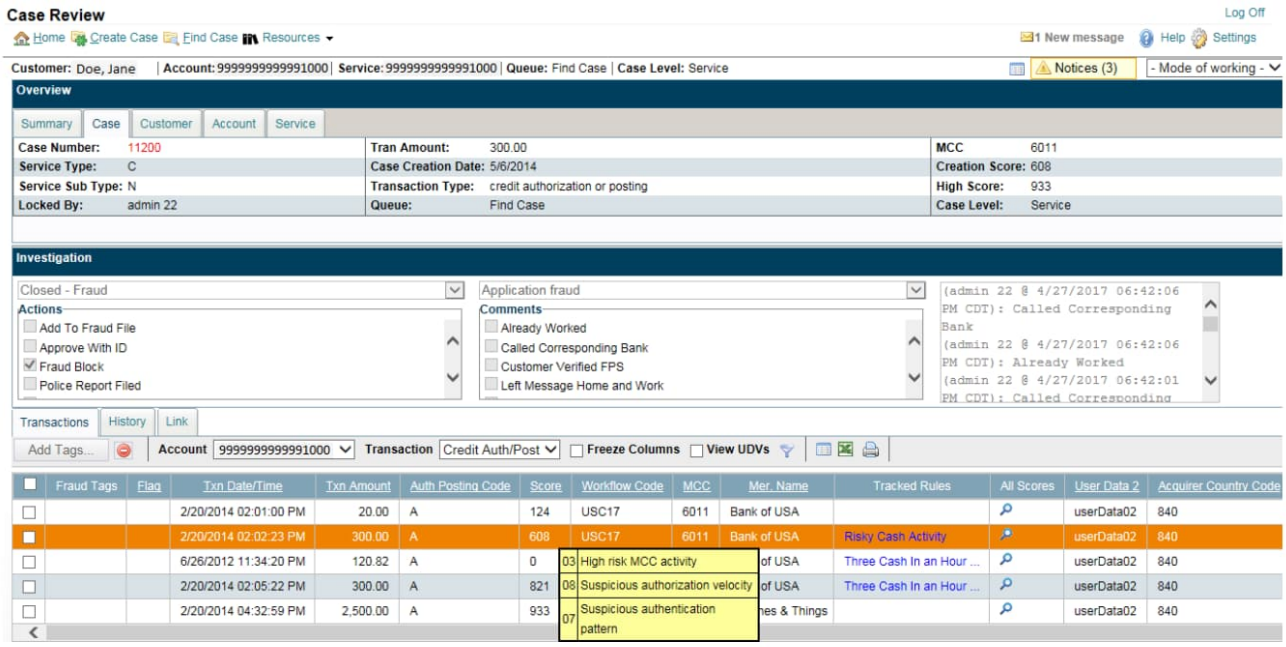
(Mis)user-driven Innovation: Enhanced Authentication

One of the most notable examples of (mis)user-driven innovation for adjudication consistency is the ongoing transformation of authentication procedures. As fraudsters repurpose existing features or exploit gaps in authentication processes, Canadian financial institutions modify and enhance the ways they verify customer identity and authorize transactions. In doing so, financial institutions reconfigure the evidentiary terrain itself, illustrating how both fraudulent and disputed transaction claims become sites of contested liability, prompting institutions to refine their internal logics in order to better differentiate between the two categories and mitigate losses absorbed on the institutional side.

To illustrate this process, I provide an example of how fraud investigators determine whether suspicious activity is legitimate and whether it was carried out by the customer. Investigators are typically alerted to potential cases through PAT platforms or through referrals from internal partners such as branch staff or phone channel representatives. PAT platforms

function as fraud detection and case management tools, surfacing alerts related to unusual transactions, login attempts, or behavioural patterns that trigger fraud detection algorithms (see Figure 15). These alerts give investigators an initial view of potentially unauthorized activity and serve as the entry point for verifying customer involvement.

Figure 15. Example of a Cyber Financial Crime Investigation Platform



Note. From "Explainable AI in Fraud Detection - A Back to the Future Story," by S. Zoldi, 2017, *Fico Decisions Blog*, https://www.fico.com/blogs/explainable-ai-fraud-detection-back-future-story

Once a suspicious activity alert is generated, investigators typically begin by assessing the entry point into the account. This often involves examining the authentication method used—such as password entry, biometric verification, one-time passcodes, or device recognition—to evaluate the likelihood that the activity was performed by an unauthorized user (Kiljan et al., 2016). Authentication analysis becomes a key indicator of risk, helping investigators determine whether the transaction aligns with the customer's usual access patterns or suggests external

compromise. Table 7 presents some classic authentication methods leveraged by Canadian financial institutions:

Table 7. Common Authentication Methods

Authentication Method	Examples
Personal Identification Number (PIN)	Bank card PIN
	Telephone banking PIN
Digital Banking Passwords	Online banking password
	Mobile banking password
Biometrics	Facial Recognition
	Fingerprint Recognition
	Iris Recognition
	Voice Recognition
Two Step Verification (TSV)	Text Message Verification
	Phone Call Verification
	Email Verification
	In-App (Mobile App) Verification

For each authentication method, the level of security and the degree of trust the financial institution places in it differ. A bank card PIN or online banking password can be easily shared or disclosed to a third party, making these forms of authentication more vulnerable to misuse. Biometric methods, by contrast, are far more difficult to replicate or transfer, and therefore carry a stronger presumption that the verified activity was performed by the legitimate customer. As authentication methods become more robust, investigators are more likely to interpret the reported transaction as one involving some degree of customer authorization or participation. This increases the tendency to categorize the case as a disputed transaction rather than a fully fraudulent and unauthorized event, illustrating how authentication strength directly shapes liability assessments and adjudication outcomes. Based on my interviews, financial institution practitioners generally favour more enhanced authentication processes, as they view these measures as offering stronger protection for customers:

> But to have like that type of technology where you have biometrics, right they're readily available as the primary point like authentication. I think that's absolutely fantastic. Because especially when you have facial recognition or fingerprint recognition like that, would help determine the authenticity of a lot of customers so I will I'd be all for that. (Interviewee #65Q7-JVHG)

Stronger authentication not only safeguards consumers but also supports more accurate adjudication by helping institutions distinguish between true fraud and disputed transactions. Enhanced verification provides clearer signals about user intent, reducing ambiguity in liability assessments and improving the institution's ability to identify genuine victims. As one interview participant explained, enhanced authentication should be made mandatory across the industry, as it is increasingly essential for effectively managing cyber financial crime, preventing unauthorized access and ensuring that reimbursement decisions are based on reliable indicators of authorization.

> I think authentication should be made mandatory, like you know, how it happens in India, like, you know, over here in North American market, I think because the population is less as compared to other countries. And the chances of fraud are less as compared to how it is in India. (Interviewee #Undisclosed)

The undisclosed interviewee described their experience in India, where customers are required to complete step-up authentication for most transactions, making multi-layered verification a routine part of everyday banking. These mandatory measures significantly reduce unauthorized activity by ensuring that each transaction carries a strong, verifiable signal of customer intent.

> So what I've seen in India is like there is a forced authentication; you have to enforce authentication on your customers. If I have an account in an Indian bank and if I'm transferring money, I cannot transfer it without an OTP. (Interviewee #Undisclosed)

When enhanced authentication methods are integrated into transaction reviews, reported transactions are more likely to be directed through particular case-processing pathways. However, the ways in which transactions are validated, evidence is gathered, and information is used for adjudication and reimbursement remain contingent on the elements assembled in each case. Decisions are made case by case according to the documentary traces, system outputs, institutional policies, and interpretive judgments available at the time. No rigid framework can produce fully consistent outcomes because these components retain a degree of autonomy and may enter into different relational configurations (DeLanda, 2006). Consequently, the boundary between fraud and dispute is continually renegotiated through changing practices, emerging exploitative tactics, and institutional recalibrations.

Rather than operating as fixed categories, fraud and dispute function as flexible classifications shaped through relations of exteriority. Evidentiary standards, authentication processes, analytical tools, and organizational priorities can be revised, replaced, or recomposed without requiring the entire system to be restructured. As these components are detached and reconnected in new configurations, the classification of transactions and the resulting institutional responses also change. This ongoing reconfiguration illustrates how the cyber financial crime assemblage adapts to emerging threats, changing evidence, loss-prevention pressures, and operational demands.

The Fluidity of Investigative Judgments

Investigations in the cyber financial crime assemblage do not operate by fixed procedural steps, and similarly, institutional judgments are also fluid. For each case, based on the authentication channel, the investigator at a Canadian financial institution can assess the possible risk exposure using available information. Fraud detection platforms automatically organize information critical to investigations in their user interface, including but not limited to phone numbers, residential addresses, work addresses, email addresses, device IDs, operating systems, IP addresses, bill payment payees, money transfer destination countries, and other recipient information (Prosa Mx, 2021; Rajput, 2020).

From there, human investigators, with the assistance of technology, can then determine the legitimacy of the alerted activities. Investigators can try to gather evidence to understand how likely this activity is initiated by legitimate consumers; some of the evidence collection can be related to factors such as authentication (failed) attempts, payee history, recent account maintenance, consumer transaction patterns, device health and safety, and biometric authentication risks (Prosa Mx, 2021). Investigators can also review how many times the attempts were blocked to determine the potential algorithmic risks associated with the activities (Cheng et al., 2020).

Typically, investigators rely on consumer profiles and consumer context to determine the legitimacy of a transaction. First, investigators need to determine how the suspicious activity was initiated, which could be through contactless payment, in-branch transactions, card present transactions at a merchant terminal machine, Europay/Mastercard/Visa (EMV) chip and pin verified transactions, online banking activities, or mobile banking or mobile wallet activities.

Different types of transactions may shape the investigation scope, tools used, and the investigation techniques (Experian, 2020).

Recent account suspension notices and recent activity confirmations can both signal elevated risk. An account suspension typically indicates that high-risk activity has been detected, while a transaction confirmed by the "customer" may not necessarily reflect genuine authorization, as fraudsters may impersonate legitimate users. When a transaction is blocked by fraud detection algorithms but subsequently confirmed by the "customer," and then flagged again, this sequence may indicate that the fraudster intercepted the verification message and maliciously confirmed the transaction. In such cases, the system records the activity as customer-authorized, while the real consumer is simultaneously being victimized.

8.3 The Fluid Boundaries of Criminalities

Within the assemblage of cyber financial crime, the distinction between victim and perpetrator is not neatly contained in categorical guidelines. The distinction continuously evolves as evidence, institutional judgment, and technological practices change. Deleuze and Guattari's understanding of assemblages reinforces this view by showing that categories hold together through contingent, external relations rather than through stable essences, allowing elements to drift as practices and capacities change (Deleuze & Guattari, 1987). Law and Mol similarly argue that objects and classifications are enacted differently across contexts: the fluidity of space and objects transforms the situated rules, networks, politics, and institutional realities (De Laet & Mol, 2000; Mol, 2002).

STS scholars describe these processes through the notion of boundary work, understood as the ongoing negotiation through which boundaries are established, contested, and maintained across social and institutional settings (Feenberg, 1991; Pereira, 2019). Boundary work is not a

fixed or purely technical process; rather, it is shaped by power relations, social norms, and technological developments that condition how distinctions are drawn and sustained in practice. As Feenberg argues, these boundaries are inherently unstable and continually reconfigured as technologies evolve and institutional priorities shift, making governance and knowledge claims contingent rather than settled.

Building on this broader STS tradition, Gieryn offers a more specific account of how epistemic authority is produced and defended through boundary work. He argues that scientific knowledge acquires cultural authority as it moves beyond laboratories into courtrooms, boardrooms, and public life, where actors must decide which claims are credible and whom to trust (Gieryn, 1999). Using the metaphor of maps, Gieryn illustrates how actors navigate competing knowledge claims by drawing boundaries that privilege certain forms of expertise over others. These processes unfold as credibility contests in which actors strategically mobilize claims of objectivity, empiricism, or utility to secure epistemic primacy in particular contexts (Gieryn, 1983). These fluid boundaries determine how meanings and values circulate—how they are constructed, challenged, and enacted in technological systems and everyday institutional practice.

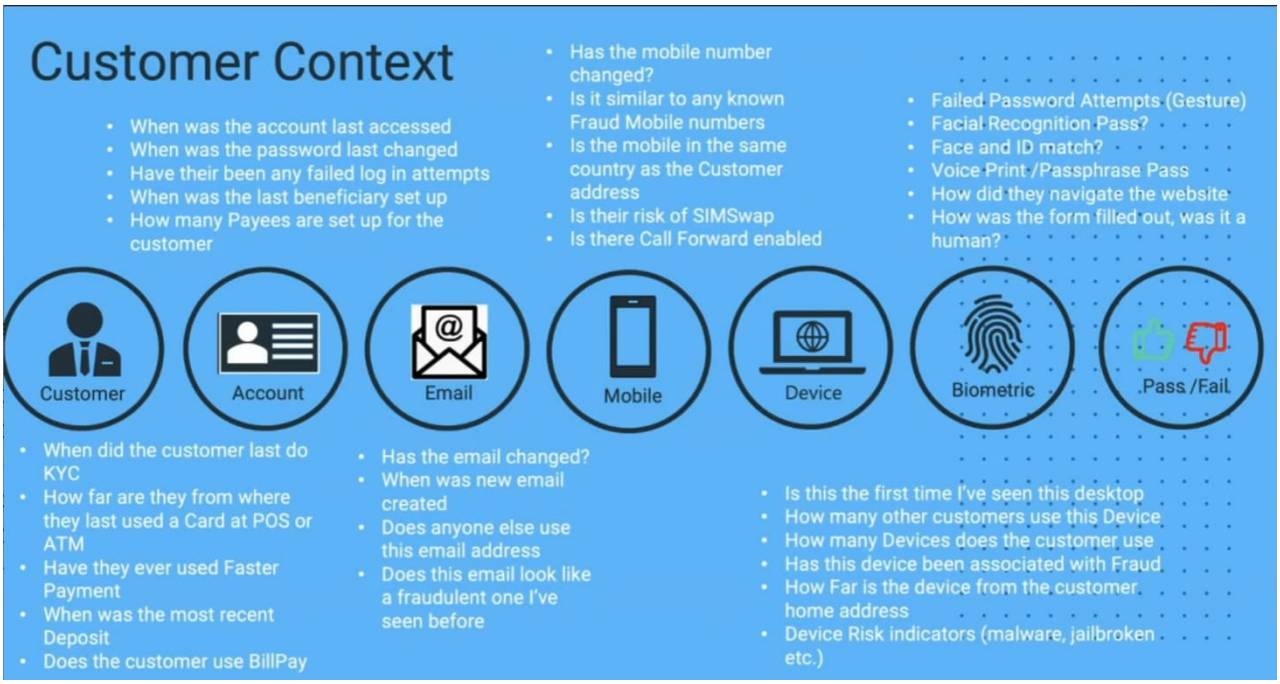
In this section, I examine the fluidity of institutional judgment and how criminality takes shape differently as investigations move across contexts. These interpretations emerge through co-existing and sometimes conflicting notions of use and misuse, which are especially visible in scam cases where a customer may be positioned at once as both victim and perpetrator. The responses applied to (mis)users are therefore situated outcomes of these relational assessments. Restrictions, penalties, or accommodations do not flow from a fixed measure of severity. Instead, severity itself is assessed through financial exposure, patterns of activity, institutional risk

tolerance, reputational concerns, and the anticipated likelihood of customer complaints. Criminality is not defined apart from these practices; it is enacted through them.

Finally, I discuss how writing off fraud losses functions as a form of (mis)user-driven innovation in Canadian financial institutions. Decisions to absorb losses instead of intensifying detection or punishment follow calculations about investigative cost, operational efficiency, and resource allocation. When intervention costs exceed the loss amount, institutional action may shift away from formal criminalization, not because the conduct is harmless but because other responses become more workable within the assemblage. In these cases, criminality is not removed but reorganized through economic and organizational logics that shape how responsibility and intervention are carried out.

Figure 16 illustrates how financial institutions form judgments about suspicious activities by investigating customer profiles. The heterogeneous elements—customer demographics, account activities, transaction patterns, email usage, mobile number legitimacy, device security, biometric signals, and authentication outcomes—move in and out of the cyber financial assemblage. Their movements coordinate productively, forming temporary unities that enable judgments to be enacted. Even when these elements appear unrelated, they circulate and converge like a fluid, producing coherence without fixed structure.

Figure 16. Human-Machine Collaboration Investigation: Customer Context



Note. From "Fraud Detection Algorithms: Contextual Profiling and Orchestration" [Video], by Prosa Mx, 2021, *YouTube.*

https://www.youtube.com/watch?v=Ys7yrIzg2t4&ab_channel=ProsaMx

Law and Mol describe a similar mode of fluidity in their analysis of Quaker meetings (Law & Mol, 1998). These unprogrammed gatherings rely on silence rather than formal agenda, yet coherence emerges through subtle arrangements: chairs, tables, flowers, texts, advice notes, schedules, clocks, sound loops, heating, and communication devices. These material and immaterial components quietly shape the meeting, enabling a shared orientation without rigid order.

The movements of the Spirit in Quaker practice cannot be counted, yet this very incommensurability is what enables the meeting to cohere (Law & Mol, 1998). Likewise, the cyber financial assemblage is sustained by a fluid interplay of dispersed elements whose coordination emerges without fixed structure. Because no two cases are identical, institutional

judgments unfold in real time, shaped not by predetermined categories but by situated interpretation, contingent evidence, and the shifting relations among human and technological actors.

Co-Existing Use and Misuse

While banks are not law enforcement agencies, major Canadian financial institutions collaborate to regulate and manage cyber financial crime as part of their broader risk and compliance responsibilities. In practice, any misuse of digital financial products or services that results in financial loss or threatens a financial institution's reputation and customer trust may be treated as misuse and categorized as cyber financial crime.

Within this framework, industry practitioners may assign multiple identities to the same individual when an incident occurs. A customer can be positioned simultaneously as a victim and a perpetrator depending on the surrounding circumstances, available evidence, and institutional interpretations. As a result, some victims of cyber financial crime may be labelled as misusers or even perpetrators due to perceived misconduct. For example, customers who incur losses may still be classified as misusers if their actions—such as sharing credentials or bypassing security protocols—are interpreted as contributing to the compromise.

Therefore, there are situations in which Canadian financial institutions maintain fluid boundaries of criminality. As institutions co-construct technologies and policies with their (mis)users, the line between offender and victim becomes contested and unstable. For example, a job scam victim may be instructed to deposit a counterfeit paycheque and, following those instructions, unknowingly misuse the digital cheque deposit feature without any fraudulent intent. In such cases, the individual is simultaneously positioned as a victim of deception and a

perpetrator of misuse, demonstrating how criminality in the cyber financial assemblage is enacted, interpreted, and redistributed rather than fixed in advance.

This scenario illustrates a revealing intersection in the fluid boundary between offenders and victims within the cyber financial crime assemblage. A job scam victim unknowingly misused digital financial services by depositing a counterfeit cheque and, as a result, incurred financial losses. Although the individual was clearly victimized, the financial institution nevertheless imposed penalties for breaching policies that prohibit depositing illegitimate cheques through digital channels, leading to restrictions on the customer's future access to mobile deposit functions. Simultaneously, the institution updated its fraud detection algorithms in response to the incident, adjusting its technological and procedural practices through (mis)user-driven innovation. In doing so, Canadian financial institutions not only participated in socially constructing the meanings of uses and misuses in the cyber financial crime assemblage but also enacted a fluid boundary in which criminality is continually shaped by networked power relations, institutional judgments, and everyday social practices (Bijker et al., 1987).

The quotations below from industry practitioners illustrate how the cyber financial crime boundary can be fluid in the Canadian financial ecosystem when defining offenders and victims. Some industry practitioners believe misusers can be victims and perpetrators at the same time. In this view, the customer's role is not singular; it is flowing and overlapping, depending on who is investigating the case and how victims position their stories.

> Whether someone is a victim or a perpetrator, I mean, I suppose somebody could be both. (Interviewee #2YNV-3L4Y)

> It depends on the intention. (Interviewee #BAWZ-SXX7)

> Those recipient fraud funds, where they're also a victim too, where their accounts are essentially being used as mules. (Interviewee #E5M8-TZRB)
>
> It's not a cybercrime […] they're doing the right things, like people who are victims of the job scams and love scams. (Interviewee #3NGU-8XTJ)

Who, then, are the victims, and who are the perpetrators? To begin, it is useful to consider a definition of victimhood widely adopted within public and legal assemblages in Canada. A victim is typically defined as a person who has suffered physical or emotional harm, property damage, or economic loss as a result of a crime (Department of Justice Canada, 2015). Under this public definition, many would assume that cyber financial crime victims are individuals who incur financial losses through events such as card compromise, identity theft, or unauthorized digital transactions. Even attempted thefts that do not result in direct loss can render individuals victims within this framework, as the experience of intrusion, fear, or harm is itself recognized.

While the Department of Justice definition is valid in many contexts, it does not always hold when examined within the operations of Canadian financial institutions. As seen in the job scam example, consumers who suffer losses can nonetheless be treated as cyber financial offenders. Based on available digital evidence and transaction records, institutions may determine that these users violated terms and conditions in their cardholder agreements, such as depositing counterfeit cheques, and therefore classify them as misusers or perpetrators. This raises a critical question: are these individuals genuinely cyber financial criminals, or are they victims of deception whose actions were shaped by manipulation and misinformation?

Canadian financial institutions construct fluid and situational interpretations of cyber financial victimization that do not always align with public definitions. Within institutional

settings, identifying a “victim” is not a fixed or universally applied category; rather, it is an interpretive and co-constructed process shaped by organizational power, evidentiary practices, and institutional risk logics (Brown, 2015; Jasanoff, 1998).

My interview participant #NF8T-GHAB shares that Canadian financial institutions have the power to shape the formation of victim identities through non-public policies and procedures, such as reimbursement guidelines:

> When it comes to scam type scenarios… yes, you can submit a claim, but the odds of them getting the money back are pretty slim. So I think that’s a grey area. That’s unfortunate because from a client perspective, they’ve been taken advantage of big loss of money. But they’re just unable to get it back at the end of the day. (Interviewee #NF8T-GHAB)

Here, Interviewee #NF8T-GHAB illustrates how scam victims in Canada may still be unable to recover their losses even after filing a fraud claim. Through reimbursement guidelines and internal procedures, financial institutions possess the resources and authority to discourage what they interpret as inappropriate digital banking practices.

As a result, victims who unknowingly engage in risky or non-recommended actions may be reframed as partial perpetrators, simultaneously suffering financial harm and being positioned as having contributed to illicit activity. A fluid object reconfigures itself through multiple enactments, and its loose boundaries allow relations among actors to shift (Mol, 2002). Human and non-human actors continually transform, and these ongoing adjustments contribute to the formation and stabilization of the assemblage. In this view, fluidity is a mode of stabilization achieved not by freezing relations but by allowing them to move, adapt, and reorganize.

Star and Griesemer’s work examines how diverse social groups, such as amateur collectors, farmers and traders, museum staff, and academic researchers, jointly contributed to

the Museum of Vertebrate Zoology's practices of knowledge production during the early twentieth century (Star & Griesemer, 1989). In their study, specimens and associated data functioned as boundary objects, interpreted and mobilized differently by each group. These objects were not fixed or neutral; rather, their meanings shifted according to the power relations, expertise, and situated practices of the actors involved. Boundary objects therefore reveal how categories and artifacts travel across social worlds while remaining flexible enough to accommodate multiple interpretations.

A similar dynamic occurs in the cyber financial crime assemblage, where financial loss accountability functions as a boundary object. Standard consumers, victimized consumers, Canadian financial institutions, public law enforcement agencies, and regulatory entities such as the Criminal Code of Canada each interpret and enact this fluid boundary differently. These human and non-human actors bring distinct priorities, evidentiary standards, and forms of authority to the process, producing fluid and sometimes contradictory understandings of who is responsible for losses. As with Star and Griesemer's boundary objects, accountability in cyber financial crime is not a fixed concept but a negotiated and context-dependent construct shaped by institutional power, social practices, and the heterogeneous actors involved (Star & Griesemer, 1989).

Fluidity in Treating (Mis)users

From an assemblage perspective, not all social phenomena or events can be neatly categorized by fixed attributes or stable natures. Fluid relations hold things together in ways that are often messy yet still coherent. McFarlane and Anderson (2011) describe assemblage thinking as a method for tracing these shifting relations—following how elements emerge or disappear, mutate or realign, generate political effects, and momentarily form unities. Such contingent and

fluid relations resist fixed structures, consistent emotional registers, and predictable outcomes. Rather than imposing rigid categories, assemblage thinking responds to emergent formations as they take shape.

Having shown how an individual may simultaneously occupy the positions of both offender and victim, I now turn to another dimension of fluid criminality within the cyber financial assemblage. My empirical findings show that some fraud professionals actively gather evidence to determine whether a customer intentionally violated financial service agreements, exploited financial products, or misused technologies in ways that indicate deliberate authorization and personal responsibility. In such cases, misusers are positioned closer to the perpetrator end of the spectrum. On the other hand, some fraud professionals view customers who misuse technology yet suffer financial losses as victims rather than perpetrators, especially when the misuse stems from manipulation, misinformation, or limited understanding of the consequences.

Interviewee #3NGU-8XTJ and Interviewee #LX4K-Z3DK noted that they continuously review customer profiles, transaction patterns, and abnormal behaviours to determine customer intent. As digital evidence unfolds, a customer's potential intent to abuse financial products or technologies emerges through the interpretive work of investigators. Their judgment calls determine whether the behaviour is classified as accidental misuse, negligent action, or intentional wrongdoing. In this sense, offender and victim are not predetermined categories but enacted positions that shift as institutional actors assess the available information, interpret intent, and apply organizational rules.

> Based on prior banking experience working in telephone banking […] I was able to understand customer interactions, understand the psychology behind banking patterns on

> customers, you know, spending habits and those foundations pretty much, you know, with the fraud knowledge that brought me here […] I can look at a profile or a scenario or situation and determine what is fraud what is not and what is actually a client authorized activity and what is a non client authorized activity. (Interviewee #3NGU-8XTJ)
>
> File a claim, submit the request, give us the details why the fraud happened so that we can work on the case. [The financial institution] has expertise in determining whether the transaction was completed by the customer or not, doesn't matter if it's online or a phone channel; we have all the tools to check digitally. So based on that story, [the financial institution] finds out whether you have been defrauded. (Interviewee #LX4K-Z3DK)

Not all misusers are treated as perpetrators when investigators do not see malicious intent behind the activities. The statements below from interviewees #LX4K-Z3DK and #AR26-4DEE show that industry practitioners are often inclined to treat customers who misuse digital financial products and services as victims, depending on the circumstances surrounding the incident. In their view, the "real" cybercriminals are located elsewhere in the digital ecosystem, operating from the opaque and often unreachable spaces of cyberspace. Punishing customers in these circumstances is seen as inappropriate, particularly when the individuals had little or no understanding of the consequences of their actions or were manipulated into misusing digital financial products and services. These practitioners argue that holding such customers fully accountable would overlook the asymmetries in fraud knowledge, technological literacy, and institutional power that shape these cyber financial crime incidents:

> Customer is a victim […] the person who's doing the fraud, they are somewhere else […] So the actual criminal is not punished, we are punishing our own customers. So I don't

> think that could make any sense to punish our customer when they lost all this money in a scam and they have no idea about it. (Interviewee #LX4K-Z3DK)
>
> So a lot of seniors are getting scammed and they are transferring to, like crypto companies. Although the companies are legitimate, but the fraudsters could be taking advantage because the seniors don't really know exactly how it works […] they don't have the knowledge to do so. (Interviewee #AR26-4DEE)

Variations in how (mis)users are treated are often shaped by investigative assessments of intent. When available information suggests that an individual may have sought financial benefit, investigators may interpret the activity as intentional misuse of financial products or services. In other cases, assessments of intent may be informed by contextual indicators, including a customer's financial profile, which can shape interpretations of motivation and risk. For example, where customers appear to have substantial available funds, investigators may be less likely to infer an intent to defraud, as such cases are assessed differently within existing investigative frameworks.

As a result, investigative and adjudicative processes may be shaped by contextual assessments of customer profiles. Where customers are perceived as financially stable or exhibit strong credit histories, incidents are more readily interpreted through a victimization frame rather than as intentional misuse of digital banking systems. Institutional considerations, including customer retention and risk management practices, may further influence these interpretations. By contrast, in cases involving financial distress, investigators may encounter greater difficulty in excluding malicious intent, as indicators of vulnerability can complicate determinations of authorization, responsibility, and misuse.

Although Canadian financial institutions have financial service agreements that outline scenarios where customers may be held liable for fraud losses, significant grey areas remain. These ambiguities create space for fluid interpretations of cyber financial criminality. As a result, industry practitioners may make different decisions based on situational considerations, including the desire to maintain customer relationships or offer goodwill reimbursements. Customer demographics, financial portfolios, reputational risks, and the potential for legal or media escalation all shape how liability is assigned and how reimbursement decisions are ultimately made.

Interviewee #LX4K-Z3DK shares an example of how they encountered a high-value customer who experienced financial losses from a cyber scam incident. Interviewee #LX4K-Z3DK wanted to help and tried to resolve the issue for the customer, and more importantly, to de-escalate the issue:

> Now the customer is fighting with us because she is a very high value customer. She is fighting with the branch "get my money back (from other financial institutions)" […] She comes every day to the branch, and you know, screams at us. (Interviewee #LX4K-Z3DK)
>
> So when these things happen […] to de-escalate or avoid any media escalation, we sometimes go out of the way, out of our regular mandate. (Interviewee #LX4K-Z3DK)

Interviewee #LX4K-Z3DK illustrates how the treatment of (mis)users may shift in cases involving customers with substantial financial resources. In this instance, investigators were unable to establish clear evidence of intentional misuse or deception. Consequently, the case was interpreted through a victimization framework, despite the fact that the customer had authorized the transfer of funds that were later identified as part of a cyber scam. Interviewee #LX4K-Z3DK

then attempted to de-escalate the issue by proactively working with the receiving bank to retrieve the transferred funds. Such effortful intervention is far less likely when the customer is financially strained and may be perceived as having a potential motive to commit fraud against the institution.

In cases where a customer has limited prior engagement with the financial institution, the relative absence of an established financial relationship may shape investigative and adjudicative responses, sometimes resulting in more restrictive remedial measures. Interviewee #2YNV-3L4Y illustrates how younger consumers with limited financial portfolios may face greater difficulty proving their innocence because they lack substantial account balances or long-term financial histories to demonstrate credibility. If a young customer unknowingly sold their bank card to an organized crime ring, and the criminals used that card to receive stolen funds, the customer would have little supporting evidence to justify their actions. This can raise suspicions among investigators, who may interpret the behaviour as intentional participation rather than accidental misuse.

> If I'm an 18-year-old, 17-year-old kid, and I unknowingly get caught up in a card sell situation. Right? And, you know, I get exited. […] I am blacklisted in a way from coming back to whatever bank because, you know, in the future, when I try to open up an account, you know, it's probably going to be difficult for me to do so because of something stupid I did when I was younger. (Interviewee #2YNV-3L4Y)

By contrast, if an elderly customer unknowingly sold their bank card under similar circumstances but possessed significant financial assets and an extensive investment portfolio, it would be easier for them to demonstrate a lack of fraudulent intent. In such cases, the elderly customer would more likely be viewed as a victim who was manipulated or deceived.

Meanwhile, the younger customer might face more severe repercussions, such as losing access to certain banking services or being restricted from future use of the institution's digital platforms. This contrast highlights how financial standing and demographic profiles can influence institutional interpretations of intent, shaping who is classified as a victim or a perpetrator within the cyber financial assemblage.

Beyond financial considerations, industry practitioners may also take into account the potential for cases to generate legal, regulatory, or public-facing implications, including the possibility of formal complaints, litigation, or media attention:

> We deal with legal, and we deal with media all the time, right? With legal it's situations where there might be reputational risk or a greater risk […] or the customer is mentioning something that is kind of a grey area, right? […] we have to kind of think of it. (Interviewee #E5M8-TZRB)

The quotation from Interviewee #E5M8-TZRB shows how Canadian financial institutions might face reputational risk. If the case adjudication decision touches on something that is not clearly outlined in the service agreement, it then becomes a grey area. If the case is escalated to legal action or media exposure, financial institutions are required to provide detailed justifications for decisions made within areas of interpretive uncertainty, a process that can place additional demands on institutional resources and operational workflows. Interviewee #2YNV-3L4Y shared a statement that reflects similar concerns:

> It's purely reputational risk, right? Is it worth this going to the media? […] Hey, we're dealing with a 21-year-old who was the victim in the traditional sense of a scam, or we're dealing with an 81-year-old that was the victim of a scam. Who's going to get paid in this

situation? […] If I'm a betting person, it's going to be the 81-year-old and not the 21-year-old. (Interviewee #2YNV-3L4Y)

In cases where anticipated reputational or legal risks outweigh the projected costs of reimbursement, financial institutions may opt to resolve the matter through reimbursement as part of a broader risk-management assessment. In contexts involving potential litigation or media exposure, such resolutions function as mechanisms for mitigating uncertainty and limiting downstream institutional exposure.

I mean, […] customer reputation and client state of mind is definitely a big deal. More and more banks actually try to, really do their best to […] pay for their customers. (Interviewee #WYUV-P7LK)

Interviewee #WYUV-P7LK's statement reflects a perspective shared by some industry practitioners, in which customer trust and relationship continuity are treated as relevant considerations in post-incident decision-making. In certain cases, a customer with substantial assets may respond to an unfavorable adjudication by discontinuing their relationship with the financial institution, including by closing loans, mortgages, investment accounts, or credit facilities.

From an institutional standpoint, reimbursement following a cyber financial crime incident may therefore be evaluated not only in relation to evidentiary assessments but also in light of potential downstream impacts on customer retention. Even where a customer's use of digital banking services raises concerns or aligns with institutional classifications of suspicious activity, decision-makers may weigh the anticipated costs of relationship deterioration against the financial cost of reimbursement. In this sense, reimbursement outcomes can reflect broader

organizational calculations about risk, continuity, and exposure, rather than a singular determination of misuse or victimization.

(Mis)user-Driven Innovation: Fraud Write-Offs

Canadian financial institutions may calibrate their cyber financial crime management practices based on features of customer portfolios, including factors related to account history, transactional patterns, and potential institutional exposure. As Law et al. note, social groups possess different interests, resources, and forms of capital, which shape how they engage with and are interpreted within sociotechnical systems (Law et al., 2012). Consequently, cases that appear similar at a surface level may be assessed and adjudicated differently as they move through institutional processes, reflecting how customer characteristics intersect with organizational routines, risk assessments, and governance considerations.

The notion of misuse is similarly defined by financial institutions themselves. Financial institutions configure products and policies to prevent and regulate misuse according to their operational interests. When digital financial tools are used in unintended or innovative ways that generate losses or reputational damage, institutions recast such use as misuse and initiate technological or policy innovations to suppress these practices.

For example, some of the classic (mis)user-driven innovations, such as enhanced fraud detection algorithms for suspicious cheque deposits and preventative policies like restricting digital-deposit access, are introduced as responses to these (mis)uses. Through these adjustments, Canadian financial institutions leverage (mis)user-driven innovation to re-establish and renegotiate the boundaries of cyber financial crime victimization, continually redefining which behaviours constitute legitimate use and which are framed as misuse.

In this section, I take a step back to assess how financial institutions respond to, evaluate, implement, and promote (mis)user-driven innovation, highlighting whose voices carry weight in shaping these processes. The reconditioning of products, policies, and technologies is not accidental; it is deeply socially constructed, revealing which actors—customers, frontline representatives, fraud analysts, or executives—are heard in the design process and who has the power to drive change.

Decision-making power varies significantly across departments. Retail branches, phone channels, digital product teams, and fraud management units are overseen by different bank executives. Some departments manage profit-generating products such as deposit accounts with service fees or loan products with interest charges. These units tend to have greater influence than loss-prevention or loss-recovery departments such as fraud management, which rely on funding from profit-generating divisions and therefore have limited discretion over what products are launched and how they are designed.

Similarly, digital product design teams construct business cases strategically to secure funding. Different teams pitch their projects to different executives, each aligning proposals with the priorities of those departments. Their agendas differ: the mortgage department may prioritize investment in loan-fraud detection technologies, while the credit card department may seek innovations that increase chargeback efficiency when fraud occurs. These internal dynamics shape how (mis)user-driven innovation is conceptualized, resourced, and ultimately enacted across the cyber financial assemblage.

Technology development in fraud departments often requires funding support from other profit-generating sides of the institution, and, according to my interview participants,

technological innovation projects go through prioritization exercises. The result is the so-called important projects get funded first:

> But again, a lot of the work that we do is based on priority … So depending on what that priority is, and what that priority looks like, that knowledge and market insight could potentially take flight and go on to do something, or it could just be pushed to the side and let fizzle away. (Interviewee #7ETR-0A6C)

> As well as ongoing costs, costs are considered when launching a new initiative. This will further prevent any [technology advancement] because of shortage of funding or shortage of talent leads to increasing operational risk from different perspective. (Interviewee #B7FQ-RANC)

Both Interviewee #7ETR-0A6C and Interviewee #B7FQ-RANC describe how cyber financial crime professionals frequently encounter funding constraints. When making investment decisions, each bank leader operates with their own imagined techno-future and distinct expectations about the role of (mis)user-driven innovation. These differing visions are expressed in the narratives that strategy managers craft when presenting business cases to secure resources. The ability to attract funding often depends less on the severity of vulnerabilities and more on how convincingly a future-oriented story aligns with the priorities of the decision-making executive.

There are moments when financial institutions are fully aware of system or procedural vulnerabilities that cybercriminals could exploit, yet they still choose to launch or continue offering the product because the new digital services provide a better overall customer experience or reduce operational costs by minimizing the need for additional branch or phone-channel staff.

As one undisclosed interviewee explains, fraudsters can intentionally deposit a bad cheque and withdraw funds using the mobile-deposit feature. Even after the fraud management team warned the digital product team about this risk, the institution continued offering the function. This decision reflects a calculated willingness to accept fraud exposure because the broader customer base benefits from the convenience of mobile deposits, and the institution saves operational costs by reducing reliance on physical branches and cheque processing facilitated by retail branch representatives.

In these cases, the institution's strategic priorities—customer experience, efficiency, and cost reduction—are weighed more heavily than the potential for misuse, demonstrating how risk tolerance and resource allocation shape the trajectory of (mis)user-driven innovation within the cyber financial assemblage.

STS literature shows that inventors of technological artifacts do not focus solely on the artifacts themselves; they also attend to how these artifacts intersect with social, economic, political, and scientific elements that are continually shifting (Law et al., 2012). The stabilization of artifacts is therefore a fluid process, dependent on the changing social interests of the groups involved and their varying capacities to mobilize resources during debates and controversies (Law et al., 2012).

In this sense, inventors hold considerable power, not because their designs are fixed, but because they act as system builders who coordinate elements that are themselves fluid and interconnected (Law et al., 2012). Their work unfolds within a landscape of shifting pressures and conflicts from various social groups (Lynch, 1979; Star & Griesemer, 1989). As these pressures evolve, inventors must continually renegotiate alignments, adapt designs, and

recalibrate systems, illustrating how technological development is not a linear process but a dynamic and fluid assemblage shaped by ongoing negotiation.

Hughes refers to these challenges as “reverse salients,” illustrating how inventors tend to prioritize such issues and analyze social, technical, and economic factors together in search of solutions (Hughes, 1979, p.14). In Hughes’ *The Electrification of America: The System Builders*, the author details how Thomas Edison encountered hurdles related to economic issues, such as competitively supplying electric lighting in comparison to gas; political barriers, such as securing approval from local authorities for developing a power system; technical complexities, such as optimizing power structures, reducing current, and increasing voltage; and scientific inquiries, such as developing a high-resistance incandescent bulb filament (Hughes, 1979, p.22). Hughes portrays Edison’s success as seamless, emphasizing the inseparable connections among the social, technological, and economic factors (Hughes, 1979).

Similarly, leaders of fraud management teams hold less decision-making power than leaders of deposit product teams, even when they occupy the same organizational level. If profit-generating teams insist on launching a new digital product and are willing to accept financial losses should cyber financial crime occur, fraud management leaders have limited discretion to halt or withdraw that functionality, even when known vulnerabilities remain. In this context, absorbing fraud losses as write-offs becomes a fluid, (mis)user-driven innovation, where institutional responses shift according to competing priorities, power dynamics, and evolving assessments of risk.

8.4 Mobilizing Operations: The Fluidity of Labour Resources

Within the cyber financial crime assemblage, financial institutions frequently face sudden surges in volume during unexpected fraud attacks, and there is rarely an easy or immediate

solution to address these operational demands. In this section, I examine how high volumes of cyber financial crime transform the assemblage by reshaping its exteriority through the addition of new operational resources. Labour, in this context, is not a constant or stable component. Instead, it is fluid, unstable, and continually adjusted as institutions expand their labour resources to manage increasing case loads.

Deleuze and Guattari use the relation of exteriority to show that an assemblage is never permanently fixed; rather, its components retain the capacity to enter and exit, take on different roles, and form new connections (Deleuze & Guattari, 1987). In *A Thousand Plateaus*, they develop the concept of the *war machine* to illustrate how nomadic groups organize through non-hierarchical, adaptive, and mobile arrangements (Deleuze & Guattari, 1987, p.393). The war machine is not a military institution but a principle of social organization grounded in movement, speed, improvisation, and innovation. It stands in exteriority to the *State* because it is constituted outside hierarchical structures, lacking a stable centre, identity, or predetermined roles. While the State organizes elements by incorporating them, the war machine organizes elements by connecting them in open-ended ways.

Deleuze and Guattari illustrate this through the mobile organizational logic associated with steppe cavalry formations, which were highly mobile mounted fighters whose coordination emerges through movement, speed, and flexible relations rather than centralized command (Deleuze & Guattari, 1987). This model does not describe a social group existing outside the State, but a mode of organization whose relations are not fully determined by hierarchical incorporation. Such formations can intersect with, be appropriated by, or operate within State structures while retaining a degree of relational mobility. The war machine therefore provides a

conceptual lens for understanding how components remain detachable and recombinable as relations shift.

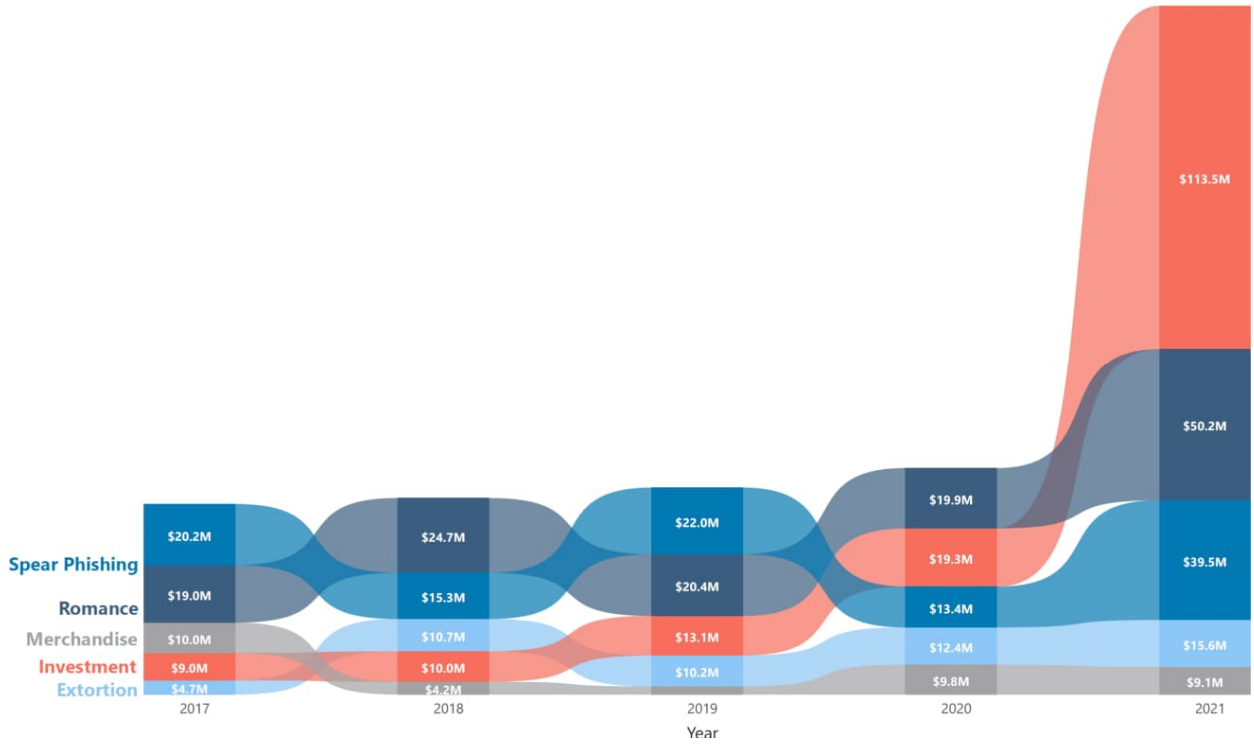
Further, DeLanda understands an assemblage's relations of exteriority as relations in which components can be detached and incorporated into other assemblages (DeLanda, 2006). Because these relations may change without altering the components themselves, the parts retain a degree of autonomy. At the same time, the properties of the parts cannot fully explain the properties of the whole, just as the properties of the whole cannot fully account for the parts. In DeLanda's interpretation of Deleuze's assemblage thinking, assemblages emerge from the capacities of their components—capacities that depend not only on a component's inherent properties but also on the properties of the entities with which it interacts (DeLanda, 2006). These relational capacities allow connections to be detached, reattached, and reconfigured. As a result, an assemblage can be taken apart and reorganized while still producing new and genuine syntheses through shifting interactions.

My interpretation of relations of exteriority in the context of contractual services within the cyber financial crime assemblage can be described as a "patch on, patch off" dynamic—temporary attachments that stop the bleeding when attacks occur. When unexpected fraud surges arise, many financial institutions are not fully prepared, and labour must be rapidly added or removed as external components. Referencing Deleuze and Guattari's interpretation of the war machine, the war machine does not represent pure exteriority but illustrates how exterior relations allow elements to remain detachable, recombinable, and responsive to changing conditions (Deleuze & Guattari, 1987). Its generative potential lies in this capacity for reconfiguration as relations are rearranged. In the following section, I draw on relations of exteriority to examine the fluidity of labour resources within the cyber financial crime

assemblage. Operational capacities can attach, detach, and reorganize across different practices and demands. Consistent with DeLanda's understanding of relations of exteriority, contractual services are not defined by a single organizational position; their properties do not fundamentally change as they move across contexts. What shifts are the relations they enter into. Their capacities—what they are able to do—depend on how they are connected, deployed, or withdrawn within the assemblage. Similar to the war machine, these capacities are not fixed to a single structural position but move across arrangements, enabling the assemblage to adapt without requiring formal institutional restructuring.

Misusers can become surprisingly creative when misusing banking products and services. The Canadian Anti-Fraud Centre 2021 annual report listed $379 million in total reported fraud losses. According to the Top 5 Dollar Loss by Year and Fraud Type chart (Figure 17), fraud has increased drastically since 2017 (Canadian Anti-Fraud Centre, 2022).

Figure 17. Top 5 Dollar Loss by Year and Fraud Type



Note. From *Canadian Anti-Fraud Centre Annual Report 2021* (p. 38), by the Canadian Anti-Fraud Centre, 2022, Government of Canada.

https://publications.gc.ca/collections/collection_2022/grc-rcmp/PS61-46-2021-eng.pdf

Unlike most services and products, the supply–demand relationship in the world of cyber financial crime is never constant, and it never will be. Fraud trends emerge unpredictably: intense waves of attacks can occur suddenly, followed by periods of relative quiet. After each attack, financial institutions typically respond to (mis)user-driven innovation by recalibrating their technologies, strategies, and policies to prevent the same exploit from occurring again. According to the interviewees, this is an ongoing battle. No one can reliably predict when the next attack will happen, and fraud management teams must remain continuously prepared to counter new tactics through their own forms of (mis)user-driven innovation.

> They (fraudsters) are always one step ahead of us. We're always playing catch up. Obviously, when the fraud hits we're just trying to restore accounts. So the scams that are occurring, they're obviously going to change with the times and we have to adapt with the changes that occur. One example of this was the whole OTP trend. And that evolved into fraud. (Interviewee #Q694-3UCT)

> Like obviously, a much bigger organization needs to be done, like not everything can be done in house, that's understandable. But we need to also kind of weigh up the risks associated with automation and outsourcing and see if it's, if I guess like the gain is worth the risk that we're putting out. (Interviewee #T35Y-LX3F)

As Interviewee #Q694-3UCT shares, Canadian financial institutions are always playing a catch-up game. The fraudsters always innovate different misuses resulting in unexpected high operation volume. Interviewee #T35Y-LX3F believes that Canadian financial institutions

understand that in-house operation teams might not be able to handle the sudden surge of high operation volume.

When a fraud attack occurs, financial institutions can recalibrate their fraud detection models to identify more suspicious activity through increasingly sophisticated algorithms. Yet once these suspicious transactions are flagged, investigators and adjudicators must take on the expanded workload. Every alert requires human review, verification, and a decision, meaning that operational pressure shifts downstream to the people responsible for case handling.

However, human investigators and adjudicators have finite capacity and can only process a limited number of cases within a given period. Their availability does not automatically scale with spikes in fraud incidents. As fraud activity increases, the volume of alerts may far exceed what existing staff can manage, revealing a structural imbalance in the cyber financial crime assemblage, as algorithms can scale instantly, but human labour cannot.

Currently, to respond to a surge in case volume, fraud operations teams in Canadian financial institutions address the challenge either through a technological response or by hiring more humans to process the cases. Interviewee #YKLR-V6US comments on how fraud operations capacity could be limited. Although collaborating with the technology team could help with financial bleeding, suspending the fraud attack requires a larger team effort. Interviewee #YKLR-V6US said they and their teams often feel overwhelmed:

> So when we're getting attacked, you know, we have a fake banking website out there that is stealing members credentials and they're using those credentials like right at the moment. [The operation team] can only do so much and our IT team tries to help with that. But it's usually reactive. And you know, the damage is already kind of done at that point. But yeah, well, I definitely encountered times where I was working way more than

way more than I was paid for to try and to try and keep things on. (Interviewee #YKLR-V6US)

Additionally, Interviewee #CVN3-7UBK comments on how engaging in contractual services can help with operation costs. The business can save money when they use contractual services such as external consultants, temporary workers, or contractors overseas. In return, the business may have extra money to invest elsewhere:

> Offshoring [are at] lower cost […] definitely is a big win for the business because it gives us that extra financials to make our investments where it's needed to even further optimize our existing process. (Interviewee #CVN3-7UBK)

As a Manager of Strategic Initiatives, I work on budgeting and operational efficiency for fraud operations teams. Financial institutions constantly search for alternative solutions to handle sudden surges in case volume. The core challenge is that the fluidity of case volume produces a corresponding fluidity in labour resource requirements. While technologies can automate portions of the investigative workflow, many cases inevitably require human review, and these cannot be fully digitized or delegated to automated systems. This creates a persistent tension: if an organization overhires, human employees become excess operational costs when case volume subsides; if the organization underhires, sudden fraud attacks can overwhelm the system, leaving cases unprocessed or significantly delayed. The assemblage therefore must continually recalibrate its labour resource arrangements in response to shifting fraud patterns, illustrating its fluidity and contingency. The following section examines this fluidity of labour resources within the cyber financial crime assemblage and assesses the opportunities and risks associated with outsourcing case work.

Benefits of Engaging Contractual Services

Although there is no existing research specifically discussing the outsourcing of fraud claims adjudication within the Canadian banking sector, there is significant comparable research available regarding the impact of outsourcing in other business areas. Baldwin et al. conducted a research study to understand the risks and benefits of an organization in the UK banking sector outsourcing aspects of its information technology/information system (IT/IS) (Baldwin et al., 2001). The authors analyzed the bank's motives and decision-making processes, as well as the political perspectives and the human and organizational issues behind the scenes.

Some of the benefits of outsourcing that can be applicable to outsourcing fraud claims adjudication work in the Canadian banking industry include but are not limited to standardized and automated processes, more efficient deployment of resources, improved chargeback recovery, enhanced employee productivity, and reduced costs through economies of scale and service level agreements. However, these benefits are accompanied by important risks and governance considerations, such as the need to monitor contractor performance, maintain strong communication and executive oversight, carefully select and periodically renegotiate vendors, evaluate long-term costs and compliance obligations, and avoid over-dependence through flexible, short-term contracting arrangements and ongoing comparison with in-house capabilities (Baldwin et al., 2001).

These examples illustrate how outsourcing can be beneficial within the fluid operational dynamics of cyber financial crime management. From a business operations perspective, reducing costs remains a central priority. As labour requirements fluctuate with shifting fraud volumes, engaging contractual services and external contractors becomes a fluid, (mis)user-driven innovation that enables institutions to respond to sudden surges in case volume and

maintain operational continuity. From the customer's perspective, the main concerns are the timely progression of their cases, including when the investigation will start, when adjudication will take place, and, most importantly, when reimbursement will be issued. Outsourcing becomes a strategy for navigating these fluid demands, allowing institutions to stabilize customer-facing outcomes despite unstable and unpredictable case volumes.

I asked interview participants about their views on outsourcing investigation and adjudication work to contractual agencies, and many appeared supportive of this strategy. Interviewee #R5PL-5ST9 expresses that using contractual services to process investigation and adjudication cases helps the business to be better prepared in situations when unexpected events such as a power outage or natural disaster occur:

> Because of any reason; it can be a reason of technology outage, it can be a power outage, it can be natural reasons. So that that helps us to make sure that you know if one side goes down the other side it is still up to you know backup because this whole operation is really time sensitive and it can cost millions and millions of dollars. (Interviewee #R5PL-5ST9)
>
> So, the Big Fives are making sure that you know this operation, fraud operations, are always running and they are set at a very high priority. Outsourcing is not a bad idea. (Interviewee #R5PL-5ST9)

Interviewee #CVN3-7UBK also suggests that one of the major reasons for using contractual services in Canadian financial institutions is to ensure the business is acting in the best interests of the shareholders. The shareholders of Canadian financial institutions do not want to spend too much money on operations, so finding a cost-effective solution without jeopardizing customer experiences is important:

> We always have our bottom line, that is the shareholders. So if we keep costs low, this impacts the shareholders equity. The great thing is it's a very cost effective solution of having a vendor. (Interviewee #CVN3-7UBK)

Risks of Engaging Contractual Services

Outsourcing fraud investigation and adjudication functions to third-party contractual service providers emerges as a (mis)user-driven innovation in response to escalating fraud volumes and cost pressures. Although mobilized to improve efficiency and scalability, this operational shift introduces organizational risks. Employees in Canada may experience concerns about job security and role displacement, requiring fraud operations managers to implement structured change-management processes to manage workforce uncertainty and transition.

During this phase, fraud operations managers must address the expectations and concerns of their existing investigators and adjudicators, explaining the shift toward engaging contract workers to absorb sudden surges in operational volume. The employment relationships within the cyber financial crime assemblage are therefore also shaped by the relations of exteriority—in this case exemplified by the contractual service providers whose presence introduces new dynamics of fluidity and uncertainty.

Some employees may worry that the availability of contract services places their own positions at risk. I discussed this issue in depth with Interviewee #U9D3-AXN9, who has experience managing organizational change involving the introduction of contractual service providers:

> I mean, change management is huge. And making sure the team is informed. The rationale as to why the changes taking place. It is the biggest. You know, I think transparency is and essentially tying it to the customer experiences is pivotal. Right? A

> lot of times employees look at it and you know, opportunities lost for them or maybe a compromise of the quality being put within the actual work itself. But at the end of the day, the outcome is all for the customer. It's all to enhance the customer experience. So we don't have you know, extreme volumes (that we are not able to process). We don't have customers waiting upwards to 20 plus business days to get to get their claims adjudicated […] Tying everything back to the customer experience is evident in that change management and constantly having that communication. Not be afraid to have those difficult conversations. (Interviewee #U9D3-AXN9)

Interviewee #U9D3-AXN9 explains that the primary reason for persuading their employees was the belief that outsourcing would enhance customer service, aligning with the organization's goals. Despite concerns from existing employees about losing opportunities and potential compromises in work quality when tasks were handled by outsourced labour, the primary benefit was the reduction in customer wait times. Weighing the trade-offs, employees should be equipped to make informed decisions. Interviewee #U9D3-AXN9 said that as a manager it is important to not shy away from these difficult conversations.

In addition to concerns about job security, existing employees also worry about the data risks associated with outsourcing. Interviewee #Q694-3UCT emphasized that contractual service providers must be carefully selected and that strong operational controls are essential to protect customers' identities and other sensitive information:

> We need to ensure you know that the individuals that they are there's the level of integrity, because we are dealing with a lot of sensitive data. And we cannot wait that one day we find that you know data was leaked or there was unethical transactions that went through the thing we take measures we need to think of those and have barriers you

> know, to ensure that if we are outsourcing that, who we are outsourcing it to that they have, you know, the required level of security in terms of you know, protecting customers information, good information, and also that the people working there, they are vetted so that we ensure that everything is safe and remains confidential. (Interviewee #Q694-3UCT)

Interviewee #T35Y-LX3F is also concerned about the security risks posed by contractual service providers. Because these investigators and adjudicators are temporary vendor workers instead of internal permanent employees, they might not be able to keep certain information confidential. Given that cyber financial crime assemblages represent a high-risk profession, the associated risks are significantly elevated compared to those in more routine roles such as administrative or data entry positions:

> In terms of outsourcing, I'm not entirely sure what the process is of, I guess, like doing like background checks or anything like that. I'm not sure what the process is, but I do think it poses a security risk when you're working with I think staff or contractors that are outside of the actual internal organization. (Interviewee #T35Y-LX3F)

Although many practitioners view contractors as a welcome relief from overwhelming workloads, they also express hesitation due to the sensitivity of financial data and the potential downstream impacts should a case become uncontrolled or mishandled. I further extend my analysis with a publicly available case involving the risks and privacy concerns associated with outsourcing, in which bank employees filed complaints against financial institutions operating overseas.

On August 4, 2020, the Office of the Privacy Commissioner of Canada issued an investigation statement (PIPEDA Findings #2020-001) declaring that banks should ensure

"openness and comparable protection for personal information transferred to third party" (Office of the Privacy Commissioner of Canada, 2020). This statement is the result of a complaint that stems from a former TD employee about how TD had outsourced its fraud claims processes to a third-party processing service provider in India.

According to CBC News, former TD employee Alyson Mosher was a fraud claim agent handling tasks related to fraud claim adjudications (Johnson, 2017). There were three primary elements to Mosher's complaint: first, that TD worked with the outsourcing giant Tata Consultancy Services to hire approximately 120 contract workers in India to handle tasks formerly done by Canadian workers; second, Mosher was concerned that Canadian consumers' private information was being shared with temporary workers in India without knowledge or consent; and third, that TD was not being transparent with its customers by having offshore workers only process the cases, while still having Canadian workers answer incoming customer inquiry calls.

Three years later, the Office of the Privacy Commissioner of Canada found that TD was not required to obtain additional consent for this activity: "It was appropriately open to current and potential customers about its outsourcing. We also found that TD remained accountable for the personal information of its clients through a strong contract and monitoring approach" (Office of the Privacy Commissioner of Canada, 2020). The Office of the Privacy Commissioner of Canada also determined that TD had been accountable for maintaining a comparable level of protection for information being shared with offshore workers via a robust contract, as well as other methods such as regular audits, compliance checks, and re-visiting contractual requirements (Office of the Privacy Commissioner of Canada, 2020).

Overall, the Office of the Privacy Commissioner of Canada found each of the matters they investigated to be not well-founded. Outsourcing fraud claim investigation work to a third-party service provider is therefore acceptable in Canada as long as the process is compliant with the *Personal Information Protection and Electronic Documents Act* (PIPEDA). The ruling illustrates how accountability and liability are reconfigured rather than eliminated when operational functions move across institutional boundaries. Although investigative labour was relocated to an offshore service provider, responsibility for data protection and decision-making remained formally attached to the Canadian financial institution. This arrangement demonstrates how elements can enter and exit the cyber financial crime assemblage without fully detaching from its governance structures. In this sense, outsourcing exemplifies the fluid relations of exteriority discussed throughout this chapter: operational components may shift location, yet institutional accountability is re-articulated and stabilized through contractual, regulatory, and monitoring mechanisms.

8.5 Conclusion

In this chapter, I examined the fluidity of the cyber financial crime assemblage by tracing its shifting categorizations, relational reconfigurations, and relations of exteriority. I began by analyzing the contested liabilities that shape how fraudulent and disputed transactions are classified, and how financial losses are allocated.

I then examined the fluid boundaries of criminality by exploring how use and misuse are enacted within Canadian financial institutions.

Finally, I have illustrated how contractual service providers exemplify relations of exteriority within the cyber financial crime assemblage. Their involvement demonstrates how operational

components can enter, exit, and reconfigure investigative and adjudicative processes without being fully defined by a single institutional location, highlighting the mobility of relations through which institutional responses are organized.

Taken together, these analyses show that fluidity is a defining feature of cyber financial crime, where classifications remain unstable, investigative and adjudicative decisions shift as evidence evolves, and labour arrangements reorganize as fraud volumes rise or fall.

Chapter 9 - Conclusion

9.1 Summary

In conclusion, this dissertation offers a multifaceted examination of cyber financial crime as a dynamic and evolving sociotechnical phenomenon. Drawing on assemblage thinking within an STS theoretical orientation, the dissertation analyzes cyber financial crime as constituted through heterogeneous configurations of human and non-human actors, institutional practices, technological systems, and forms of judgment within the Canadian financial ecosystem. By mobilizing assemblage graphing and other visual analytical techniques, the dissertation makes visible the relational complexity, instability, and fluidity through which cyber financial crime is enacted, governed, and reconfigured over time.

The three primary challenges identified in this dissertation directly shaped the research objectives of the project and provide a basis for reassessing the findings. The research objectives respond to longstanding limitations in how cyber financial crime has been conceptualized, analyzed, and governed within academic scholarship and institutional practice. The first research objective was to identify and deploy an analytical framework capable of capturing the complexity of cyber financial crime. This objective addresses dominant approaches within

cybercrime, financial risk, and security literatures that emphasize bounded classifications, linear causal models, and technical controls (Grabosky et al., 2001; Levi, 2017; Ololade et al., 2020). As argued throughout the dissertation, such approaches struggle to account for heterogeneous actors, competing interpretations, affective judgments, and the continual reconfiguration of sociotechnical arrangements. By mobilizing assemblage thinking within STS, the dissertation provides a systematic and flexible framework for analyzing cyber financial crime as a phenomenon of ongoing becoming (Law, 2004; Mol, 2002).

The second research objective was to examine how cyber financial crime is defined, interpreted, and provisionally stabilized across institutional, regulatory, and organizational contexts. Definitions of cyber financial crime emerge through assemblage processes in which meanings, responsibilities, and classifications are negotiated through practice (Law & Callon, 1992). The empirical analysis shows that interpretations vary across institutional sites and professional roles, shaped by regulatory expectations, organizational incentives, technological infrastructures, and situated judgment (Briassoulis, 2017; Lysgård, 2019). Consistent with STS accounts of boundary work and credibility contests, definitional instability appears as a constitutive feature of cyber financial crime governance (Gieryn, 1983, 1999). Provisional stabilization occurs through everyday practices such as claim assessment, investigative decision-making, and policy interpretation, producing consequential effects on reporting practices, institutional priorities, and consumer outcomes (Massumi, 2021; Vertesi, 2014).

The third research objective was to analyze how (mis)user-driven innovation continually reconfigures the cyber financial crime assemblage, reshaping vulnerabilities, investigative practices, governance strategies, and institutional responses within an evolving financial ecosystem. Across the empirical chapters, the dissertation argues that users and misusers actively

adapt, repurpose, resist, and exploit digital financial technologies in response to institutional controls and design constraints. These findings align with STS and innovation scholarship emphasizing the co-production of users, technologies, and governance arrangements (Oudshoorn & Pinch, 2003; von Hippel, 2005). Adaptive practices reorganize relations within the assemblage and prompt iterative institutional responses, including product redesign, policy adjustment, and the deployment of automated systems and detachable resources. Governance emerges through these interactions as an ongoing and contingent process shaped by (mis)user-driven innovation (Jensen, 2012; Latzko-Toth et al., 2019; Söderberg, 2010).

Revisiting the research aims underscores the contribution of this dissertation to reconceptualizing cyber financial crime as a dynamic sociotechnical phenomenon. By deploying an assemblage-based analytical framework, examining processes of definition and stabilization in practice, and tracing the productive role of (mis)user-driven innovation, the project advances an understanding of cyber financial crime governance attentive to complexity, multiplicity, affectivity, and continual reconfiguration.

9.2 Key Theoretical Contribution and Empirical Findings

This dissertation contributes to existing scholarship in three key ways. First, it challenges dominant and often reductive understandings of cyber financial crime by demonstrating how definitions, classifications, and institutional responses are neither fixed nor uniform but are shaped through practice and interpretation. Rather than treating cyber financial crime as a stable object of governance, the analysis shows how meanings of use, misuse, responsibility, and harm are continually negotiated.

Second, the dissertation develops an assemblage-based analytical tool grounded in four sensitizing characteristics—heterogeneity, multiplicity, affectivity, and fluidity—which together offer a systematic yet flexible way of examining cyber financial crime without reducing it to linear stages, isolated actors, or purely technical failures.

Third, the dissertation demonstrates the analytical value of this tool through sustained empirical analysis. Drawing on document analysis and 24 semi-structured interviews with fraud industry practitioners working in Canadian financial institutions, the empirical chapters apply the four characteristics to examine how cyber financial crime emerges through everyday operational practices, technological design decisions, institutional priorities, and user and misuser interactions. Across the empirical cases, (mis)user-driven innovation emerges as a central force that continuously reshapes financial technologies, governance arrangements, and risk assumptions, underscoring cyber financial crime as a phenomenon of ongoing becoming rather than one amenable to definitive resolution.

To sum up, this dissertation advances an assemblage-oriented approach that captures the complexity, contingency, and productivity of cyber financial crime. By refusing static definitions and linear explanations, it opens analytical space for understanding how cyber financial crime is continually made and remade through sociotechnical relations, and how governance responses themselves participate in this process. The framework developed here is therefore not intended as a closed or final model, but as an adaptable analytical resource capable of evolving alongside the shifting configurations of cyber financial crime.

Across the dissertation, particular attention is paid to (mis)user-driven innovation as a productive force within the cyber financial crime assemblage. Drawing on STS scholarship that emphasizes the co-production of technology, users, and governance arrangements, the analysis

shows how users and misusers actively adapt, repurpose, and reinterpret digital financial technologies in response to institutional controls, design frictions, and everyday financial needs (Oudshoorn & Pinch, 2003; von Hippel, 2005). These adaptive practices not only enable new forms of financial participation but also generate novel vulnerabilities, governance challenges, and institutional responses. In this sense, cyber financial crime emerges not simply from technical weaknesses or criminal intent, but through the ongoing reconfiguration of sociotechnical relations shaped by both legitimate and illicit forms of innovation.

Consistent with STS accounts of boundary work and credibility contests, the dissertation's empirical findings show that distinctions between use and misuse, as well as determinations of responsibility, harm, and legitimacy, are neither fixed nor universally applied (Gieryn, 1983, 1999). Instead, they are negotiated dynamically, shaped by economic pressures, regulatory expectations, organizational incentives, professional experience, and the interpretive frameworks mobilized by institutional actors. Cyber financial crime governance thus operates less as the application of stable rules and more as an ongoing process of negotiation across multiple sites and actors (Law & Callon, 1992).

The findings regarding power must also be interpreted in relation to the empirical standpoint of the study and the structuring role of financial institutions within the cyber financial crime assemblage. Because the research examines cyber financial crime primarily through Canadian financial institutions and industry practitioners, it provides particularly detailed insight into how these institutions configure internal processes, deploy technologies, define risk, allocate responsibility, and organize responses to cyber financial crime. In doing so, the analysis shows that financial institutions are not merely one set of actors among others within a neutral field of

relations, but are key sites through which the cyber financial crime assemblage is actively structured, stabilized, and made operational.

At the same time, this institutional centrality also shapes what forms of power become most visible in the analysis. The dissertation exemplifies how financial institutions exercise power through their capacity to define fraud categories, design authentication systems, implement monitoring and detection infrastructures, and determine thresholds for intervention and escalation. These capacities influence how other components of the assemblage—customers, technologies, regulatory requirements, and misusers—are positioned, interpreted, and connected within institutional responses to cyber financial crime. However, because the empirical material is primarily generated from within financial institutions, the analysis does not fully capture how these institutional configurations are experienced, resisted, or reconfigured by actors situated outside the financial sector.

The dissertation therefore does not claim to provide a comprehensive mapping of power across the entire cyber financial crime assemblage. Instead, it demonstrates how financial institutions, through their privileged access to data, technological infrastructures, regulatory interfaces, and operational decision-making, play a constitutive role in shaping the organization and boundaries of the assemblage itself. The analysis of power is thus necessarily partial and institutionally situated: it highlights how financial institutions structure key relations within the assemblage, while also acknowledging that a fuller account of power would require greater empirical access to the perspectives and practices of non-institutional actors and to the broader political-economic conditions that shape these institutional capacities.

9.3 Industry Implications: Governing Cyber Financial Crime as an Evolving Assemblage

This dissertation argues that cyber financial crime cannot be effectively managed through static controls, linear risk models, or purely technical interventions. Instead, it shows that cyber financial crime is continually produced and reconfigured through the interactions of heterogeneous actors, technologies, institutional practices, and (mis)user-driven innovation within the Canadian financial ecosystem. This reconceptualization carries important implications for industry practitioners, as it calls for a rethinking of how cyber financial crime is understood, governed, and operationalized in practice.

Building on the empirical findings, this section outlines three industry implications that warrant critical attention if financial institutions are to manage cyber financial crime as an evolving assemblage. These implications concern: (1) recognizing (mis)user-driven innovation as a productive force and addressing the limits of reactive governance strategies; (2) rethinking boundaries of responsibility, liability, and fault; and (3) ensuring decision consistency across detachable decision-making resources, including automated systems and contracted services.

First, one of the central strengths of an assemblage-based approach lies in its capacity to accommodate ongoing change. As cyber financial crime evolves alongside digital financial products, payment infrastructures, automation tools, and shifting regulatory expectations, governance frameworks cannot be oriented toward definitive or permanent solutions. Instead, they must remain responsive to processes of becoming through which new vulnerabilities, practices, and interpretations are enacted.

Across this dissertation, (mis)user-driven innovation is traced through a range of sociotechnical reconfigurations, such as the evolving legal definitions of cyber financial crime

and associated regulatory requirements; enhanced authentication strategies to reduce fraud and scams; and the integration of automated systems to streamline detection, investigation, and adjudication. These examples demonstrate that innovation is not confined to technological artefacts but is distributed across legal, organizational, operational, and interpretive domains.

The analytical framework developed in this dissertation is therefore not a closed model but a flexible resource that enables institutions to examine how emerging technologies, organizational restructurings, and shifting user practices reconfigure existing arrangements of risk, responsibility, and trust. This adaptive capacity is particularly valuable in environments characterized by rapid innovation and persistent uncertainty. From an industry perspective, this suggests the need for dedicated research and development functions that explicitly engage with (mis)user-driven innovation as an internal dynamic of governance, rather than treating it as an external disruption or anomalous source of risk.

Second, the findings indicate that effective governance of cyber financial crime requires sustained attention to how boundaries of responsibility, liability, and fault are continually drawn and redrawn in practice. Industry decisions concerning prioritization, remediation, automation, and customer treatment are shaped not only by technical risk assessments but also by institutional interpretations of responsibility and accountability. These boundaries are neither fixed nor reducible to formal legal thresholds; rather, they evolve as (mis)user-driven innovation reconfigures the assemblage and introduces new relations of action, harm, and contestation.

Across the empirical chapters, the dissertation shows how the fluidity of investigative judgments produces corresponding fluidities in the boundaries of criminality. The coexistence of use and misuse within everyday financial practices complicates categorical distinctions between legitimate users, negligent actors, and criminal offenders, resulting in shifting approaches to

customer treatment, reimbursement, and remediation. Investigative determinations are enacted through sociotechnical arrangements that combine automated assessments, institutional policies, and human discretion, each of which contributes to how responsibility and fault are provisionally stabilized within specific cases.

By conceptualizing governance as an ongoing process of adjustment and negotiation, this dissertation offers industry practitioners a lens for understanding responsibility and liability as emergent and relational outcomes rather than stable policy endpoints. From an industry perspective, this highlights the importance of critically examining how investigative practices, automation strategies, and loss allocation frameworks participate in boundary-making processes, and how these processes, in turn, shape institutional accountability and customer trust.

Finally, the analysis highlights the importance of aligning decision consistency across detachable decision-making resources, including automated mechanisms and external contractors engaged in investigation and adjudication. As the findings demonstrate, investigative and adjudicative work is increasingly distributed across frontline employees, algorithmic systems, and third-party service providers. While these detachable components enable institutions to manage operational volume, cost, and efficiency, they also introduce the possibility of divergent interpretations, thresholds, and outcomes across otherwise comparable cases. Consistency within such distributed arrangements is therefore not merely an operational concern but a core governance obligation that shapes how responsibility, fairness, and accountability are enacted in practice.

Across the empirical chapters, the dissertation shows how automated decision logics and contractual services participate in the assemblage not as neutral tools but as affective and interpretive actors that stabilize certain judgments while obscuring others. Variations in training,

system calibration, contractual incentives, and case framing can amplify inconsistencies over time, particularly when automated decisions are scaled or externalized. Although continuous training, system updates, and governance oversight require sustained investment, the risks of unmanaged inconsistency are more consequential in the long term. An assemblage-based approach therefore invites financial institutions to critically examine how decisions are formulated, reinforced, and rationalized across heterogeneous sites of action and to treat alignment itself as an ongoing sociotechnical accomplishment rather than a one-time compliance exercise.

To sum up, by mobilizing an assemblage-based analytical framework structured around heterogeneity, multiplicity, affectivity, and fluidity, this research provides industry practitioners with a systematic way to examine cyber financial crime beyond compliance checklists or isolated fraud typologies. It offers a means to engage cyber financial crime governance as a dynamic and ongoing process shaped by sociotechnical relations and (mis)user-driven innovation. In doing so, it encourages institutions to reflect on how their own practices, technologies, and interpretive decisions actively participate in producing the phenomena they seek to manage. This orientation opens space for more reflexive, adaptive, and context-sensitive forms of governance capable of responding to evolving configurations of risk, responsibility, and trust.

9.4 Policy Implications: Claims, Crimes, and Knowledge

Throughout this dissertation, cyber financial crime is shown to be continuously shaped by perceptions, knowledge practices, and decision-making processes that operate across institutional boundaries. These processes do not merely respond to cyber financial crime; they actively participate in its ongoing production, stabilization, and reconfiguration. Building on these

insights, this section outlines three policy implications that policymakers, academic scholars, and institutional actors should critically consider: (1) the need to critically unpack claims about cyber financial crime; (2) the importance of incorporating fluidity and multiplicity into criminological and policy dialogues; and (3) the necessity of constructing more democratic forms of knowledge about cyber financial crime to support sustainable governance and cyber defence.

First, this dissertation argues that claims about cyber financial crime made by Canadian financial institutions require careful and sustained scrutiny. From an STS perspective, claims are not neutral descriptions of reality but are shaped by underlying assumptions, institutional interests, and networks of influence (Law & Callon, 1992). Critically unpacking such claims involves examining how cyber financial crime is defined by different actors within the assemblage, tracing the origins of dominant understandings, interrogating assumptions embedded in pay-or-decline decisions, and assessing the forms of evidence mobilized to justify reimbursement guidelines. Attention to language and rhetoric is particularly important, as financial service agreements often define victimization in narrow ways and frame mobile financial losses as boundary objects that separate legitimate crime from misuse.

While regulatory bodies such as the Financial Consumer Agency of Canada establish consumer protection requirements, including reimbursement mandates for unauthorized transactions, not all reported fraud incidents are reimbursed in practice. Financial institutions rely heavily on unilateral financial service agreements to distinguish proper use from misuse of financial products and services. Investigators and adjudicators interpret reported cases through these agreements, often in combination with customer profiles, perceived financial resilience, risk indicators, and prior victimization histories, to determine whether an incident qualifies as criminal. Two key policy concerns arise from this arrangement.

The first significant policy concern is the lack of diversity in participation during the drafting of financial service agreements. These agreements are often created unilaterally by financial institutions, which leads to minimal meaningful involvement or negotiation from users. This limited engagement can affect the fairness and accessibility of the agreements for users. As a result, these documents function less as neutral legal frameworks and more as institutional instruments that predefine the terms under which responsibility and legitimacy are evaluated. Users typically encounter these agreements through standardized acceptance procedures, meaning their role is not to help co-construct the rules but rather to be positioned within them. As a result, the contractual framework stabilizes institutional interpretations of use and misuse while constraining the capacity of users to contest how their actions are classified. This asymmetry shapes how cyber financial crime is defined in practice, as contractual clauses become key devices through which institutional judgments are anchored.

Second, the discretionary interpretation of ambiguous contractual language creates a fluid boundary around cyber financial crime, which varies across different cases and institutional contexts. Terms like “reasonable care,” “authorized use,” and “negligence” are not inherently clear; their meanings are shaped through case-by-case assessments that rely on evidence, behavioural expectations, and institutional risk considerations. As a result, the same contractual clause can lead to different outcomes depending on the unique combination of actors, data, and organizational pressures involved. Criminality is not merely identified through the agreement; it is constructed through its interpretation. This discretionary space allows for flexibility in responding to various scenarios, but it also introduces variability in how responsibility, victimhood, and liability are assigned. This reveals how legal, technical, and organizational factors work together to create the shifting landscape of cyber financial crime.

The next policy implication highlights the opportunity for criminological and policy approaches to cyber financial crime to enhance their effectiveness by integrating the dimensions of fluidity and multiplicity. This integration could lead to more robust strategies in addressing the complexities of such crimes. Existing frameworks, including the Conjunction of Criminal Opportunity (CCO) model, offer valuable insights into offender motivation, resources, target suitability, and environmental conditions (Clarke & Felson, 2017; Cornish & Clarke, 2014; Ekblom, 1994). However, such models tend to presume relatively stable configurations of crime and opportunity. The empirical evidence presented in this dissertation shows that cyber financial crime is enacted through multiple, coexisting realities that change across technological platforms, institutional processes, and interpretive contexts. Without accounting for this multiplicity and fluidity, policy interventions risk oversimplifying the phenomenon and overlooking how criminality, victimization, and responsibility are continually negotiated in practice.

Incorporating these dimensions encourages a move away from static risk categories and toward adaptive, relational forms of governance. Policies could be designed to recognize that the same transaction, actor, or technological trace may be interpreted differently as relations change, requiring mechanisms for ongoing reassessment rather than one-time classification. This approach supports regulatory and institutional practices that remain responsive to emerging tactics, evolving user behaviours, and shifting organizational constraints. It also foregrounds the need for coordination across technical, legal, and organizational domains, since interventions in one area inevitably reshape conditions in others. By treating cyber financial crime as a fluid and multiple phenomenon, policy can better address the dynamic processes through which harms, responsibilities, and institutional responses are continuously reconfigured.

Finally, this dissertation highlights the importance of democratizing knowledge production about cyber financial crime. Stability and social order within sociotechnical networks depend on the alignment and translation of interests among human and non-human actors (Callon, 1998). At present, governance processes related to cyber financial crime—such as drafting cardholder agreements, designing reimbursement guidelines, and adjudicating consumer complaints—are largely dominated by industry experts and institutional actors. This concentration of situated knowledge positions financial institutions as authoritative arbiters whose decisions are difficult for outsiders to challenge. The resulting separation between "expert" and "public" knowledge risks undermining democratic and scientific governance (Jasanoff, 1999, 2003; Jensen, 2012).

The policy implication advanced here is the need to construct cyber financial crime as a democratic boundary object, one that allows broader public participation in shaping how crime, misuse, and responsibility are defined. This includes creating institutional mechanisms that enable consumers to participate meaningfully in the development and revision of cardholder agreements, reimbursement policies, and complaint-handling processes. Such participation would not eliminate conflict or disagreement, but it could reduce asymmetries of power and knowledge that currently place consumers in structurally vulnerable positions.

At the same time, this dissertation identifies two challenges associated with democratizing cyber financial crime governance. First, meaningful participation may be constrained by institutions' reliance on confidential digital evidence, proprietary fraud detection systems, and opaque adjudication criteria, which limit public access to relevant knowledge. Second, increased transparency may introduce new risks of exploitation, as (mis)users could leverage disclosed criteria or decision logics to manipulate institutional processes. These tensions

underscore the need for careful policy design that balances transparency, accountability, and security, rather than treating democratization as a purely technical solution.

Taken together, these policy implications call for a shift in how cyber financial crime is governed—from a model centred on unilateral claims, static classifications, and expert exclusivity toward one that recognizes cyber financial crime as a fluid, multiple, and collectively negotiated phenomenon.

9.5 Future Research Directions

As cyber financial crime continues to evolve, this dissertation lays the groundwork for future research by identifying key components and dynamics within dynamic cyber financial crime assemblages. Building on the empirical and theoretical insights developed throughout the study, this final section outlines several future research directions. These directions are organized into three broad categories that reflect distinct yet interconnected assemblages within the cyber financial crime ecosystem.

The first research direction concerns vulnerabilities and exploitation processes. Future research could further examine how different forms of vulnerability are assembled and targeted, including technological vulnerabilities, human vulnerabilities, physical security risks, and insider threats. Scholars may investigate how specific technologies, institutional policies, and governance strategies are mobilized to exploit or mitigate these vulnerabilities, as well as how such interventions differentially shape patterns of victimization and financial loss. Integrating empirical data on loss magnitude and victim impact would allow researchers to assess which vulnerabilities generate the greatest harm, thereby informing more strategic prioritization of technological and policy investments.

The second research direction focuses on investigation and adjudication processes within cyber financial crime assemblages. Future research could productively integrate the CCO framework to examine how heterogeneous human and non-human actors—such as investigators, automated systems, contractual service providers, evidentiary artefacts, and institutional policies—jointly shape the organization and outcomes of investigative and adjudicative practices. Rather than treating criminal opportunity as a fixed situational condition, such an approach would allow scholars to examine how criminal opportunities are enacted, stabilized, and transformed through distributed decision-making processes. By situating the CCO model within an assemblage-based analysis, future studies could trace how investigative priorities, evidentiary thresholds, and liability determinations emerge from the interaction between technological infrastructures, organizational logics, and human judgment. This line of inquiry would deepen understanding of how investigative and adjudicative processes not only respond to cyber financial crime but actively participate in reconfiguring the assemblage itself.

The third research direction centres on cybervictimization. While monetary reimbursement is often treated as the primary mechanism for restoring customer relationships, this dissertation suggests that reparations extend well beyond financial compensation. Victims of cyber financial crime may experience psychological distress, physiological effects, and long-term erosion of trust in both digital technologies and financial institutions. These harms are particularly pronounced in cases such as investment scams, romance scams, employment scams, and other frauds that mobilize affective forces including greed, loneliness, and urgency, and are frequently compounded by post-incident shame, self-blame, and depression. At present, few actors within either public or non-public sectors address these affective and relational harms in a systematic or sustained manner. Future research could examine how victim services might be

integrated into cyber financial crime governance, including mechanisms for psychological support, trust repair, and institutional accountability. In line with the policy implications discussed earlier, inviting cyber financial crime victims to participate as stakeholders in reshaping cyber financial crime assemblages presents a particularly promising avenue for future research, especially from a policy-oriented perspective in this AI-driven world.

By pursuing these research directions, scholars, policymakers, and industry practitioners can deepen collective understanding of cyber financial crime and contribute to the development of more reflexive, equitable, and sustainable approaches to its governance within an evolving financial ecosystem.

References

Abbate, J. (2000). *Inventing the internet.* MIT Press.

Abraham, J., & Sheppard, J. (1997). Democracy, technocracy, and the secret state of medicines control: Expert and nonexpert perspectives. *Science, Technology, & Human Values*, *22*(2), 139–167. https://doi.org/10.1177/016224399702200201

Acuto, M., & Curtis, S. (2014). Assemblage thinking and international relations. In M. Acuto & S. Curtis (Eds.), *Reassembling international theory* (pp. 1–15). Palgrave Pivot. https://doi.org/10.1057/9781137383969

Adams, W. C. (2015). Conducting semi-structured interviews. In K. E. Newcomer, H. P. Hatry, & J. S. Wholey (Eds.), *Handbook of practical program evaluation* (pp. 492–505). Wiley. https://doi.org/10.1002/9781119171386

Adrian, T., & Mancini-Griffoli, T. (2019). The rise of digital money. *FinTech Notes*, *2019*(001). https://doi.org/10.5089/9781498324908.063

Ajayi, E. F. G. (2016). The challenges to enforcement of cyber-crimes laws and policy. *Journal of Internet and Information Systems*, *6*(1), 1–12. https://doi.org/10.2139/ssrn.2612389

Akers, R. L. (2017). Rational choice, deterrence, and social learning theory in criminology: The path not taken. In M. Natarajan (Ed.), *Crime Opportunity Theories* (1st ed., pp. 299–322). Routledge. https://doi.org/10.4324/9781315095301-14

Akhgar, B., Gercke, M., Vrochidis, S., & Gibson, H. (Eds.). (2021). *Dark web investigation.* Springer International Publishing. https://doi.org/10.1007/978-3-030-55343-2

AltexSoft. (2018, November 14). How to choose fraud detection software: Features, characteristics, key providers. *AltexSoft.* https://www.altexsoft.com/blog/business/how-to-choose-fraud-detection-software-features-characteristics-key-providers/

Altheide, D. L. (1996). *Qualitative media analysis.* Sage Publications. https://doi.org/10.4135/9781412985536

Amato, D. (2018, October 16). *Five simple steps to hack-proof your passwords.* Discover & learn. *RBC.* https://discover.rbcroyalbank.com/five-simple-steps-to-hack-proof-your-passwords/

Anderson, B., Kearnes, M., McFarlane, C., & Swanton, D. (2012). On assemblages and geography. *Dialogues in Human Geography*, *2*(2), 171–189. https://doi.org/10.1177/2043820612449261

Anderson, B., & McFarlane, C. (2011). Assemblage and geography. *Area*, *43*(2), 124–127. https://doi.org/10.1111/j.1475-4762.2011.01004.x

Andrews, N. (2018). Can I get your digits: Illegal acquisition of wireless phone numbers for sim-swap attacks and wireless provider liability. *Northwestern Journal of Technology and Intellectual Property*, *16*, 79.

Anesa, P. (2022). Fighting cybercrime through linguistic analysis. In V. Guillén-Nieto & D. Stein (Eds.), *Language as evidence: Doing forensic linguistics* (pp. 419–438). Springer International Publishing. https://doi.org/10.1007/978-3-030-84330-4_12

Arimoto, T., & Sato, Y. (2012). Rebuilding public trust in science for policy-making. *Science*, *337*(6099), 1176–1177. https://doi.org/10.1126/science.1224004

ASEAN. (n.d.). Cyber Security. *ASEAN Main Portal*. https://asean.org/our-communities/asean-political-security-community/peaceful-secure-and-stable-region/cyber-security/

Ashton, M. (2017). Debugging the real world: Robust criminal prosecution in the internet of things. *Arizona Law Rev.*, *59*, 805.

Australian Competition and Consumer Commission. (2018, January 5). Types of scams. Australian Competition and Consumer Commission. https://www.scamwatch.gov.au/types-of-scams

Bader, L., Bürger, J. C., Matzutt, R., & Wehrle, K. (2018). Smart contract-based car insurance policies. *2018 IEEE Globecom Workshops (GC Wkshps)*, 1–7. https://doi.org/10.1109/glocomw.2018.8644136

Baker, T., & McGuirk, P. (2017). Assemblage thinking as methodology: Commitments and practices for critical policy research. *Territory, Politics, Governance*, *5*(4), 425–442. https://doi.org/10.1080/21622671.2016.1231631

Baldwin, L. P., Irani, Z., & Love, P. E. D. (2001). Outsourcing information systems: Drawing lessons from a banking case study. *European Journal of Information Systems*, *10*(1), 15–24. https://doi.org/10.1057/palgrave.ejis.3000372

Barad, K. (2007). *Meeting the universe halfway: Quantum physics and the entanglement of matter and meaning*. Duke University Press.

Barn, R., & Barn, B. (2016). *An ontological representation of a taxonomy for cybercrime.* Middlesex University. https://eprints.mdx.ac.uk/19205/1/ECIS2016-submission-CAMERA-READY-FINAL.pdf

Barr, L. (2022, January 20). FBI warns criminals are using fake QR codes to scam users. *ABC News*. https://abcnews.go.com/Politics/fbi-warns-criminals-fake-qr-codes-scam-users/story?id=82371866

Barrett, J. C. (2013). The archaeology of mind: It's not what you think. *Cambridge Archaeological Journal*, *23*(1), 1–17. https://doi.org/10.1017/s0959774313000012

Bartman-Gatt, A. (1990). Expert systems in data processing: California travel expense claim system. *Proceedings [1990]. IEEE Conference on Managing Expert System Programs and Projects*, 176-185. https://doi.org/10.1109/mespp.1990.122704

Beda, Z., Smith, S. M., & Orr, J. (2020). Creativity on demand – Hacking into creative problem solving. *NeuroImage*, *216*, 116867. https://doi.org/10.1016/j.neuroimage.2020.116867

Beirne, P. (1987). Adolphe Quetelet and the origins of positivist criminology. *American Journal of Sociology*, *92*(5), 1140–1169. https://doi.org/10.1086/228630

Bennet, J. (2005). The agency of assemblages and the North American blackout. *Public Culture*, *17*(3), 445-466. https://doi.org/10.1215/08992363-17-3-445

Berger, A. A. (1992). *Media analysis techniques*. Sage Publications.

Bijker, W. E., Hughes, T. P., & Pinch, T. J. (1987). *The social construction of technological systems: New directions in the sociology and history of technology*. MIT Press.

Blaikie, N., & Priest, J. (2019). *Designing social research: The logic of anticipation.* John Wiley & Sons.

Blok, A. (2013). Urban green assemblages. *Science & Technology Studies*, *26*(1), 5–24. https://doi.org/10.23987/sts.55306

Blumer, H. (1954). What is wrong with social theory? *American Sociological Review, 19*(1), 3–10.

Blumer, H. (1969). *Symbolic interactionism: Perspective and method. University of California Press.*

BMO. (n.d.-a). Lock/unlock your credit card. https://bmodemos.com/en/course/start/public-lock-unlock-your-credit-card-mobile/emulator-lock-unlock-your-credit-card-mobile/emulator

BMO. (n.d.-b). Scams alerts: Learn what to look for—BMO Canada. https://www.bmo.com/main/personal/ways-to-bank/security-centre/scam-alerts/

BMO. (2023a). *Electronic banking and services agreement.* https://www.bmo.com/en-ca/main/personal/electronic-service-agreement/

BMO. (2023b). Online security. https://www.bmo.com/self-directed/popups/online-security#--tabs-1675597791900-

Bose, S., Dong, G., & Simpson, A. (2019). *The financial ecosystem.* Springer.

Bowen, G. A. (2006). Grounded theory and sensitizing concepts. *International Journal of Qualitative Methods*, *5*(3), 12–23. https://doi.org/10.1177/160940690600500304

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, *9*(2), 27–40. https://doi.org/10.3316/qrj0902027

Brammer, S., Jackson, G., & Matten, D. (2012). Corporate social responsibility and institutional theory: New perspectives on private governance. *Socio-Economic Review*, *10*(1), 3–28. https://doi.org/10.1093/ser/mwr030

Brach, B. (2017, October 10). TD Bank customer frustrated with fraud investigation leaving him owing thousands. *CBC News.* https://www.cbc.ca/news/canada/british-columbia/td-customer-fraud-unhappy-1.4341899

Branch, J. (2021). What's in a name? Metaphors and cybersecurity. *International Organization*, *75*(1), 39–70. https://doi.org/10.1017/s002081832000051x

Braune, K., Lal, R. A., Petruželková, L., Scheiner, G., Winterdijk, P., Schmidt, S., Raimond, L., Hood, K. K., Riddell, M. C., Skinner, T. C., Raile, K., & Hussain, S. (2022). Open-source automated insulin delivery: International consensus statement and practical guidance for health-care professionals. *The Lancet Diabetes & Endocrinology*, *10*(1), 58–74. https://doi.org/10.1016/S2213-8587(21)00267-9

Brenner, N., Madden, D. J., & Wachsmuth, D. (2011). Assemblage urbanism and the challenges of critical urban theory. *City*, *15*(2), 225–240. https://doi.org/10.1080/13604813.2011.568717

Briassoulis, H. (2017). Tourism destinations as multiplicities: The view from assemblage thinking. *International Journal of Tourism Research*, *19*(3), 304–317. https://doi.org/10.1002/jtr.2113

Briassoulis, H. (2019). Governance as multiplicity: The assemblage thinking perspective. *Policy Sciences*, *52*(3), 419–450. https://doi.org/10.1007/s11077-018-09345-9

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management, 29*(3), 408–433. https://doi.org/10.1108/13639510610684674

Brown, H. (2002). Abuse of people with learning disabilities: Layers of concern and analysis. *Institutional Abuse*, 101–121.

Brown, M. B. (2015). Politicizing science: Conceptions of politics in science and technology studies. *Social Studies of Science, 45*(1), 3–30.

Brown, S. (2006). The criminology of hybrids: Rethinking crime and law in technosocial networks. *Theoretical Criminology, 10*(2), 223–244. https://doi.org/10.1177/1362480606063140

Buchanan, I. (2015). Assemblage theory and its discontents. *Deleuze Studies, 9*(3), 382–392. https://doi.org/10.3366/dls.2015.0193

Bulakh, V., & Gupta, M. (2015). Characterizing credit card black markets on the web. *Proceedings of the 24th International Conference on World Wide Web*, 1435–1440. https://doi.org/10.1145/2740908.2778846

Buser, M. (2014). Thinking through non-representational and affective atmospheres in planning theory and practice. *Planning Theory, 13*(3), 227–243. https://doi.org/10.1177/1473095213491744

Bush, D. (2016). How data breaches lead to fraud. *Network Security, 2016*(7), 11–13. https://doi.org/10.1016/s1353-4858(16)30069-1

Button, M., & Cross, C. (2017). *Cyber frauds, scams and their victims* (1st ed.). Routledge. https://doi.org/10.4324/9781315679877

Callon, M. (1986). The Sociology of an actor-network: The case of the electric vehicle. In M. Callon, J. Law, & A. Rip (Eds.), *Mapping the dynamics of science and technology: Sociology of science in the real world* (pp. 19–34). Palgrave Macmillan UK. https://doi.org/10.1007/978-1-349-07408-2_2

Callon, M. (1998). Some elements of translation: Domestication of scallops and the fishermen of St. Brieuc Bay. In M. Biagioli (Ed.), *The science studies reader* (pp. 67–83). Routledge.

Callon, M. (1999). The role of lay people in the production and dissemination of scientific knowledge. *Science, Technology and Society,* 4(1), 81-94. https://doi.org/10.1177/097172189900400106

Callon, M., & Rabeharisoa, V. (2003). Research “in the wild” and the shaping of new social identities. *Technology in Society*, *25*(2), 193–204. https://doi.org/10.1016/s0160-791x(03)00021-6

Canada Mortgage and Housing Corporation. (2018, March 13). Mortgage fraud: What you need to know. https://www.cmhc-schl.gc.ca/en/consumers/owning-a-home/mortgage-management/mortgage-fraud

Canadian Anti-Fraud Centre. (2020, January 31). About the Canadian Anti-fraud Centre. https://www.antifraudcentre-centreantifraude.ca/about-ausujet/index-eng.htm

Canadian Anti-Fraud Centre. (2022). *Canadian Anti-Fraud Centre annual report 2021*. Royal Canadian Mounted Police. https://publications.gc.ca/collections/collection_2022/grc-rcmp/PS61-46-2021-eng.pdf

Canadian Anti-Fraud Centre. (2023, February 1). Frauds by medium. *Government of Canada*. https://antifraudcentre-centreantifraude.ca/scams-fraudes/medium-moyen-eng.htm

Canadian Bankers Association. (2021, June 1). “Tap to pay” card security—An FAQ. https://cba.ca/tap-to-pay-card-security-an-faq

Canadian Centre for Cyber Security. (2020, April 6). Don’t take the bait: Recognize and avoid phishing attacks - ITSAP.00.101. https://www.cyber.gc.ca/en/guidance/dont-take-bait-recognize-and-avoid-phishing-attacks

Canadian Centre for Cyber Security. (2022a, May 15). Industry collaboration. *Government of Canada*. https://cyber.gc.ca/en/about-cyber-centre/industry-collaboration

Canadian Centre for Cyber Security. (2022b, October 28). An introduction to the cyber threat environment. *Government of Canada*. https://cyber.gc.ca/en/guidance/introduction-cyber-threat-environment

Canadian Centre for Cyber Security. (2025, October 31). Report a cyber incident: Individuals. *Government of Canada*. https://www.cyber.gc.ca/en/incident-management/report-cyber-incident-individuals

Capital One. (2022, April 22). 2019 Capital One cyber incident | What happened. Capital One. https://www.capitalone.com/digital/facts2019/

Capital One. (2023a). Capital One data breach—Home. https://www.capitalonesettlement.com/en

Capital One. (2023b). *Responsible disclosure program*. Capital One. https://www.capitalone.com/digital/responsible-disclosure/

Carter, D. (2018). Reimagining the big data assemblage. *Big Data & Society*, *5*(2), 2053951718818194. https://doi.org/10.1177/2053951718818194

CBC News. (2019, October 24). Police warn Calgarians about "shoulder-surfing" scam. https://www.cbc.ca/news/canada/calgary/theft-incident-scam-shoulder-surfing-distraction-crime-arrest-1.5334250

CBS News. (2022, June 8). 2 million affected by Shields Health Care Group cyberattack. https://www.cbsnews.com/boston/news/shields-health-care-group-data-breach-cyber-attack-massachusetts/

Chandra, A., & Snowe, M. J. (2020). A taxonomy of cybercrime: Theory and design. *International Journal of Accounting Information Systems*, *38*, 100467. https://doi.org/10.1016/j.accinf.2020.100467

Chargeback Gurus. (2020, November 24). Don't fall victim to fraud from botnet attacks. https://www.chargebackgurus.com/blog/botnet-fraud

Chargeback Gurus. (2021a, May 7). How to use velocity checks as an effective fraud ool. https://www.chargebackgurus.com/blog/velocity-checks

Chargeback Gurus. (2021b, May 23). Visa trial and subscription mandate explained. https://www.chargebackgurus.com/blog/visa-trial-and-subscription-mandate-explained

Chargeback Gurus. (2021c, October 2). Getting familiar with merchant fraud. https://www.chargebackgurus.com/blog/merchant-fraud

Chargeback Gurus. (2021d, October 6). Preventing fraud with behavioral analytics. https://www.chargebackgurus.com/blog/behavioral-analytics

Chargebacks911. (2022, November 15). Bust-out fraud: When patient criminals "take the long view." https://chargebacks911.com/bust-out-fraud/

Chargebacks911. (2023). What happens if you file a false chargeback claim? https://chargebacks911.com/false-chargeback-claims/

Chatain, P.-L., Herndez-Coss, R., Borowik, K., & Zerzan, A. (2008). *Integrity in mobile phone financial services: Measures for mitigating the risks from money laundering and terrorist financing. The World Bank.* https://doi.org/10.1596/978-0-8213-7556-3

CheckPoint Research. (2019, December 23). Canadian banks targeted in a massive phishing campaign. https://research.checkpoint.com/2019/canadian-banks-targeted-in-a-massive-phishing-campaign/

Cheng, D., Wang, X., Zhang, Y., & Zhang, L. (2020). Graph neural network for fraud detection via spatial-temporal attention. *IEEE Transactions on Knowledge and Data Engineering*, *34*(8), 3800–3813. https://doi.org/10.1109/tkde.2020.3025588

Chertoff, M. (2017). A public policy perspective of the dark web. *Journal of Cyber Policy*, *2*(1), 26–38. https://doi.org/10.1080/23738871.2017.1298643

Chhotray, V., & Stoker, G. (2009). Governance: From theory to practice. In V. Chhotray & G. Stoker, (Eds.). *Governance theory and practice: A cross-disciplinary approach* (pp. 214–247). Palgrave Macmillan UK.

Choi, K.-S., & Lee, J. R. (2017). Theoretical analysis of cyber-interpersonal violence victimization and offending using cyber-routine activities theory. *Computers in Human Behavior*, *73*, 394–402. https://doi.org/10.1016/j.chb.2017.03.061

Christou, G. (2018). The challenges of cybercrime governance in the European union. *European Politics and Society*, *19*(3), 355–375. https://doi.org/10.1080/23745118.2018.1430722

CIBC. (n.d.-a). Debit and credit card fraud alerts. https://www.cibc.com/en/privacy-security/fraud-alerts.html

CIBC. (n.d.-b). Examples of fraud and scams. https://www.cibc.com/en/privacy-security/fraud-examples/fraud-example1.html

CIBC. (2019). *CIBC cardholder banking service agreement*. https://www.cibc.com/en/legal.html

CIBC. (2023). Online banking safety tips. https://www.cibc.com/en/privacy-security/online-banking-safety-tips.html

City of London Police. (2023). *Advice about fraud.* https://www.cityoflondon.police.uk/advice/advice-and-information/fa2/fraud/

Clarke, R. V., & Felson, M. (2017). Introduction: Criminology, routine activity, and rational choice. In R.D. Lambert (Ed.), *Routine activity and rational choice* (pp. 1–14). Routledge. https://doi.org/10.4324/9781315128788-1

Cleghorn, J., & Griffiths, M. D. (2015). Why do gamers buy ‘virtual assets’? An insight in to the psychology behind purchase behaviour. *Digital Education Review*, *27*, 85–104.

Code, L. (2006). *Ecological thinking: The politics of epistemic location*. Oxford University Press.

Collins, H. M., & Yearley, S. (1992). Epistemological chicken. In A. Pickering (Ed.), *Science as practice and culture*. University of Chicago Press.

Cook, P. J. (1986). The demand and supply of criminal opportunities. *Crime and Justice*, *7*, 1–27. https://doi.org/10.1086/449111

Copeland, R. (2019). Affectio-affectus in Latin rhetoric up to c. 1200. In J. Ruys, M. Champion, & K. Essary (Eds.), *Before emotion: The language of feeling, 400-1800* (pp. 38–50). Routledge.

Corlett, S., & Mavin, S. (2018). Reflexivity and researcher positionality. In C. Cassell, A. Cunliffe, & G. Grandy (Eds.), *The SAGE handbook of qualitative business and management research Methods: History and Traditions*, (pp. 377–398). SAGE Publications Ltd. https://doi.org/10.4135/9781526430212.n23

Cornish, D. B., & Clarke, R. V. (Eds.). (2014). *The reasoning criminal: Rational choice perspectives on offending*. Routledge.

Correia, S. G., (2019). Responding to victimisation in a digital world: A case study of fraud and computer misuse reported in Wales. *Crime Science*, *8*(1), 4. https://doi.org/10.1186/s40163-019-0099-7

Corporation for Digital Scholarship. (n.d.). *Zotero*. [Computer software] https://www.zotero.org/

Council of Europe. (2001). Council of Europe: Convention on cybercrime. *International Legal Materials*, *20*(2), 317–325. https://doi.org/10.1017/S0020782900032873

Council of Europe. (2023). *Cybercrime Convention Committee*. https://www.coe.int/en/web/cybercrime/tcy

Cross, C. (2017). “I’ve lost some sleep over it”: Secondary trauma in the provision of support to older fraud victims. *Canadian Journal of Criminology and Criminal Justice*, *59*(2), 168–197. https://doi.org/10.3138/cjccj.2016.E11

Cross, C., Dragiewicz, M., & Richards, K. (2018). Understanding romance fraud: Insights from domestic violence research. *The British Journal of Criminology*, *58*(6), 1303–1322. https://doi.org/10.1093/bjc/azy005

Cross, C., Parker, M., & Sansom, D. (2019). Media discourses surrounding 'non-ideal' victims: The case of the Ashley Madison data breach. *International Review of Victimology*, *25*(1), 53–69. https://doi.org/10.1177/0269758017752410

Currie, J., & Spatz Widom, C. (2010). Long-term consequences of child abuse and neglect on adult economic well-being. *Child Maltreatment, 15*(2), 111–120. https://doi.org/10.1177/1077559509355316

Cybersecurity & Infrastructure Security Agency. (2023). Defining insider threats. https://www.cisa.gov/defining-insider-threats

Cyber Security Intelligence. (2022, June 6). Cyber crime's history—Part 2—Current social effects. https://www.cybersecurityintelligence.com/blog/cyber-crimes-history---part-2---current-social-effects--6328.html

Das, S., & Nayak, T. (2013). Impact of cyber crime: Issues and challenges. *International Journal of Engineering Sciences, 6*(2), 12.

De Laet, M., & Mol, A. (2000). The Zimbabwe bush pump: Mechanics of a fluid technology. *Social Studies of Science*, *30*(2), 225–263. https://doi.org/10.1177/030631200030002002

DeLanda, M. (2006). *A new philosophy of society: Assemblage theory and social complexity*. Bloomsbury Publishing.

Deleuze, G. (1994). *Difference and repetition* (P. Patton, Trans.). Columbia University Press.

Deleuze, G., & Guattari, F. (1983). *Anti-Oedipus* (R. Hurley, M. Seem, & H. R. Lane, Trans.). University of Minnesota Press.

Deleuze, G., & Guattari, F. (1987). *A thousand plateaus* (B. Massumi, Trans.). University of Minnesota Press.

Deleuze, G., & Parnet, C. (2007). *Dialogues II* (H. Tomlinson & B. Habberjam, Trans.). Columbia University Press.

Department of Justice. (2021, November 30). International hacking group members sentenced for SIM hijacking conspiracy that resulted in the theft of millions in cryptocurrency. https://www.justice.gov/usao-edmi/pr/international-hacking-group-members-sentenced-sim-hijacking-conspiracy-resulted-theft

Department of Justice Canada. (2015, July 23). Who is a victim of crime. https://www.justice.gc.ca/eng/cj-jp/victims-victimes/rights-droits/who-qui.html

DiCicco-Bloom, B., & Crabtree, B. F. (2006). The qualitative research interview. *Medical Education*, *40*(4), 314–321.

Dilek, S., Çakır, H., & Aydın, M. (2015). Applications of artificial intelligence techniques to combating cyber crimes: A review. *International Journal of Artificial Intelligence &* Applications, 6(1), 21-39. https://doi.org/10.5121/ijaia.2015.6102

Dludla, A. S. (2021). *An analysis of a cheque to identify fraud* (Doctoral dissertation, University of South Africa). UNISA Institutional Repository. https://ir.unisa.ac.za/handle/10500/29368

Domashova, J., & Zabelina, O. (2021). Detection of fraudulent transactions using SAS Viya machine learning algorithms. *Procedia Computer Science*, *190*, 204–209. https://doi.org/10.1016/j.procs.2021.06.025

Donalds, C., & Osei-Bryson, K.-M. (2014). A cybercrime taxonomy: Case of the Jamaican jurisdiction. *CONF-IRM 2014 Proceedings.* 5. https://aisel.aisnet.org/confirm2014/5

Duff, C. (2014). *Assemblages of health: Deleuze's empiricism and the ethology of life*. Springer Netherlands. https://doi.org/10.1007/978-94-017-8893-9

Edwards, J. (2021, December 31). Capital One to pay $190M settlement after hacker stole data from millions of consumers. *Top Class Actions.* https://topclassactions.com/lawsuit-settlements/privacy/data-breach/capital-one-to-pay-190m-settlement-after-hacker-stole-data-from-millions-of-consumers/

Ekblom, P. (1994). Proximal circumstances: A mechanism-based classification of crime prevention. *Crime Prevention Studies*, *2*, 185–232. https://popcenter.asu.edu/sites/g/files/litvpz3631/files/library/CrimePrevention/Volume_02/09ekblom.pdf

Ekblom, P. (2010). *Crime prevention, security and community safety using the 5Is framework.* Springer.

European Insurance and Occupational Pensions Authority. (2025). *Digital Operational Resilience Act (DORA)—EIOPA*. https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

Europol. (2021, December 1). Money muling. *Europol*. https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/money-muling

Ewen, P. (2021). The finance of sex trafficking and impact of COVID-19. *Journal of Modern Slavery: A Multidisciplinary Exploration of Human Trafficking Solutions*, *6*(2), 159-168. https://doi.org/10.22150/jms/mnbg4893

Experian. (2020, August 19). How do credit card companies investigate fraud? https://www.experian.com/blogs/ask-experian/how-do-credit-card-companies-investigate-fraud/

Farman, J. (2014). Creative misuse as resistance: Surveillance, mobile technologies, and locative games. *Surveillance & Society*, *12*(3), 377–388. https://doi.org/10.24908/ss.v12i3.4981

Fathy, C. A., & Donahue, S. P. (2016). Reimbursement rates for photoscreening by insurance provider. *Journal of American Association for Pediatric Ophthalmology and Strabismus, 20*(4), e4. https://doi.org/10.1016/j.jaapos.2016.07.016

Federal Bureau of Investigation. (n.d.). Business email compromise. *Federal Bureau of Investigation.* https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/business-email-compromise

Federal Trade Commission. (2021, May 27). How to recognize, remove, and avoid malware. https://consumer.ftc.gov/articles/how-recognize-remove-avoid-malware The webpage is no longer publicly available but can be accessed via the Internet Archive.

Feenberg, A. (1991). *Critical theory of technology* (Vol. 5). Oxford University Press.

Financial Consumer Agency of Canada. (2018, January 24). Resolving an unauthorized transaction. https://www.canada.ca/en/financial-consumer-agency/services/resolving-unauthorized-transaction.html

Findley, P. A., Plummer, S.-B., & McMahon, S. (2016). Exploring the experiences of abuse of college students with disabilities. *Journal of Interpersonal Violence*, *31*(17), 2801–2823. https://doi.org/10.1177/0886260515581906

Fine, G. A., & Kleinman, S. (1979). Rethinking subculture: An interactionist analysis. *American Journal of Sociology*, *85*(1), 1–20. https://doi.org/10.1086/226971

Fintech News Malaysia. (2023, January 18). The growing threat of cybercrime as a service to Asia's financial institutions. https://fintechnews.my/34083/security/the-growing-threat-of-cybercrime-as-a-service-to-asias-financial-institutions/

Fletcher, N. (2007). Challenges for regulating financial fraud in cyberspace. *Journal of Financial Crime*, *14*(2), 190-207. https://doi.org/10.1108/13590790710742672

Foote, M. Q., & Gau Bartell, T. (2011). Pathways to equity in mathematics education: How life experiences impact researcher positionality. *Educational Studies in Mathematics, 78*(1), 45–68. https://doi.org/10.1007/s10649-011-9309-2

Funk, C. (2017). Mixed messages about public trust in science. *Issues in Science and Technology*, *34*(1), 86–88. https://issues.org/real-numbers-mixed-messages-about-public-trust-in-science/

Furlong, K. (2014). STS beyond the "modern infrastructure ideal": Extending theory by engaging with infrastructure challenges in the South. *Technology in Society, 38,* 139–147. https://doi.org/10.1016/j.techsoc.2014.04.001

Furnell, S. (2007). Phishing: Can we spot the signs? *Computer Fraud & Security*, *2007*(3), 10–15. https://doi.org/10.1016/s1361-3723(07)70035-0

Furnell, S. (2020). Technology use, abuse, and public perceptions of cybercrime. In T. Holt & A. Bossler (Eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 45–66). Palgrave Macmillan. https://doi.org/10.1007/978-3-319-78440-3_9

García-Holgado, A., & García-Peñalvo, F. J. (2018). Human interaction in learning ecosystems based on open source solutions. In P. Zaphiris & A. Ioannou (Eds.), *Learning and collaboration technologies. Design, development and technological innovation* (Vol. 10924, pp. 218-232) Springer International Publishing. https://doi.org/10.1007/978-3-319-91743-6_17

Gieryn, T. F. (1983). Boundary-work and the demarcation of science from non-science: Strains and interests in professional ideologies of scientists. *American Sociological Review*, 48(6), 781–795. https://doi.org/10.2307/2095325

Gieryn, T. F. (1999). *Cultural boundaries of science: Credibility on the line*. University of Chicago Press.

Gillespie, T. (2006). Designed to 'effectively frustrate': Copyright, technology and the agency of users. *New Media & Society*, *8*(4), 651–669. https://doi.org/10.1177/1461444806065662

Gonzalez, C. (2022, April 26). Top 5 social engineering techniques and how to prevent them. *Exabeam*. https://www.exabeam.com/information-security/top-8-social-engineering-techniques-and-how-to-prevent-them-2022/

Goodman, L. A. (1961). Snowball sampling. *The Annals of Mathematical Statistics*, 148–170.

Gottschalk, P. (2010). Categories of financial crime. *Journal of Financial Crime*, *17*(4), 441–458. https://doi.org/10.1108/13590791011082797

Government of Canada (2014b, December 9). *Consolidated Federal Laws of Canada, Protecting Canadians from Online Crime Act.* https://laws-lois.justice.gc.ca/eng/annualstatutes/2014_31/page-1.html

Government of Canada (2015, July 8). *Canada completes ratification of convention on cybercrime*. *Government of Canada.* https://www.canada.ca/en/news/archive/2015/07/canada-completes-ratification-convention-cybercrime.html

Grabosky, P., Smith, R. G., & Dempsey, G. (2001). *Electronic theft: Unlawful acquisition in cyberspace*. Cambridge University Press.

Grove, K., & Pugh, J. (2015). Assemblage thinking and participatory development: Potentiality, ethics, biopolitics. *Geography Compass*, *9*(1), 1–13. https://doi.org/10.1111/gec3.12191

Haasio, A., Harviainen, J. T., & Savolainen, R. (2020). Information needs of drug users on a local dark web marketplace. *Information Processing & Management, 57*(2), 102080. https://doi.org/10.1016/j.ipm.2019.102080

Hafiz, K. T., Aghili, S., & Zavarsky, P. (2016). The use of predictive analytics technology to detect credit card fraud in Canada. *2016 11th Iberian Conference on Information Systems and Technologies (CISTI),* 1–6. https://doi.org/10.1109/cisti.2016.7521522

Halder, D., & Jaishankar, K. (2011). *Cyber crime and the victimization of women: Laws, rights and regulations.* Igi Global. https://doi.org/10.4018/978-1-60960-830-9

Haraway, D. (1988). Situated Knowledges: The science question in feminism and the privilege of partial perspective. *Feminist Studies, 14*(3), 575–599. https://doi.org/10.4324/9780203427415-40

Haraway, D. (1989). *Primate visions: Gender, race, and nature in the world of modern science.* Routledge.

Haraway, D. (1991). *Simians, cyborgs, and women: The reinvention of nature.* Routledge.

Hasham, S., Joshi, S., & Mikkelsen, D. (2019). *Financial crime and fraud in the age of cybersecurity*. McKinsey & Company, *2019*, 1–11. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/Financial%20crime%20and%20fraud%20in%20the%20age%20of%20cybersecurity/Financial-crime-and-fraud-in-the-age-of-cybersecurity.pdf

Hayes, D., Cappa, F., & Cardon, J. (2018). A framework for more effective dark web marketplace investigations. *Information, 9*(8), 186. https://doi.org/10.3390/info9080186

Hayles, K. (1999). *How we became posthuman: Virtual bodies in cybernetics, literatures, and informatics.* University of Chicago.

Hazar, A., & Babuşcu, Ş. (2023). Financial technologies: Digital payment systems and digital banking. Today's dynamics. *Journal of Research. Innovation and Technologies, 2*(4), 162–178. https://doi.org/10.57017/jorit.v2.2(4).04

Hazelwood, S. D., & Koon-Magnin, S. (2013). Cyber stalking and cyber harassment legislation in the United States: A qualitative analysis. *International Journal of Cyber Criminology, 7*(2), 155. https://cybercrimejournal.com/pdf/hazelwoodkoonmagninijcc2013vol7issue2.pdf

Higbee, A. (2018). The role of crypto-currency in cybercrime. *Computer Fraud & Security, 2018*(7), 13–15. https://doi.org/10.1016/S1361-3723(18)30064-2

Holt, T. J. (2012). Exploring the intersections of technology, crime, and terror. *Terrorism and Political Violence, 24*(2), 337–354. https://doi.org/10.1080/09546553.2011.648350

Holt, T. J., Freilich, J. D., & Chermak, S. M. (2017). Exploring the subculture of ideologically motivated cyber-attackers. *Journal of Contemporary Criminal Justice, 33*(3), 212–233. https://doi.org/10.1177/1043986217699100

Holt, T. J., Leukfeldt, R., & van de Weijer, S. (2020). An examination of motivation and routine activity theory to account for cyberattacks against Dutch web sites. *Criminal Justice and Behavior, 47*(4), 487–505. https://doi.org/10.1177/0093854819900322

Horan, T. J. (2018, July 10). Fraud detection: Applying behavioral analytics. *FICO Decisions Blog*. https://www.fico.com/blogs/fraud-detection-applying-behavioral-analytics

Hughes, T. P. (1979). The electrification of America: The system builders. *Technology and Culture, 20*(1), 124–161. https://doi.org/10.2307/3103115

Hwang, J., & Christensen, C. M. (2008). Disruptive innovation in health care delivery: A framework for business-model innovation. *Health Affairs, 27*(5), 1329–1335. https://doi.org/10.1377/hlthaff.27.5.1329

Hyysalo, S., Jensen, T. E., & Oudshoorn, N. (2016). *The new production of users: Changing innovation collectives and involvement strategies.* Routledge.

IdentityTheft.gov. (2023, January 28). Federal Trade Commission. https://www.identitytheft.gov/#/

Interac. (2023). How Interac works to protect your payments. https://www.interac.ca/en/consumers/security/interac-e-transfer/

Interpol. (n.d.). Spotlight cybercrime outreach. https://www.interpol.int/en/Resources/INTERPOL-Spotlight/Spotlight-Issue-2-Cybercrime/Spotlight-Cybercrime-Outreach

Irwin, A. (2008). STS perspectives on scientific governance. In E.J. Hackett, O. Amsterdamska, M. Lynch, &. J. Wajcman (Eds.). *The handbook of science and technology studies* (pp. 583-607). MIT Press.

Israel, M., & Hay, I. (2006). *Research ethics for social scientists.* Sage.

Jamshed, S. (2014). Qualitative research method-interviewing and observation. *Journal of Basic and Clinical Pharmacy*, *5*(4), 87. https://doi.org/10.4103/0976-0105.141942

Jasanoff, S. (1998). *The fifth branch: Science advisers as policymakers*. Harvard University Press.

Jasanoff, S. (1999). STS and public policy: Getting beyond deconstruction. *Science, Technology and Society*, *4*(1), 59–72. https://doi.org/10.1177/097172189900400104

Jasanoff, S. (2003). Technologies of humility: Citizen participation in governing science. *Minerva*, *41*(3), 223–244. https://doi.org/10.1023/A:1025557512320

Jasanoff, S. (2017). Back from the brink: Truth and trust in the public sphere. *Issues in Science and Technology*, *33*(4), 25–28. https://issues.org/perspective-back-from-the-brink-truth-and-trust-in-the-public-sphere/

Jensen, T. E. (2012). Intervention by invitation: New concerns and new versions of the user in STS. *Science & Technology Studies*, *25*(1), 13–36. https://doi.org/10.23987/sts.55279

Johnson, E. (2017, October 20). “They have access to your entire identity”: TD Bank insider blows whistle on work being moved to India. *CBC News*. https://www.cbc.ca/news/business/td-bank-outsourcing-fraud-india-1.4362324

Johnson, E. (2021, November 15). Banks blame customers duped by fake cheques in online job scams. *CBC News*. https://www.cbc.ca/news/canada/toronto/banks-online-scam-fake-cheque-fraud-td-1.6244111

Junger, M., Wang, V., & Schlömer, M. (2020). Fraud against businesses both online and offline: Crime scripts, business characteristics, efforts, and benefits. *Crime Science*, *9*(1), 13. https://doi.org/10.1186/s40163-020-00119-4

Kajjumba, G. W., Nagitta, O. P., Osra, F. A., & Mkansi, M. (2020). Offshoring-outsourcing and onshoring tradeoffs: The impact of coronavirus on global supply chain. In M. Franco (Ed.), *Outsourcing and Offshoring*. IntechOpen. https://doi.org/10.5772/intechopen.95281

Kallio, H., Pietilä, A.-M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: Developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing*, *72*(12), 2954–2965. https://doi.org/10.1111/jan.13031

Kebande, V. R., Karie, N. M., Michael, A., Malapane, S. M., & Venter, H. S. (2017). How an IoT-enabled "smart refrigerator" can play a clandestine role in perpetuating cyber-crime. *2017 IST-Africa Week Conference (IST-Africa)*, 1–10. https://doi.org/10.23919/istafrica.2017.8102362

Kigerl, A. (2016). Cyber crime nation typologies: K-means clustering of countries based on cyber crime rates. *International Journal of Cyber Criminology*, *10*(2). https://doi.org/10.5281/zenodo.163399

Kigerl, A. (2020). Behind the Scenes of the Underworld: Hierarchical Clustering of Two Leaked Carding Forum Databases. *Social Science Computer Review*, 40(3), 618-640. https://doi.org/10.1177/0894439320924735

Kiljan, S., Simoens, K., Cock, D. D., Eekelen, M. V., & Vranken, H. (2016). A survey of authentication and communications security in online banking. *ACM Computing Surveys (CSUR)*, *49*(4), 1–35. https://doi.org/10.1145/3002170

King, A. (2024, April 11). 140 BMO customers say they lost $1.5M in transfer frauds, plan to sue bank. *CBC News.* https://www.cbc.ca/news/canada/toronto/bmo-customers-transfer-theft-cybercrime-1.7169622

Kinkaid, E. (2019). Can assemblage think difference? A feminist critique of assemblage geographies. *Progress in Human Geography*, 030913251983616. https://doi.org/10.1177/0309132519836162

Kleinrock, L. (1961). *Information flow in large communication nets.* Massachusetts Institute of Technology.

Kline, R., & Pinch, T. (1996). Users as agents of technological change: The social construction of the automobile in the rural United States. *Technology and Culture, 37*(4), 763–795. https://doi.org/10.2307/3107097

Korauš, A., Dobrovič, J., Rajnoha, R., & Brezina, I. (2017). The safety risks related to bank cards and cyber attacks. *Journal of Security and Sustainability Issues*, 563–574. https://doi.org/10.9770/jssi.2017.6.4(3)

Kosi, F. (2019). *Robotic process automation (RPA) and security*. Mercy College.

Kraemer-Mbula, E., Tang, P., & Rush, H. (2013). The cybercrime ecosystem: Online innovation in the shadows? *Technological Forecasting and Social Change*, *80*(3), 541–555. https://doi.org/10.1016/j.techfore.2012.07.002

Kuehn, A., & Mueller, M. (2014). Shifts in the cybersecurity paradigm: Zero-day exploits, discourse, and emerging institutions. *Proceedings of the 2014 New Security Paradigms Workshop*, 63–68. https://doi.org/10.1145/2683467.2683473

Kumar, A., Luthra, S., Mangla, S. K., & Kazançoğlu, Y. (2020). Covid-19 impact on sustainable production and operations management. *Sustainable Operations and Computers*, *1*, 1–7. https://doi.org/10.1016/j.susoc.2020.06.001

Kuo, C., & Tsang, S.-S. (2023). Detection of price manipulation fraud through rational choice theory: Evidence for the retail industry in Taiwan. *Security Journal*, *36*(4), 712–731. https://doi.org/10.1057/s41284-022-00360-3

Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. *Computers & Security*, *45*, 58–74. https://doi.org/10.1016/j.cose.2014.05.006

Latour, B. (1987). *Science in action: How to follow scientists and engineers through society*. Harvard University Press.

Latour, B. (1992). Where are the missing masses? The sociology of a few mundane artifacts. In W. E. Bijker and J. Law (Eds.), *Shaping technology/building society: Studies in sociotechnical change*, (pp. 255–258). MIT Press.

Latour, B. (1993a). *The pasteurization of France* (A. Sheridan & J. Law, Trans.). Harvard University Press.

Latour, B. (1993b). *We have never been modern* (C. Porter, Trans.). Harvard University.

Latour, B. (2005). *Reassembling the social: An introduction to actor-network-theory*. Oxford University Press.

Latzko-Toth, G., Söderberg, J., Millerand, F., & Jones, S. (2019). Misuser innovations the role of “misuses” and “misusers” in digital communication technologies. In J. Vertesi & D.

Ribes (Eds.), *digitalSTS: A field guide for science & technology studies* (pp. 393–411). Princeton University Press.

Law, J. (1992). Notes on the theory of the actor-network: Ordering, strategy, and heterogeneity. *Systems Practice*, *5*, 379–393. https://doi.org/10.1007/bf01059830

Law, J. (2002). Objects and spaces. *Theory, Culture & Society*, *19*(5–6), 91–105. https://doi.org/10.1177/026327602761899165

Law, J. (2004). *After method: Mess in social science research*. Routledge.

Law, J. (2015). What's wrong with a one-world world? *Distinktion: Scandinavian Journal of Social Theory*, *16*(1), 126–139. https://doi.org/10.1080/1600910X.2015.1020066

Law, J., Bijker, W. E., Hughes, T. P., & Pinch, T. (2012). Technology and heterogeneous engineering: The case of Portuguese expansion. In W. E. Bijker, T. P. Hughes, & T. Pinch (Eds.), *The social construction of technological systems: New directions in the sociology and history of technology* (pp. 105–128). MIT Press.

Law, J., & Callon, M. (1992). The life and death of an aircraft: A network analysis of technical change. In W. E. Bijker & J. Law (Eds.), *Shaping technology/building society: Studies in sociotechnical change* (pp. 21-52). MIT Press.

Law, J., & Mol, A. M. (1998). On metrics and fluids: Notes on otherness. In R. Chia (Ed.), *Organized worlds* (pp. 26-43). Routledge. https://doi.org/10.4324/9780203209073-8

Law, J., & Singleton, V. (2014). ANT, multiplicity and policy. *Critical Policy Studies*, *8*(4), 379–396. https://doi.org/10.1080/19460171.2014.957056

Lee, C. S., & Wang, Y. (2022). Typology of cybercrime victimization in Europe: A multilevel latent class analysis. *Crime & Delinquency*, *70*(4), 1196-1223. https://doi.org/10.1177/00111287221118880

Lee, K.-F., Chan, M. Y., & Mohamad Ali, A. (2022). Self and desired partner descriptions in the online romance scam: A linguistic analysis of scammer and general user profiles on online dating portals. *Crime Prevention and Community Safety*, 25(1), 20-46. https://doi.org/10.1057/s41300-022-00169-7

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L. G., & Wolff, S. (2009). A brief history of the internet. *ACM SIGCOMM Computer Communication Review*, *39*(5), 22–31. https://doi.org/10.1145/1629607.1629613

Lerner, J., & Seru, A. (2017). *The use and misuse of patent data: Issues for corporate finance and beyond* (No. W24053; p. w24053). National Bureau of Economic Research. https://doi.org/10.3386/w24053.

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017). A typology of cybercriminal networks: From low-tech all-rounders to high-tech specialists. *Crime, Law and Social Change*, *67*, 21–37. https://doi.org/10.1007/s10611-016-9662-2

Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: Overview and issues. *Crime, Law and Social Change*, *67*(1), 3–20. https://doi.org/10.1007/s10611-016-9645-3

Liggett, R., Lee, J. R., Roddy, A. L., & Wallin, M. A. (2019). The dark web as a platform for crime: An exploration of illicit drug, firearm, CSAM, and cybercrime markets. In T. J. Holt & A. M. Bossler (Eds.), *The Palgrave handbook of international cybercrime and cyberdeviance*, (pp. 91–116). Palgrave Macmillan.

Lindlof, T. R., & Taylor, B. C. (2017). *Qualitative communication research methods*. Sage Publications.

Lord, B. (2010). *Spinoza's Ethics: An Edinburgh philosophical guide*. Edinburgh University Press.

Luthje, C., Herstatt, C., & Eric, von H. (2005). User-innovators and "local" information: The case of mountain biking. *Research Policy*, 34(6), 951-965. https://doi.org/10.1016/j.respol.2005.05.005

Lynch, M. E. (1979). *Art and artifact in laboratory science: A study of shop work and shop talk in a research laboratory.* University of California, Irvine.

Lysgård, H. K. (2019). The assemblage of culture-led policies in small towns and rural communities. *Geoforum*, *101*, 10–17. https://doi.org/10.1016/j.geoforum.2019.02.019

Ma, K. W. F., Dhot, T., & Raza, M. (2023). Considerations for using artificial intelligence to manage authorized push payment (APP) scams. *IEEE Engineering Management Review*, *51*(3), 166-179. https://doi.org/10.1109/emr.2023.3288432

Ma, K. W. F., & McKinnon, T. (2022). Covid-19 and cyber fraud: Emerging threats during the pandemic. *Journal of Financial Crime*, *29*(2), 433–446. https://doi.org/10.2139/ssrn.3718845

MacKenzie, D. (2001). Physics and finance: S-terms and modern finance as a topic for science studies. *Science, Technology, & Human Values*, *26*(2), 115–144. https://doi.org/10.1002/9780470774274.ch6

MacKenzie, D., & Millo, Y. (2003). Constructing a market, performing theory: The historical sociology of a financial derivatives exchange. *American Journal of Sociology*, *109*(1), 107–145. https://doi.org/10.4324/9780429494338-15

Madakam, S., Holmukhe, R. M., & Jaiswal, D. K. (2019). The future digital work force: Robotic process automation (RPA). *JISTEM-Journal of Information Systems and Technology Management*, 16. https://doi.org/10.4301/s1807-1775201916001

Magaldi, D., & Berler, M. (2020). Semi-structured interviews. In V. Zeigler-Hill & T. K. Shackelford (Eds.), *Encyclopedia of Personality and Individual Differences* (pp. 4825–4830). Springer.

Malins, P. (2017). Desiring assemblages: A case for desire over pleasure in critical drug studies. *International Journal of Drug Policy*, *49*, 126–132. https://doi.org/10.1016/j.drugpo.2017.07.018

Maruatona, O. O., Vamplew, P., & Dazeley, R. (2012). Prudent fraud detection in internet banking. *2012 Third Cybercrime and Trustworthy Computing Workshop*, 60–65. https://doi.org/10.1109/ctc.2012.13

Massumi, B. (1996). Becoming-Deleuzian. *Environment and Planning D: Society and Space*, *14*(4), 395–406. https://doi.org/10.1068/d140395

Massumi, B. (2021). *Parables for the virtual: Movement, affect, sensation*. Duke University Press.

Mbaziira, A., & Jones, J. (2016). A text-based deception detection model for cybercrime. *International Conference on Technology and Management*, 1–8.

Mbaziira, A. V. (2017). *Detecting and analyzing cybercrime in text-based communication of cybercriminal networks through computational linguistic and psycholinguistic feature modeling* [Unpublished doctoral dissertation]. George Mason University.

McCuddy, T. (2022). Digital disclosure of delinquency: Online peers and the sharing of offline crime. *Crime & Delinquency*, 68(13-14), 2554-2580. . https://doi.org/10.1177/00111287211067179

McFarlane, C. (2011). The city as assemblage: Dwelling and urban space. *Environment And Planning D: Society and Space*, *29*(4), 649–671. https://doi.org/10.1068/d4710

McFarlane, C., & Anderson, B. (2011). Thinking with assemblage. *Area*, *43*(2), 162–164. https://doi.org/10.1111/j.1475-4762.2011.01012.x

McGuire, M. R., & Holt, T. J. (2017). *The Routledge handbook of technology, crime and justice*. Taylor & Francis.

Meyer, M. (1995). Stop! Cyberthief! *Newsweek*, *125*(6), 36–38. https://www.newsweek.com/stop-cyberthief-185230

OpenText. (n.d.). *What is an insider threat?* https://www.opentext.com/what-is/insider-threat

Mills, J. E., & Byun, S. (2006). Cybercrimes Against Consumers: Could Biometric Technology Be the Solution? *IEEE Internet Computing*, *10*(4), 64–71. https://doi.org/10.1109/mic.2006.73

Minister of Public Safety and Emergency Preparedness. (2021). *Royal Canadian Mounted Police (RCMP) 2021-22 Departmental Plan*. *Government of Canada*. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/dprtmntl-pln-2021-22/dprtmntl-pln-2021-22-en.pdf

Mirdala, R., Mizdraković, V., Arežina, N., & Stefanović, D. (2014). Creative accounting: From creativity to misuse. *Proceedings of the 1st International Scientific Conference - FINIZ 2014*, 5–7. https://doi.org/10.15308/finiz-2014-5-7

Moitra, S. (2005). Developing policies for cybercrime: Some empirical issues. *European Journal of Crime, Criminal Law and Criminal Justice*, *13*(3), 435–464. https://doi.org/10.1163/1571817054604119

Mol, A. (1999). Ontological politics. A word and some questions. *The Sociological Review*, *47*(1_suppl), 74–89. https://doi.org/10.1111/1467-954x.46.s.5

Mol, A. (2002). *The body multiple: Ontology in medical practice*. Duke University Press.

Mol, A. (2010). Actor-network Theory: Sensitive Terms and Enduring Tensions. *Kölner Zeitschrift Für Soziologie Und Sozialpsychologie*, *50*(1), 253–269. https://hdl.handle.net/11245/1.330874

Mollick, E. (2005, July 15). Tapping into the underground. *MIT Sloan Management Review*. https://sloanreview.mit.edu/article/tapping-into-the-underground/

Morgan, H. (2021). Conducting a qualitative document analysis. *The Qualitative Report*, *27*(1), 64–77. https://doi.org/10.46743/2160-3715/2022.5044

Morrison, P. D., Roberts, J. H., & Von Hippel, E. (2000). Determinants of user innovation and innovation sharing in a local market. *Management Science*, *46*(12), 1513–1527.

MSU Federal Credit Union. (2017, November 2). *Fraud vs. dispute: What's the difference?* https://www.msufcu.org/fin40/story/1036/1036/

Müller, M. (2015). Assemblages and actor-networks: Rethinking socio-material power, politics and space. *Geography Compass*, *9*(1), 27–41. https://doi.org/10.1111/gec3.12192

Müller, M., & Schurr, C. (2016). Assemblage thinking and actor-network theory: Conjunctions, disjunctions, cross-fertilisations. *Transactions of the Institute of British Geographers*, *41*(3), 217–229. https://doi.org/10.1111/tran.12117

Mulligan, P. (2019, June 27). Nova Scotia woman phones number on her bank card, gets a fraudster instead, police say. *CBC News.* https://www.cbc.ca/news/canada/nova-scotia/phone-scam-bank-nova-scotia-victim-1.5192508

Muniesa, F. (2007). Market technologies and the pragmatics of prices. *Economy and Society*, *36*(3), 377–395. https://doi.org/10.1080/03085140701428340

Muniesa, F. (2021). Finance: Cultural or political? *Journal of Cultural Economy*, 17(5), 716-719. https://doi.org/10.1080/17530350.2021.1927151

Murphy, P. R., & Dacin, M. T. (2011). Psychological pathways to fraud: Understanding and preventing fraud in organizations. *Journal of Business Ethics*, *101*(4), 601–618. https://doi.org/10.1007/s10551-011-0741-0

National Institute of Standards and Technology. . (n.d.-a). Vulnerability. In *Computer Security Resource Center Glossary*. https://csrc.nist.gov/glossary/term/vulnerability

National Institute of Standards and Technology. (n.d.-b). *Malware*. In *Computer Security Resource Center Glossary*. https://csrc.nist.gov/glossary/term/malware

Nguyen, L. (2021, December 23). Capital One settles a class-action lawsuit for $190 million in a 2019 hacking. *The New York Times*. https://www.nytimes.com/2021/12/23/business/capital-one-hacking-settlement.html

O'Connor, P. (2021). 2021: Hackers value quality over quantity. *ITNOW*, *63*(4), 48–49. https://doi.org/10.1093/itnow/bwab122

Office of the Privacy Commissioner of Canada. (2020, August 4). Pipeda findings #2020-001: Bank ensures openness and comparable protection for personal information transferred to

third party. https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/pipeda-2020-001/

Office of the Superintendent of Financial Institutions. (2023, January 23). Financial data for banks. *Government of Canada*. https://www.osfi-bsif.gc.ca:443/Eng/wt-ow/Pages/FINDAT.aspx

Ololade, B. M., Salawu, M. K., & Adekanmi, A. D. (2020). E-fraud in Nigerian Banks: Why and How? *Journal of Financial Risk Management, 9*(3), 211–228. https://doi.org/10.4236/jfrm.2020.93012

Ombudsman for Banking Services and Investments. (2020, December 18). Bank customer is a victim of multiple incidents of fraud. https://www.obsi.ca/en/news/posts/bank-customer-is-a-victim-of-multiple-incidents-of-fraud/

Oudshoorn, N. E., & Pinch, T. (2003). *How users matter: The co-construction of users and technologies*. MIT press.

Padgett, D. K. (2004). Coming of age: Theoretical thinking, social responsibility and a global perspective in qualitative research. In D. K. Padgett (Ed.), *The qualitative research experience* (pp. 301-319). Wadsworth Publishers.

Parr, A. (Ed.). (2010). *Deleuze dictionary revised edition*. Edinburgh University Press.

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University.

Patil, K., Kulkarni, M., Sriraman, A., & Karande, S. (2017). Deep learning based car damage classification. *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)*, 50–54. https://doi.org/10.1109/icmla.2017.0-179

Patton, M. Q. (1990). *Qualitative evaluation and research methods*. SAGE Publications, inc.

PaymentsJournal. (2022, December 16). Data sharing as a means to combat fraud. https://www.paymentsjournal.com/data-sharing-as-a-means-to-combat-fraud/

Payne, B. K. (2020). Defining Cybercrime. In T. J. Holt & A. M. Bossler (Eds.), *The Palgrave andbook of international cybercrime and cyberdeviance* (pp. 3–25). Palgrave Macmillan.

Pereira, M. do M. (2019). Boundary-work that does not work: Social inequalities and the non-performativity of scientific boundary-work. *Science, Technology, & Human Values, 44*(2), 338–365. https://doi.org/10.1177/0162243918795043

Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing cybercrime: Definitions, typologies and taxonomies. *Forensic Sciences*, *2*(2), 379–398. https://doi.org/10.3390/forensicsci2020028

Picchietti, D. L., Arbuckle, R. A., Abetz, L., Durmer, J. S., Ivanenko, A., Owens, J. A., Croenlein, J., Allen, R. P., & Walters, A. S. (2011). Pediatric restless legs syndrome: Analysis of symptom descriptions and drawings. *Journal of Child Neurology*, *26*(11), 1365–1376. https://doi.org/10.1177/0883073811405852

Pinch, T. J., & Bijker, W. E. (1984). The social construction of facts and artefacts: Or how the sociology of science and the sociology of technology might benefit each other. *Social Studies of Science*, *14*(3) 399–441. https://doi.org/10.1177/030631284014003004

Prosa Mx (Director). (2021, October 7). *Fraud prevention in the banking sector—Adam Davies, FICO* [Video]. https://www.youtube.com/watch?v=Ys7yrIzg2t4

Public Safety Canada. (2016, January 29). *Cybercrime*. https://www.canada.ca/en/services/policing/police/crime-and-crime-prevention/cybercrime.html

Qabajeh, I., Thabtah, F., & Chiclana, F. (2018). A recent review of conventional vs. automated cybersecurity anti-phishing techniques. *Computer Science Review*, *29*, 44–55. https://doi.org/10.1016/j.cosrev.2018.05.003

Queen, K. (2015, May 13). Advances in fraud analytics promise to stop crooks, not you. *Yahoo Finance*. http://finance.yahoo.com/news/advances-fraud-analytics-promise-stop-120000685.html

Rajput, B. (2020). *Cyber economic crime in India: An integrated model for prevention and investigation*. Springer International Publishing. https://doi.org/10.1007/978-3-030-44655-0

RBC. (n.d.). *RBC alerts.* https://www.rbcroyalbank.com/ways-to-bank/banking-services/alerts.html#bank-account-content

RBC. (2020, December). *View scam alerts.* https://www.rbc.com/cyber-security/alerts/index.html

RBC. (2021). *Service agreement for personal accounts*. https://www.rbcroyalbank.com/onlinebanking/legal.html

Rider, B. (2022a). *A research agenda for financial crime*. Edward Elgar Publishing Limited.

Robertson, S. (2020). *Foundations in sociology I*. Saskatchewan Open Education Resources. https://www.saskoer.ca/soc112/

Romao, M., Costa, J., & Costa, C. J. (2019). Robotic process automation: A case study in the banking industry. *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*, 1–6. https://doi.org/10.23919/cisti.2019.8760733

Roth, A. L., Dunsby, J., & Bero, L. A. (2003). Framing processes in public commentary on US federal tobacco control regulation. *Social Studies of Science*, *33*(1), 7–44. https://doi.org/10.1177/0306312703033001038

Rowe, W. E. (2014). Positionality. In D. Coghlan & M. Brydon-Miller (Eds.), *The Sage encyclopedia of action research*, *628*. https://doi.org/10.4135/9781446294406

Royal Canadian Mounted Police. (2021, October 16). Business email compromise (BEC). https://www.rcmp-grc.gc.ca/en/business-email-compromise-bec

Royal Canadian Mounted Police. (2023). *About the RCMP in Ontario*. https://www.rcmp-grc.gc.ca/on/about-apropos/index-eng.htm

Rubin, H. J., & Rubin, I. S. (2011). *Qualitative interviewing: The art of hearing data*. Sage Publications.

Rutzou, T., & Elder-Vass, D. (2019). On Assemblages and Things: Fluidity, Stability, Causation Stories, and Formation Stories. *Sociological Theory*, *37*(4), 401–424. https://doi.org/10.1177/0735275119888250

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, *11*(4), 89. https://doi.org/10.3390/fi11040089

Savin-Baden, M., & Major, C. (2013). *Qualitative Research: The Essential Guide to Theory and Practice*. Routledge.

Scotiabank. (n.d.-a). Enable fingerprint or face authentication. https://www.scotiabank.com/content/scotiabank/ca/en/personal/bank-your-way/digital-banking-guide/banking-basics/fingerprint-face-authentication.html

Scotiabank. (n.d.-b). Report an incident or suspicious activity. https://www.scotiabank.com/content/scotiabank/ca/en/security/report-an-incident-or-suspicious-activity.html

Scotiabank. (2020). *Personal financial services agreement and personal credit agreement*. https://tc.scotiabank.com/about-scotiabank/connect-with-scotiabank/financial-services-agreements-pfsa-pca.html

Scotiabank. (2023). I use a third-party money management app or website to help manage my finances. How does Scotiabank's 2SV security enhancement impact these third-party services? *Scotiabank Help Centre*. https://help.scotiabank.com/article/i-use-a-third-party-money-management-app-or-website-to-help-manage-my-finances.-how-does-scotiabanks-2sv-security-enhancement-impact-these-third-party-services?origin=help-center

Scott, S. V., & Zachariadis, M. (2012). Origins and development of SWIFT, 1973–2009. *Business History*, *54*(3), 462–482. https://doi.org/10.1080/00076791.2011.638502

Seebruck, R. (2015). A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model. *Digital Investigation*, *14*, 36–45. https://doi.org/10.1016/j.diin.2015.07.002

Segal, M. J., Morris, S., & Rubin, J. M. (2002). Automated claim and payment verification. *The Journal of Medical Practice Management: MPM*, *17*(6), 297–301.

Serpe, R. T., & Stryker, S. (2011). The symbolic interactionist perspective and identity theory. In S. J. Schwartz, K. Luyckx, & V. L. Vignoles (Eds.), *Handbook of identity theory and research* (pp. 225–248). Springer.

Shao, X., Xie, J., Hong, T., & Jost, A. (2009). *U.S. Patent No. 7,562,814*. Washington, DC: U.S. Patent and Trademark Office. https://patents.google.com/patent/US7562814B1/en

Shapin, S., & Schaffer, S. (2011). *Leviathan and the air-pump: Hobbes, Boyle, and the experimental life* (Vol. 109). Princeton University Press.

Shaw, E. D., Ruby, K. G., & Post, J. M. (1998). The insider threat to information systems. *Security Awareness Bulletin*, *2*(98), 1–10.

Siddiqui, M. Z., Yadav, S., & Husain, M. S. (2018). Application of artificial intelligence in fighting against cyber crimes: A review. *International Journal of Advanced Research in Computer Science*, *9*(2), 118–122.

Silvast, A., & Virtanen, M. J. (2019). An assemblage of framings and tamings: Multi-sited analysis of infrastructures as a methodology. *Journal of Cultural Economy, 12*(6), 461–477. https://doi.org/10.1080/17530350.2019.1646156

Singapore National Crime Prevention Council. (2023). *Scam signs*. https://www.scamalert.sg/scam-signs

Söderberg, J. (2010). Misuser inventions and the invention of the misuser: Hackers, crackers and fileshares. 19(2), 151-179. https://doi.org/10.1080/09505430903168177

Soon-Sinclair, J. M., Imathiu, S., Obadina, A. O., Dongho Dongmo, F. F., Kamgain, A. D. T., Moholisa, E., Saba, C. K. S., Walekhwa, A. W., Hunga, H., & Kussaga, J. (2023). How worried are you about food fraud? A preliminary multi-country study among consumers in selected Sub-Saharan African countries. *Foods*, *12*(19), 3627. https://doi.org/10.3390/foods12193627

Ssewamala, F. M., & Ismayilova, L. (2009). Integrating children's savings accounts in the care and support of orphaned adolescents in rural Uganda. *Social Service Review*, *83*(3), 453–472. https://doi.org/10.1086/605941

Star, S. L., & Griesemer, J. R. (1989). Institutional ecology, translations' and boundary objects: Amateurs and professionals in Berkeley's museum of vertebrate zoology, 1907-39. *Social Studies of Science*, *19*(3), 387–420. https://doi.org/10.7551/mitpress/10113.003.0011

Stephens, G. (1995). Crime in cyberspace. *The Futurist*, 29(5), 24.

Sterne, J., & Sawhney, M. (2022). The acousmatic question and the will to datafy: Otter. Ai, low-resource languages, and the politics of machine listening. *Kalfou*, *9*(2), 288–306. https://doi.org/10.15367/kf.v9i2.617

Strathern, M. (2004). *Partial connections*. AltaMira Press.

Strumeyer, G. (2017). *The capital markets: Evolution of the financial ecosystem*. John Wiley & Sons.

Suchman, L. A. (2008). Feminist STS and the sciences of the artificial. In E. J. Hackett, O. Amsterdamska, M. Lynch, & J. Wajcman (Eds.), *The handbook of science and technology studies*, (3rd ed., pp. 139–164). MIT Press.

Suchman, L. A. (1983). Office procedure as practical action: Models of work and system design. *ACM Transactions on Information Systems*, *1*(4), 320–328. https://doi.org/10.1145/357442.357445

Sullivan, G. (2022). Law, technology, and data-driven security: *Infra*-legalities as method assemblage. *Journal of Law and Society, 49*, S31–S50. https://doi.org/10.1111/jols.12352

SWIFT. (2024). *Fraud & anomalies*. https://www.swift.com/our-solutions/compliance-and-shared-services/financial-crime-compliance/fraud-and-anomalies

Synytsia, M. (2021, April 13). Automated claims processing: Using RPA and machine learning to manage insurance Cclaims. *AltexSoft*. https://www.altexsoft.com/blog/automated-claims-processing/

Tabassum, A., Mustafa, M. S., & Maadeed, S. A. A. (2018). The need for a global response against cybercrime: Qatar as a case study. *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, 1–6. https://doi.org/10.1109/ISDFS.2018.8355331

Tade, O. (2022). Nature of frauds in Nigeria's banking ecosystem, 2015-2019. *Journal of Financial Crime, 29*(4), 1241–1248. https://doi.org/10.1108/jfc-08-2021-0185

Tade, O., & Adeniyi, O. (2020). Dimensions of electronic fraud and governance of trust in Nigeria's cashless ecosystem. *International Journal of Offender Therapy and Comparative Criminology, 64*(16), 1717–1740. https://doi.org/10.1177/0306624x20928028

Tariq, N. (2018). Impact of cyberattacks on financial institutions. *Journal of Internet Banking and Commerce, 23*(2), 1–11.

Taylor, M. (2003). Fraud detection and security system for financial institutions (U.S. Patent Application No. US20030182214A1). United States Patent and Trademark Office. https://patentimages.storage.googleapis.com/d3/e1/cf/099b6250a74e05/US20030182214A1.pdf

TD Bank. (n.d.-a). Protecting yourself from financial fraud and scams. https://stories.td.com/ca/en/featuredevents/fraud-prevention-advice

TD Bank. (n.d.-b). TD fraud alerts. https://www.td.com/ca/en/personal-banking/fraud-alerts

TD Bank. (2023a). Cardholder and electronic financial services terms and conditions. https://www.td.com/ca/en/personal-banking/advice/day-to-day-banking/cardholder-agreement

TD Bank. (2023b). *Online fraud & scam prevention—Online protection*. https://www.td.com/ca/en/about-td/privacy-and-security/how-you-can-protect-yourself/protect-yourself/online-protection

TD Stories. (2019, September 24). *TD explains: How to help protect yourself from phone scams*. https://stories.td.com/ca/en/article/td-explains-the-landline-phone-scam

The Association of Certified Fraud Examiners. (2014). *Report to the nations on occupational fraud and abuse: 2014 global fraud study*. https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2014/2014-report-to-nations.pdf

United Nations Office on Drugs and Crime. (n.d.). Mutual legal assistance request writer tool. https://www.unodc.org/mla/

United Nations Office on Drugs and Crime. (2022, August 19). Global programme on cybercrime. https://www.unodc.org/e4j/en/cybercrime/module-2/key-issues/intro.html

United States v. Thompson, No. CR19-159RSL (W.D. Wash. 2019).

UpGuard. (2023). *14 biggest healthcare data breaches*. https://www.upguard.com/blog/biggest-data-breaches-in-healthcare

US Federal Trade Commission. (2021). FTC consumer advice—Scams. https://consumer.ftc.gov/scams

Van der Wagen, W. (2018). *From cybercrime to cyborg crime: An exploration of high-tech cybercrime, offenders and victims through the lens of actor-network theory*. Rijksuniversiteit Groningen.

Van der Wagen, W., & Pieters, W. (2015). From cybercrime to cyborg crime: Botnets as hybrid criminal actor-networks. *British Journal of Criminology*, *55*(3), 578–595. https://doi.org/10.1093/bjc/azv009

Van Oost, E., Verhaegh, S., & Oudshoorn, N. (2009). From innovation community to community innovation: User-initiated innovation in wireless Leiden. *Science, Technology, & Human Values, 34*(2), 182–205. https://doi.org/10.1177/0162243907311556

Varadarajan, S., Rao, K. K., & Gangadharpalli, S. (2009). *U.S. Patent No. 7,552,865*. Washington, DC: U.S. Patent and Trademark Office.

Vertesi, J. (2014). Seamful spaces: Heterogeneous infrastructures in interaction. *Science, Technology, & Human Values*, *39*(2), 264–284. https://doi.org/10.1177/0162243913516012

Villar, A. S., & Khan, N. (2021). Robotic process automation in banking industry: A case study on Deutsche Bank. *Journal of Banking and Financial Technology, 5*(1), 71–86. https://doi.org/10.1007/s42786-021-00030-9

Vishnu, S., Agochiya, V., & Palkar, R. (2017). Data-centered dependencies and opportunities for robotics process automation in banking. *Journal of Financial Transformation*, *45*, 68–76.

Voicu, M.-C., & Babonea, A.-M. (1997). Using the snowball method in marketing research on hidden populations. *Social Problems, 44*(2), 1341–1351.

Wajcman, J., & Jones, P. K. (2012). Border communication: Media sociology and STS. *Media, Culture & Society*, *34*(6), 673–690. https://doi.org/10.1177/0163443712449496

Wall, D. (2007). *Cybercrime: The transformation of crime in the information age*. Polity.

Wall, D. S. (2008). Cybercrime and the culture of fear: Social science fiction(s) and the production of knowledge about cybercrime. *Information, Communication & Society*, *11*(6), 861–884. https://doi.org/10.1080/13691180802007788

WhatIsMyIPAddress.com, (n.d.). Money mules: How scammers exploit job seekers to launder money. https://whatismyipaddress.com/money-mule

Whitchurch, G. G., & Constantine, L. L. (1993). Systems theory. In P. Boss, W. J. Doherty, R. LaRossa, W. R. Schumm, S. K. Steinmetz (Eds.), *Sourcebook of family theories and methods: A contextual approach* (pp. 325–355). Springer.

Winner, L. (1988). Do Artifacts Have Politics? In L. Winner (Ed.), *The Whale and the reactor: A search for limits in an age of high technology* (pp. 19–39). University of Chicago.

Winner, L. (1993). Upon opening the black box and finding it empty: Social constructivism and the philosophy of technology. *Science, Technology, & Human Values, 18*(3), 362–378. https://doi.org/10.1177/016224399301800306

Wynne, B. (1992). Misunderstood misunderstanding: Social identities and public uptake of science. *Public Understanding of Science, 1*(3), 281. https://doi.org/10.1017/cbo9780511563737.002

Wynne, B. (2007). Public participation in science and technology: Performing and obscuring a political–conceptual category mistake. *East Asian Science, Technology and Society: An International Journal, 1*(1), 99–110. https://doi.org/10.1215/s12280-007-9004-7

Yar, M. (2005). The Novelty of ‘Cybercrime’ An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, *2*(4), 407–427. https://doi.org/10.1177/147737080556056

Yates, J. S., Harris, L. M., & Wilson, N. J. (2017). Multiple ontologies of water: Politics, conflict and implications for governance. *Environment and Planning D: Society and Space*, *35*(5), 797–815. https://doi.org/10.1177/0263775817700395

Yin R. K. (1994). *Case study research: Design and methods.* Sage Publications.

Zawoad, S., & Hasan, R. (2015). Faiot: Towards building a forensics aware eco system for the Internet of Things. *2015 IEEE International Conference on Services Computing*, 279–284. https://doi.org/10.1109/scc.2015.46

Zhang, Z., Jia, J., Wang, B., & Gong, N. Z. (2021). Backdoor attacks to graph neural networks. *Proceedings of the 26th ACM Symposium on Access Control Models and Technologies*, 15–26.

Zoldi, S. (2017, September 27) Explainable AI in fraud detection - A back to the future story. *Fico Decisions Blog*. https://www.fico.com/blogs/explainable-ai-fraud-detection-back-future-story

Zoldi, S. M., & Xu, H. (2020). Fraud detection by profiling aggregate customer anonymous behavior (U.S. Patent Application No. US10692058B2). United States Patent and Trademark Office. https://patentimages.storage.googleapis.com/f2/ad/e6/eee6ffd04335ad/US10692058.pdf

Žukauskaitė, A. (2020). Multiplicity as a life: Deleuze, Simondon, Ruyer. In R. Przedpełski & S. E. Wilmer (Eds.), *Deleuze, Guattari and the Art of Multiplicity*. Edinburgh University Press.

Appendices

Appendix A: Codebook

Parent Code	Child Codes
(Mis)users	Cybercriminals Hackers Customers Client Intentional (CI) First Party Fraud Misuse Abuse Take Advantage
Technology and Strategies	Analytics Technology Algorithm Model Prediction Statistical Detection Block Pending Suspend Alert
Policies and Strategies	Interview Investigate Ask Evidence Determine Reimbursement Decision Payout Guidelines Policies Cardholder Agreement Financial Service Agreement
Customer Experience	Fraud Education Campaign User Experience Wait Time Complaints Escalation Regulatory Requirements Media Legal Reputation
Authentication	Text Message SMS In-App

	Mobile Phone Email Phone Call Toll Free Number Biometrics PIN Password Two Step Verification Multi Factor Authentication One-Time Passcode (OTP) SIM Card
Human Vulnerabilities	Loneliness Greed Opportunistic Fear of Authority Curiosity Distress Urgency or Emergency APP Scams Social Engineering Techniques
Automation	RPA Process Map Business Rules Triggers Efficiencies Cost Reduction Service Level Agreement Human Actions Human Decisions Operation Opportunities Operation Risks System Error