Interdisciplinary Journal of Information, Knowledge, and Management

An Official Publication of the Informing Science Institute
InformingScience.org

IJIKM.org

Volume 18, 2023

ECOMMERCE FRAUD INCIDENT RESPONSE: A GROUNDED THEORY STUDY

Joshua Dwight — School of Science, Engineering, and Technology, Royal Melbourne Institute of Technology, Hanoi, Vietnam — Joshua.dwight@rmit.edu.vn

ABSTRACT

Aim/Purpose This research study aimed to explore ecommerce fraud practitioners' experiences and develop a grounded theory framework to help define an ecommerce fraud incident response process, roles and responsibilities, systems, stakeholders, and types of incidents.

Background With a surge in global ecommerce, online transactions have become increasingly fraudulent, complex, and borderless. There are undefined ecommerce fraud roles, responsibilities, processes, and systems that limit and hinder cyber incident response to fraudulent activities.

Methodology A constructivist grounded theory approach was used to investigate and develop a theoretical foundation of ecommerce fraud incident response based on fraud practitioners' experiences and job descriptions. The study sample consisted of 8 interviews with ecommerce fraud experts.

Contribution This research contributes to the body of knowledge by helping define a novel framework that outlines an ecommerce fraud incident response process, roles and responsibilities, systems, stakeholders, and incident types.

Findings An ecommerce fraud incident response framework was developed from fraud experts' perspectives. The framework helps define processes, roles, responsibilities, systems, incidents, and stakeholders. The first finding defined the ecommerce fraud incident response process. The process includes planning, identification, analysis, response, and improvement. The second finding was that the fraud incident response model did not include the containment phase. The next finding was that common roles and responsibilities included fraud prevention analysis, tool development, reporting, leadership, and collaboration. The fourth finding described practitioners utilizing hybrid tools and systems for fraud prevention and detection. The fifth finding was the identification of internal and

Accepting Editor Salah Kabanda | Received: January 12, 2023 | Revised: April 3, April 17, 2023 | Accepted: April 24, 2023.
Cite as: Dwight, J. (2023). Ecommerce fraud incident response: A grounded theory study. *Interdisciplinary Journal of Information, Knowledge, and Management*, *18,* 173-202. https://doi.org/10.28945/5110

	external stakeholders for communication, collaboration, and information sharing. The sixth finding is that research participants experienced different organizational alignments. The seventh key finding was stakeholders do not have a holistic view of the data and information to make some connections about fraudulent behavior. The last finding was participants experienced complex fraud incidents.
Recommendations for Practitioners	It is recommended to adopt the ecommerce fraud response framework to help ecommerce fraud and security professionals develop an awareness of cyber fraud activities and/or help mitigate cyber fraud activities.
Future Research	Future research could entail conducting a quantitative analysis by surveying the industry on the different components such as processes, systems, and responsibilities of the ecommerce fraud incident response framework. Other areas to explore and evaluate are maturity models and organizational alignment, collaboration, information sharing, and stakeholders. Lastly, further research can be pursued on the nuances of ecommerce fraud incidents using frameworks such as attack graph generation, crime scripts, and attack trees to develop ecommerce fraud response playbooks, plans, and metrics.
Keywords	cyber incident response, ecommerce fraud, fraud prevention, grounded theory

INTRODUCTION

Online payments and ecommerce have significantly increased in use and adoption globally (Ali et al., 2018; Marchal & Szyller, 2019; Singh & Jain, 2019; Wickramanayake et al., 2020). However, ecommerce fraud incidents are some of the most prevalent and underreported cybercrimes in the Internet era, costing global organizations and nations billions of dollars each year (Cross, 2018; Donegan, 2019; M. He et al., 2018; Kemp, 2020; Park et al., 2019; Smith, 2008). Global ecommerce online payment fraud has resulted in an estimated $41 billion of losses (Statista, 2022). With the surge in global ecommerce, online transactions have become increasingly fraudulent, complex, and borderless (Kolodiziev et al., 2020; Minastireanu & Mesnita, 2019).

Cyber incidents and vulnerabilities are nearly limitless and unavoidable (Mugari, 2017; Onwubiko & Ouazzane, 2020; Rollason-Reese, 2003) and can stem from internal areas of an organization or from outside the organization. Ecommerce fraud incidents are not new but continue to evolve in sophistication and organization with technological advancements and mechanisms such as the Internet and social media to perpetrate fraudulent activities (Albakri et al., 2018; Cross, 2018). Payment security, in particular, is a significant and important concern for merchants and consumers (Chen et al., 2019). K. Huang et al. (2018) also suggest that corporations reacting passively to combat cybercrimes are losing the battle against cybercriminals. Levi et al. (2017) indicate it is difficult for ecommerce stakeholders to respond appropriately to cyber fraud because there is a lack of reliable data on the problem, a lack of best practices, the capacity to respond, and the motivation to mitigate. Early threat discovery (Adamov & Carlsson, 2016), fast incident response (Adamov & Carlsson, 2016), and the complex, interdisciplinary nature of cybercrimes also present major challenges (Bednar et al., 2014; Doeland, 2017; Zibak & Simpson, 2019).

These challenges continuously plague organizations and make it difficult for ecommerce organizations to act effectively and efficiently to prevent incidents. Thus, it is imperative to respond quickly and effectively to cyber incidents (Onwubiko & Ouazzane, 2020). Incident response can minimize loss, theft, and disruptions but depends on the personnel's availability, knowledge, and ability to deal with the magnitude of an incident (Van der Kleij et al., 2017). However, much of the academic literature on cyber incident response focuses topically on cyber security and does not focus on the

ecommerce industry at large. Therefore, it is important to establish a methodical incident response approach for ecommerce fraud-related incidents to mitigate the growing threats.

Even though cyber incident response and ecommerce fraud have been researched by academic, private, and public organizations for many years, the literature has not connected these two important areas. The major ecommerce fraud and cyber incident response gaps are the undefined ecommerce fraud roles, responsibilities, processes, and systems (Krambia-Kapardis & Zopiatis, 2010; Marchal & Szyller, 2019; Onwubiko & Ouazzane, 2020; Van der Kleij et al., 2017). This study co-constructs a framework based on the experiences of ecommerce fraud stakeholders with fraud and cyber incident response to explore these gaps. The purpose of this qualitative study aimed to explore these fraud industry experiences and develop a Grounded Theory framework to help define an ecommerce fraud incident response process, roles and responsibilities, systems, stakeholders, and incident types.

This paper is an adaptation of the author's unpublished dissertation. The content is organized as follows. The literature review section of this study centers on cyber incident response and ecommerce to generate general themes and areas of comparison for the Constructivist grounded theory study and also identifies gaps in the literature. The methodology section outlines the Constructivist grounded theory research method, sampling and data collection, and description of participants. The results section presents the findings culminating in the ecommerce fraud incident response framework. The discussion section discusses and compares the grounded theory framework against the literature review and identifies the academic and practical contributions, limitations, and future areas of study.

LITERATURE REVIEW

A literature review was commenced to understand and generate generic themes and areas for comparison for this Constructivist grounded theory study. The first area generates a theoretical cyber incident response model based on the academic literature. The second area reviews the ecommerce fraud ecosystem to outline the people, processes, and systems. The last section focuses on the gaps in the literature.

CYBER INCIDENT RESPONSE

The academic literature has defined cyber incident response in slightly different ways. Lamis described an incident as any unintended negative activity against an information security system (2010). Sun et al. (2019) suggested incidents are unauthorized activities against a computer system that violates a security policy. An incident is a violation or imminent threat of computer security policies, acceptable use policies, or standard security practices (Van der Kleij et al., 2017). Onwubiko and Ouazzane (2020) suggested cyber incidents are often unannounced, urgent, abrupt, and have serious consequences.

The purpose of incident response is to provide a framework for an orderly, coordinated response within a firm (Rollason-Reese, 2003). A benefit of incident response is handling an incident efficiently and consistently. Adequate handling of an incident can minimize loss, theft, and disruptions. Adequate incident handling depends on the personnel's availability, knowledge, and ability to deal with the magnitude of an incident. Ideally, incident response personnel will analyze incident data, determine the impact of the incident, and act appropriately to limit the damage and restore normal services (Van der Kleij et al., 2017).

Many organizations have developed incident response frameworks and methodologies for their people, processes, and systems. Much of the academic literature provided slight variations on similar phases, processes, and activities of the incident response approach. This section reviews academic literature to identify various incident response models.

Rollason-Reese (2003) suggested the incident response model has five phases. These phases are alert, analysis, response, recovery, and maintenance. The maritime information incident response model included prevention, detection, response, and recovery (Pinto & Talley, 2006). Lamis (2010) presented the incident response model as a process to mitigate, investigate, and learn from incidents. The phases included preparation, identification, containment, eradication, recovery, and follow-up. Ruefle et al. (2014) presented an incident response lifecycle that consists of identification, declaration, analysis, response, knowledge, and closure and includes reporting, situational awareness, detection, triage, analysis, and response. The conventional incident response model consisted of six phases: preparation, discovery, containment, investigation, threat analysis, and remediation. A cloud incident response model includes seven phases. The phases are preparation, discovery, containment, investigation, remediation, prevention, and lessons learned (Adamov & Carlsson, 2016). The incident lifecycle presented identification and declaration, analysis, response, and lessons learned phases (Jalal et al., 2018). Al-Dhaqm et al. (2020) suggested the incident phases include pre-incident response, incident response, and post-incident response. Pre-incident activities focused on security policy development and incident response activities related to containment, investigation, and response. Post-incident activities included lessons learned and improvement. Moreno et al. (2020) defined the incident response model as preparation, identification, analysis, containment, eradication, recovery, and lessons learned. The cyber threat response model included identifying, protecting, detecting, responding, and recovering (Sadik et al., 2020). The general approach to incident response has four phases. These phases are preparation, detection and analysis, containment, and lessons learned (Pilitsky et al., 2021).

The proposed incident response model included six phases based on the academic literature reviewed above. The phases are preparation and planning, discovery and detection, containment and continuity, analysis and investigation, response and recovery, and improvement. Table 1 illustrates the comparison between academic cyber incident response models.

Table 1. Comparison of the academic literature incident response models

IR phases	*Preparation*	*Detection*	*Containment*	*Analysis*	*Response*	*Improvement*
Rollason-Reese, 2003		X	X	X	X	X
Pinto & Talley, 2006		X	X		X	
Lamis, 2010	X	X	X		X	X
Ruefle et al., 2014		X	X	X	X	X
Adamov & Carlsson, 2016	X	X	X	X	X	X
Jalal et al., 2018		X		X	X	X
Al-Dhaqm et al., 2020	X		X	X	X	X
Sadik et al., 2020		X	X		X	
Pilitsky et al., 2021	X	X	X	X	X	X
Y. He et al., 2022	X	X	X	X	X	X

Preparation and planning

Organizations need to proactively prepare and plan for cyber-attacks. Albakri et al. (2018) indicated a preparational need for awareness and mitigation of threats before cyber-attacks occur. This phase includes developing a foundation to protect an organization's systems, processes, and people from cyber threats and supports incident prevention and response efforts. The planning and preparation phase included personnel acquisition, the development of organizational and operational policies, situational awareness and cyber threat intelligence, and playbook development.

The preparation and planning phase helps determine the resources necessary to combat threats and vulnerabilities, such as the tools, methods, and personnel. The tools can include tracing software, security patches, and resource kits. Methods can include policies and procedures. The preparation phase included constructing a playbook or incident handling plans and identifying data sources (Moreno et al., 2020; Onwubiko & Ouazzane, 2020).

Discovery and detection

Detection and discovery refer to monitoring systems and networks to identify malicious, suspicious, or anomalous events (Midi et al., 2016; Ruefle et al., 2014). Incident responders receive notification of an actual or potential threat from an incident detection system (IDS). An initial alert may come from firewalls, virus software, recipients of threatening emails, third parties, and other sources (Adamov & Carlsson, 2016; Rollason-Reese, 2003).

The detection and discovery phase determines whether an event is an incident or not. Typical classifications utilize Likert scales on impact and likelihood (Lamis, 2010). Lamis (2010) noted the impact levels high, medium, and low severity levels could be associated with severe impact, significant impact, and minimal impact, respectively. Moreno et al. (2020) suggested the incident response discovery and detection phase has four major activities. The incident must be properly identified, categorized, prioritized, and communicated.

Rule-based automation tools can be used for the detection and discovery of incidents. The rules look for specified patterns and can trigger different actions, such as sending notifications to the incident response team or preventing an attack (Pilitsky et al., 2021). For monitoring the Internet of Things (IoT), Midi et al. (2016) suggested involving a lightweight prevention IDS to include an event-condition-action paradigm for resource-constrained hardware or software. After discovery, detection, prevention, identification, and classification, an organization can implement several potential actions to contain an incident and return core business processes to normal operations.

Containment and continuity

The containment and continuity phase focused on mitigating the impact of the incident by preventing further damage and returning systems, processes, and people to the average business state (Adamov & Carlsson, 2016; Moreno et al., 2020). Depending on the severity of the incident, containment activities included disabling systems and services, changing or configuring systems and services, installing patches, expelling malicious attackers, and removing compromised systems (Adamov & Carlsson, 2016; Lamis, 2010; Moreno et al., 2020). This phase also included short-term continuity efforts. Continuity refers to ensuring core processes remain operational. Continuity may mean using manual processes or backup systems to reduce the impact on consumer and business units.

Analysis and investigation

Analysis and investigation entailed acquiring sufficient knowledge about an incident and the state of the systems, processes, and people impacted (Midi et al., 2016). A cybercrime (incident) investigation may include hardware, software, and storage containing private business data (Bednar et al., 2014). Al-Dhaqm et al. (2020) suggested that incident investigation includes preserving data, preparing an

investigation environment, analyzing data, reconstructing a timeline of events, searching for evidence, and creating documentation.

Adamov and Carlsson (2016) presented creating a forensic image duplication for data collection and analysis. Incident analysis can utilize different aspects, including the type of attackers, types of exploit tools, vulnerabilities exploited, attackers' actions, targets, unauthorized results of incident, and objectives of attacker step by step (Sun et al., 2019). Adamov and Carlsson (2016) suggested creating a threat analysis report that explains the attack and recommends remediation efforts.

The threat analysis phase emphasizes a quick and informed decision to prevent further damage (Rollason-Reese, 2003). Threat intelligence analyzes threat actors, including their capabilities and motivation and how they use the cyber domain to achieve their aims. In practice, threat intelligence analysis is used to determine facts and derive reliable conclusions. These conclusions can assist in decision-making and facilitate operational processes such as detection, prevention, and response (Zibak & Simpson, 2019). When the analysis is complete, the organization must resolve the incident and recover the systems, people, and processes.

Response and recovery

After completing the analysis and investigation, incident response teams must fix the problem (Al-Dhaqm et al., 2020). The response and recovery phase refers to preventing the reoccurrence of a specific attack by eliminating the incident and vulnerability and restoring all impacted and/or compromised systems and services back to normal operations (Adamov & Carlsson, 2016; Lamis, 2010; Rollason-Reese, 2003). Response and recovery activities can include removing malicious code, recovering systems from backups, system configuration, and account management (Adamov & Carlsson, 2016). Various response plans and playbooks should document these activities.

The incident response team should deploy the incident response plans and playbooks in this phase. These plans and playbooks can use automated activities, manual activities, and/or some combination of both. Automation is beneficial as notifications can assign tasks based on predesigned incident response plans or playbooks (Pilitsky et al., 2021), which reduces response and recovery time. Once the incident response team has completed remediation and recovery efforts, the team needs to document the lessons learned to improve the organization's people, processes, and systems.

Continuous improvement and lessons learned

The last phase of the incident response methodology was continuous improvement and lessons learned. This phase focused on documenting the incident in the knowledge base, formally closing the incident, and improving the information security structure and system (Moreno et al., 2020). Lessons learned review reflect on the incident response processes and procedures to identify strengths, weaknesses, and opportunities for improvement (Lamis, 2010; Rollason-Reese, 2003). The end of the incident response lifecycle entails transforming lessons learned into security improvement activities (Moreno et al., 2020).

The continuous improvement phase changes the information security system, people, and processes to address vulnerabilities caused or exploited by the incident. Changes could include updating policies, protocols, vulnerabilities, documentation, staff training, and detection rules based on the information collected after each incident is discovered and dealt with (Adamov & Carlsson, 2016; Al-Dhaqm et al., 2020; Pilitsky et al., 2021). The incident response lifecycle starts anew once the continuous improvement phase is completed. Figure 1 illustrates the cyber incident response model based on the academic literature.

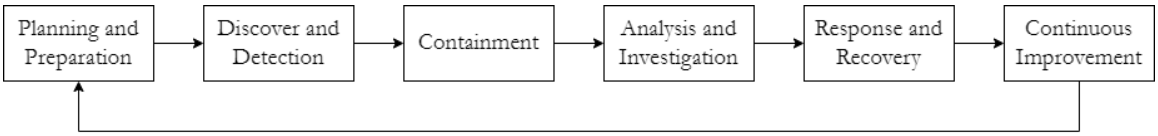

Figure 1. Academic cyber incident response model

This section of the literature review has established a comprehensive incident response model and methodology and defined the relevant components of each phase. Each of these cyber incident response phases can pertain to ecommerce fraud, but the literature is very limited when it comes to implementing cyber incident response to specific industries, people, processes, and systems. Fraud prevention roles and responsibilities in organizations are murky, and it is unclear who should assume the role (Krambia-Kapardis & Zopiatis, 2010). Private and public organizations struggle to define and allocate the roles, responsibilities, and expertise of team members, including outside groups and organizations involved in incident response (Simola, 2019; Van der Kleij et al., 2017).

Ecommerce fraud incidents have been incredibly cumbersome with the rise of the Internet. Many private and public organizations are trying to determine and use the appropriate analytical systems, tools, and methods to fight fraudulent incidents in ecommerce. The following section provides an overview of the fraud ecommerce ecosystem, exploring fraud incidents, stakeholders, fraud analytical models, and methodologies.

Ecommerce Fraud Ecosystem

Ecommerce overview

Online payments and ecommerce have significantly increased in use and adoption globally (Ali et al., 2018; Marchal & Szyller, 2019; Singh & Jain, 2019; Wickramanayake et al., 2020). Wilks (2019) specified US card payments reached over a billion payments worth trillions of dollars. Additionally, smartphones are increasingly playing a more significant role in ecommerce and online payments (Chen et al., 2019). Technologies have enabled digital transformation for businesses and payment transactions to occur within a day or instantaneously by improving the speed of the settlement processes (Chen et al., 2019; Diadiushkin et al., 2019; Eappen, 2019; Mugari, 2017; Park et al., 2019).

Ecommerce is the exchange of money for products or services over the Internet. Online payment systems have increased the efficiency and effectiveness of conducting business-to-consumer (B2C), business-to-business (B2B), and consumer-to-consumer (C2C) transactions (Chen et al., 2019). Consumers can engage in ecommerce through websites and mobile sites to search for product and service information and purchase products and services. Consumers will generally go through several phases as they engage in ecommerce transactions, including choosing an e-retailer, products, and services, check out (payment and shipping), and logistical delivery (Vakulenko et al., 2019).

Online payment systems provide a way to complete the purchase and checkout process. There are many stakeholders that can be involved in an ecommerce payment transaction. Payment security, in particular, is a significant and important concern for merchants and consumers (Chen et al., 2019). Cyber fraud incidents are the use of online criminal deception and theft intended to result in financial and/or personal gain (Diadiushkin et al., 2019; Park et al., 2019). Ecommerce fraud prevention relies on rule-based detection systems. With the surge in global ecommerce, online transactions have become increasingly fraudulent, complex, and borderless (Kolodiziev et al., 2020; Minastireanu & Mesnita, 2019). This section covers ecommerce payment systems, fraud stakeholders, fraud incidents, and fraud prevention.

Ecommerce online payment system types

Online payments are efficient and convenient but are complex and expensive to process (Wilks, 2019). There are four main online payment systems in ecommerce. The four systems are card-based, mobile payments, electronic fund transfers, and electronic money. Card-based methods may consist of credit cards, debit cards, magnetic stripe cards, smart cards, and contactless cards to commence. Mobile payments may incorporate mobile apps with smartphones, tablets, and laptops to conduct transactions. Electronic funds transfers use the Internet, email, and applications to perform transactions. Electronic money uses digital wallets with software and hardware to carry out transactions (Chen et al., 2019). These payment systems may or may not use the same components and technology. Even though online payments have helped with the efficiency and effectiveness of conducting transactions, online payments are complex and susceptible to fraudulent activities.

Ecommerce stakeholders

Ecommerce stakeholders are the people and organizations involved in the completion of ecommerce transactions and for the prevention, detection, and response to ecommerce fraudulent behaviors. Payment fraud detection has become popular among payment gateways, payment aggregators, banks, merchants, and customers who conduct transactions online (Wickramanayake et al., 2020). Many different stakeholders are involved in combating and preventing fraud activities and incidents (Doeland, 2017). Fraud detection relies heavily on user input, user behavior, and information about the consumer (Wang et al., 2018). The key stakeholders in combating ecommerce fraud are the issuer, acquirer, payment processor, card network, merchant, consumer, and law enforcement (Artikis et al., 2017; Doeland, 2017; Wilks, 2019).

The card networks, such as Visa and Mastercard, generally set the rules for card use in conjunction with financial institutions (Wilks, 2019). The issuer is the bank issuing credit cards and holding the consumers' accounts. The acquirer is the bank holding the merchants' accounts. The payment processor is the organization responsible for communicating payment information between the issuer bank and the merchant bank to settle the transaction (Artikis et al., 2017). Customers will typically conduct transactions on a merchant's (retailer) ecommerce site. If any fraudulent incidents occur, financial institutions, merchants, customers, and other organizations can report and work with law enforcement and each other to resolve fraudulent incidents. However, Donegan (2019) suggested only three to four percent of ecommerce fraud cases reported to law enforcement are disseminated and investigated. Figure 2 outlines the ecommerce fraud incident stakeholders and potential communication.

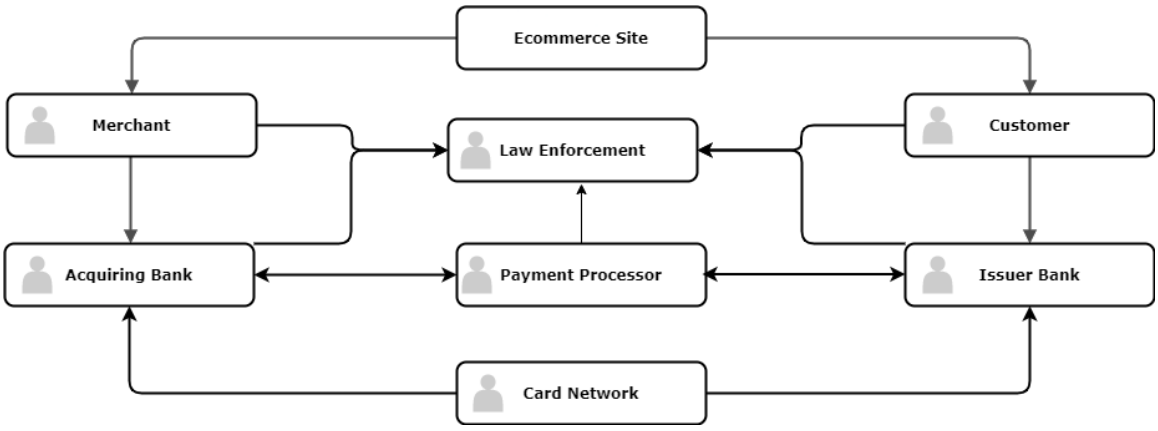

Figure 2. Ecommerce fraud stakeholders

Ecommerce fraud incidents

Ecommerce became a core competency for many retailers and merchants, but conducting transactions with e-payments became a critical issue due to fraud (T. Huang & Huang, 2019). Cyber fraud is online criminal deception and theft intended to result in financial and/or personal gain using Internet technologies (Diadiushkin et al., 2019; Park et al., 2019). Global ecommerce online payment fraud has resulted in an estimated $41 billion of losses (Statista, 2022). Wang et al. (2018) noted the fraud rate in the Chinese peer-to-peer payment market is estimated to be over 10%. Marchal and Szyller (2019) suggested multiple attacks and fraudulent ecommerce orders are orchestrated by groups of professional fraudsters, also known as organized crime. Kawase et al. (2019) noted many organizations struggle with legacy fraud verification platforms.

Amasiatu and Shah (2018) presented that ecommerce organizations suffer growing losses from fraudulent activities from online retail. There are four major fraud incidents in ecommerce, which are identity theft, mandate fraud, credit card fraud, and digital wallet fraud (Donegan, 2019; T. Huang & Huang, 2019). T. Huang and Huang (2019) suggested many fraudulent activities occur due to social engineering attacks caused by lost and stolen card information, account takeovers (ATO), and card not present (CNP) transactions.

Mandate fraud involves a fraudster convincing a customer to change a payment process by pretending to be a company that receives the payments (Donegan, 2019). This fraud scheme is typically completed by compromising and accessing a customer's email account. Payment card fraud can be considered one of the biggest cybercrimes and threatens a trustworthy digital ecosystem (Stojanović et al., 2021; Wickramanayake et al., 2020). Much like payment cards, digital wallets are susceptible to similar fraudulent techniques. The fraudulent attacks can include social engineering using text messages and phone calls asking for personal information, malware attacks such as ransomware, or man-in-the-middle attacks such as fake websites (Fadhilah et al., 2021; Levitin, 2018). This would suggest that ecommerce fraud and cyber security incident professionals are needed to mitigate ecommerce incidents.

Ecommerce fraud prevention systems

Many organizations have been combating ecommerce fraud with detection platforms with rule-based approaches (Diadiushkin et al., 2019; Kawase et al., 2019). A rules-based system is a special type of expert system consisting of if-then rules used for classification, regression, and association (Liu et al., 2016). Kawase et al. (2019) suggested several machine-learning models can help identify, prevent, predict, and detect fraudulent behavior. Yasaka (2020) noted detecting suspicious transactions has evolved from manual data analysis to deep learning and artificial intelligence. Organizations can employ artificial intelligence and machine learning techniques to detect suspicious transactions, then a human to validate and verify (Yasaka, 2020). Much of the ecommerce literature focuses on machine learning detection methods but not on response processes.

The literature showcases similar aspects to cyber incident response but does not specifically connect the two areas together. Additionally, most of the academic taxonomy construed refers to fraud as attacks rather than incidents. What are the gaps between cyber incident response and ecommerce fraud?

Gaps in Literature

The main gap is that literature was limited and/or vague about the connection between ecommerce fraud and cyber incident response; specifically, the lack of processes, roles and responsibilities, systems, stakeholders, and types of incidents. Table 2 specifies the identified gaps in the academic literature and respective authors.

Smith (2008) suggested that systems for responding to fraud are disparate and uncoordinated across private and public sectors. Fraud prevention roles and responsibilities in organizations are murky, and

it is unclear who should assume the role (Krambia-Kapardis & Zopiatis, 2010). Private and public organizations struggle to define and allocate the roles, responsibilities, and expertise of team members, including outside groups and organizations involved in incident response (Simola, 2019; Van der Kleij et al., 2017). Dsouza (2018) noted that incident response teams inconsistently collect and define information, derailing the comparison of cyber and fraud incidents. Specifically, inconsistencies involve terminology and taxonomy, categorization of attacks, threats, vulnerabilities, and data presentation methods. Levitin (2018) specified fraud incidents could be exacerbated due to confusion about who to contact when fraud occurs for consumers and merchants due to undefined roles and processes between ecommerce stakeholders involved in online payments. Onwubiko and Ouazzane (2020) discussed a lack of a coordinated operational and technical framework for prevention, detection, response, and recovery that includes the taxonomy, stakeholders, and other departments. To explore this phenomenon and develop an ecommerce fraud response framework, a qualitative analysis study was conducted.

Table 2. Literature gaps between ecommerce fraud and cyber incident response

Gaps	*Authors*
Roles and responsibilities	Krambia-Kapardis & Zopiatis, 2010; Simola, 2019; Van der Kleij et al., 2017
Processes	Dsouza, 2018; Levitin, 2018; Onwubiko and Ouazzane, 2020
Stakeholders	Levitin, 2018; Onwubiko and Ouazzane, 2020; Simola, 2019; Van der Kleij et al., 2017; Levitin, 2018
Systems	Onwubiko and Ouazzane, 2020
Types of incidents	Donegan, 2019; T. Huang & Huang, 2019; Fadhilah et al., 2021; Levitin, 2018

METHODOLOGY

This study employed a qualitative methodology because it seemed best suited to explore ecommerce fraud incident response due to the complex nature and limited academic literature specific to ecommerce fraud incident response.

Glaser and Strauss (1967) first developed the grounded theory in the 1960s but have since diverged into different variations of the initial theory (Charmaz & Thornberg, 2020; Yu & Smith, 2021). Charmaz (2006) built upon the grounded theory with the constructivist grounded theory model. This model focused on co-constructing experiences and meaning between the researcher and participants (Tie et al., 2019). Tie et al. (2019) suggested that the constructivist theory uses initial coding, focused coding, and theoretical coding techniques. The constructivist approach suggests conducting a literature review that will help researchers gain knowledge in the research problem or area, composing research questions, stimulating theoretical sensitivity, directing theoretical sampling, and providing additional evidence and validity to the research (Yu & Smith, 2021).

In the constructivist approach, there are four main grounded theory quality components. These are credibility, originality, resonance, and usefulness (Charmaz & Thornberg, 2020). Credibility refers to having sufficient relevant data for asking intelligent questions about the data, making systematic comparisons throughout the research process, and developing a thorough analysis. Originality refers to whether the theory offers new insights into a problem and establishes the significance of the analysis. Resonance is whether the theory and researcher have constructed concepts to represent the research participants' experiences and provide insights to others. Usefulness focuses on whether the research clarifies the research participants' experience, forms foundations for the policy or practical

applications, contributes to a new line of research, and reveals pervasive processes and practices (Charmaz & Thornberg, 2020).

Research Approach

The steps are purposive sampling, generating and collecting data, initial coding, intermediate coding, and advanced coding. Appendix A shows a sample of coding. The first step, purposive sampling, entails intentionally selecting participants that can answer the research question. The second step is generating and collecting data. For this qualitative study, iterative interviews were conducted with the appropriate ecommerce professionals. Appendix B showcases the interview questions for this study. The third step is initial coding to identify the initial categories. The fourth step is intermediate coding focuses on selecting core categories and reviewing data until thematic saturation is reached. The fifth step is advanced coding, in which the researcher determines a storyline or theoretical narrative (Tie et al., 2019). Figure 3 showcases the approach.

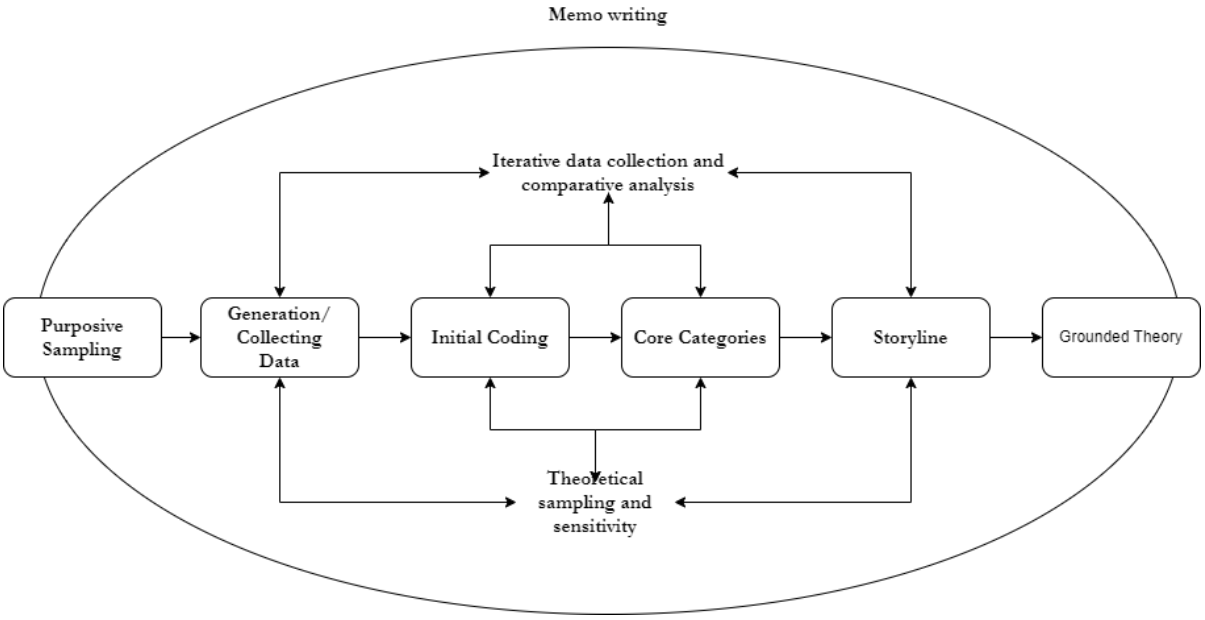

Figure 3. Constructivist grounded theory approach

Note: Steps of the Constructivist Grounded Theory Approach (adapted from Tie et al., 2019).

This study used the Quirkos qualitative analysis software to help with initial coding and identifying categories from the interview transcripts. Evers et al. (2020) specified Quirkos as a software tool that provides fundamental data analysis functionalities. Alammar et al. (2019) described Quirkos as a data visualization tool that allows researchers to code transcripts into categories or themes. The coding is color-coordinated, and as themes or categories increase in frequency, the bubbles become more prominent. The coding process starts with creating Quirks (labels), which are then assigned to chunks of text. Themes are derived inductively through this process in Quirkos (Evers et al., 2020).

Sampling and Data Collection

The primary source of data for this qualitative grounded theory study was interviews. A total of eight interviews were conducted to capture the experiences, feelings, and insights of ecommerce fraud practitioners regarding ecommerce fraud response activities. There are an estimated 50,000 ecommerce fraud practitioners worldwide. Purposive sampling was used to find participants with over five years of work experience in the field. Participants were recruited online using digital flyers on LinkedIn and trade association sites. The participants were asked open-ended questions (see

Appendix B). Each interview was scheduled for 60 minutes and was conducted upon reaching a data saturation point (Dwight, 2022).

Description of the Participants

The sample's demographics comprised various ecommerce professionals representing fraud-related positions across different industries and global regions. The research participants' experience levels varied from five to twenty years of experience. The research participants educational levels spanned from no college to completion of graduate-level degrees. Table 3 showcases the participants' experience and education levels (Dwight, 2022).

Table 3. Participant fraud experience and education level

Participant	*Years of experience*	*Education level*
Participant 1	5+	Technical college
Participant 2	20+	Master's degree
Participant 3	5+	NA
Participant 4	10+	Bachelor's degree
Participant 5	5+	Bachelor's degree
Participant 6	5+	Bachelor's degree
Participant 7	5+	Master's degree
Participant 8	10+	Technical college

Table 4 presents the participants' industries and regions. The research participants represented merchants, banks, fraud solution providers, and non-profits in the ecommerce ecosystem. The research participants who contributed to this study worked in North America and Europe (Dwight, 2022).

Table 4. Participant stakeholder type and region

Participant	*Stakeholder*	*Region*
Participant 1	Ecommerce merchant	North America
Participant 2	Bank	Europe
Participant 3	Ecommerce merchant	North America
Participant 4	Fraud solution provider	North America
Participant 5	Ecommerce merchant	North America
Participant 6	Ecommerce merchant	North America
Participant 7	Non-profit community group	North America
Participant 8	Fraud solution provider	Europe

IRB Approval

This study was reviewed and approved by the university's Institutional Review Board (IRB). It was declared exempt under 45 CFR 46.101(b). The approval was limited to the approved protocols described in the application, which have been reviewed as acceptable activities outlined by the Office of Human Research Protections.

Results

The ecommerce fraud incident response is a critical process to establish in an organization. The objective of this study is to explore the phenomena and develop a grounded theory framework to help

define an ecommerce fraud incident response process, roles and responsibilities, systems, stakeholders, and incident types. The results section first provides a summary of the findings. Next, the results construct each component of the ecommerce fraud response framework: processes, roles, responsibilities, systems, stakeholders, and fraud incidents from the findings. The final area of this section illustrates the constructed ecommerce fraud response framework.

Summary of Findings

The first finding defined the ecommerce fraud incident response process. The process includes planning, identification, analysis, response, and improvement. The second finding was that the fraud incident response model did not include the containment phase. The next finding was that common roles and responsibilities included fraud prevention analysis, tool development, reporting, leadership, and collaboration. The fourth finding described practitioners utilizing hybrid tools and systems for fraud prevention and detection. The fifth finding was the identification of internal and external stakeholders for communication, collaboration, and information sharing. The sixth finding is that research participants experienced different organizational alignments. The seventh key finding was stakeholders do not have a holistic view of the data and information to make some connections about fraudulent behavior. The last finding was participants experienced complex fraud incidents (Dwight, 2022).

Processes

The first finding is the participants described five major processes of planning, identification, analysis, response, and improvement. The research participants described hypothesis creation, playbook development, vulnerability assessments, and fraud awareness as frequent planning activities. In the second phase of research, participants described flags, alerts, triggers, monitoring, filtering, discovery, and detection as identification activities. In the third phase of research, the experts discussed analysis and investigation to find connections and patterns between data points and information. In the fourth phase, participants depicted response activities consisting of stopping orders, processing orders, chargebacks, and rule implementation. The last phase of improvement illustrates training, learning, tools, systems, rule updates, and implementation. Table 5 illustrates the initial coding, frequency, core categories, and major themes.

Table 5. Qualitative coding of e-commerce fraud incident response

Initial coding	*Frequency*	*Core category*	*Storyline*
Hypothesis creation	2	Planning activities	Ecommerce Fraud Response activities to prepare and plan for potential ecommerce fraud incidents.
Playbook/plan	3		
Vulnerability assessment	7		
Fraud awareness	12		
Flags/alerts/triggers	23	Identification activities	Ecommerce Fraud Response activities to detect and identify ecommerce fraud incidents.
Monitoring	6		
Detection	21		
Filter	38		
Identify/discover	16		
Analysis	21	Analysis and investigation activities	Ecommerce Fraud Response activities to analyze and investigate ecommerce fraud incidents to find connections and patterns.
Investigate/investigation	7		
Connections/patterns	15		
Data points	7		
Data/information	129		

Initial coding	*Frequency*	*Core category*	*Storyline*
Implement rules Stop/decline bad orders Process good orders Chargebacks	3 3 15 15	Response activities	Ecommerce Fraud Response activities to respond to ecommerce fraud incidents.
Learning/training Tool and system Rule updates Rule implementation	16 6 4 3	Improvement activities	Ecommerce Fraud Response activities to continuously improve processes, systems, and people.

The second finding was the ecommerce fraud incident response process did not include a containment phase. This is reviewed in the Discussion section under Processes, Systems, and Roles.

Roles and Responsibilities

The third finding that arose from the research participant's experiences regarding common roles and responsibilities include tool development, reporting, leadership and management, and fraud prevention. Tool development is defined as the creation of internal and external fraud prevention tools. Reporting is the metrics and key performance indicators related to fraud prevention. Leadership and management focused on managing and developing people. Collaboration refers to information sharing with internal and external stakeholders for fraud planning, detection, analysis, response, and improvement. Fraud prevention analysis is the fraud prevention and response activities used in the fraud ecommerce incident response process. Fraud prevention analysis was the most prominent role and responsibility of the research participants.

Participants 1 and 8 experienced reporting, leadership, management, collaboration, and fraud prevention analysis. Participant 6 experienced tool development, collaboration, and fraud prevention analysis. Participants 2, 3, 4, 5, and 7 experienced all five roles and responsibilities. For example, Research Participant 2 specified, "We could really see that this [fraud] is getting more and more sophisticated. We developed some tools, and they really worked well". Table 6 showcases the common roles and responsibilities experienced and discussed by each participant.

Table 6. Participant experiences of roles and responsibilities

Participant	*Tool development*	*Reporting*	*Leadership & management*	*Collaboration*	*Fraud prevention analysis*
Participant 1		x	x	x	x
Participant 2	x	x	x	x	x
Participant 3	x	x	x	x	x
Participant 4	x	x	x	x	x
Participant 5	x	x	x	x	x
Participant 6	x			x	x
Participant 7	x	x	x	x	x
Participant 8		x	x	x	x

Systems and Tools

The fourth finding described practitioners utilizing hybrid tools and systems for fraud prevention and detection. The participants described several fraud prevention tools and systems. The participants

noted using internally developed tools and third-party systems to help detect and prevent fraud. Rule-based systems arose 57 times, and third-party systems occurred 20 times during the interviews. This finding suggests the participants used multiple tools and systems as a hybrid approach for their detection, investigation, and analysis. The participants mentioned a mix of open-source and third-party proprietary software such as "3D Secure", "Google Analytics," "Forensically," "Maxmind," and "Ekata." Table 7 shows the fraud prevention systems and tools experienced by the participants.

A rules-based system is a special type of expert system consisting of if-then rules (Liu et al., 2016). Open-source intelligence (OSINT) tools are typically free or low-cost tools for gathering data and information (Hwang et al., 2022). Third-party tools refer to the use of commercial software purchased and used for fraud prevention, detection, and response. Participants 1, 2, and 8 specified using rule-based and third-party commercial software. Participants 3, 5, and 6 noted using rule-based, third-party software and OSINT systems and tools. Participant 4 only identified a rule-based approach, and participant 7 only used a database for analysis.

Table 7. Participant experiences with fraud prevention systems and tools

Participant	*Systems and tools*	*Core Category*
Participant 1	Rule-based, third-party	Hybrid systems
Participant 2	Rule-based, third-party	
Participant 3	Rule-based, OSINT, third-party	
Participant 4	Rule-based	
Participant 5	Rule-based, OSINT, third-party	
Participant 6	Rule-based, OSINT, third-party	
Participant 7	Database	
Participant 8	Rule-based, third-party	

Stakeholders

The fifth finding was the identification of internal and external stakeholders for communication, collaboration, and information sharing. Internal stakeholders are individuals that work within the same company. Identifying and building relationships are essential aspects of information sharing. The research participants identified nine internal stakeholders and eleven external stakeholders. The internal stakeholders described by the research participants include customer service, information security, legal, shipping and warehouse, data teams, accounting, IT teams, payments teams, and product teams. The research participants described customer service, information security, and shipping internal teams and departments frequently. Legal, accounting, product, and data teams were rarely discussed. Table 8 illustrates internal stakeholders' initial coding, frequency, and core category.

Table 8. Qualitative coding of internal stakeholders

Initial coding	*Frequency*	*Core category*	*Storyline*
Customer service team	18	Internal stakeholders	Internal stakeholders help provide communication, collaboration, and information sharing throughout the response phases.
Information security team	11		
Legal team	2		
Shipping/warehouse team	20		
Data team	3		
IT Team	7		
Payments team	6		
Accounting	1		
Product team	1		

Internal stakeholders can generally fall under business, technical, or both. Technical departments can consist of information security, data, and IT. Research Participant 5 discussed how collaboration helps with fraud mitigation. He specified:

> We have a monthly meeting with them [information security team] to go over incidents that pop up that might kind of impact those teams. Like, card testing is one that is kind of in that middle ground … So, we meet with them monthly to go over situations like that. We have open communication lines with both our dropship and support, our stock order support, and our traffic team because if an order does successfully get past our filter and then we find out about it.

The sixth finding is that research participants experienced different organizational alignments. Even though there is communication and collaboration internally in organizations, research participants noted having different organizational alignments. This is examined in the discussion section of the paper.

The external stakeholders experienced by the research participants are merchants, issuing banks, acquiring banks, payment service providers, fraud solution providers, card networks, law enforcement, customers, community groups, workgroups, and non-profit organizations. The research participants described customers/victims, banks, and fraud solution providers most frequently. Payment service providers and work groups were rarely discussed. Table 9 displays the initial coding, frequency, and core category for external stakeholders experienced by the research participants.

Table 9. Qualitative coding of external stakeholders

Initial coding	*Frequency*	*Core category*	*Storyline*
Payment service provider	2	External Stakeholders	External stakeholders can help provide communication, collaboration, and information sharing throughout the response phases.
Fraud community	6		
Workgroups	2		
Merchant	31		
Issuing bank	14		
Acquiring bank	4		
Fraud solution provider	20		
Card networks/schemes	9		
Law enforcement	18		
Customer/victim	53		
Non-profit associations	6		

Figure 4 showcases the potential collaboration and information sharing between the various external stakeholders.

Another key finding was stakeholders do not have a holistic view of the data and information to make connections about fraudulent behavior. Key stakeholders have different pieces of data that need to be shared to identify and detect fraudulent actions and behavior. The research participants also specified missing data that could help each stakeholder. Research Participant 2 explained:

> We all [stakeholders] have different pieces of the puzzle from an issuing side, acquiring side, merchant side, PSP [payment service provider], but no one has that full overview… So, we will need to have a holistic or full overview of whatever the customer is doing. And if you

> talk to banks, you will hear that, yes, that is what we are aiming for. We want tools that will enable us to get everything [data] into one platform.

Research Participant 8 also noted a holistic approach to fraud prevention with various stakeholders. He specified:

> Because what always is an issue in our industry is that nobody sees the complete picture. Of course, it's not perfect, but at least they try to get that more holistic view on that and find ways to exchange data, which is, of course, is always challenging because everybody wants to share data. It's a good course. But it still, of course, has to comply with regulations and laws which sometimes prevent also fraudsters or protect fraudsters from being detected because you're basically saying that you can't get. And that's what we are working on there.

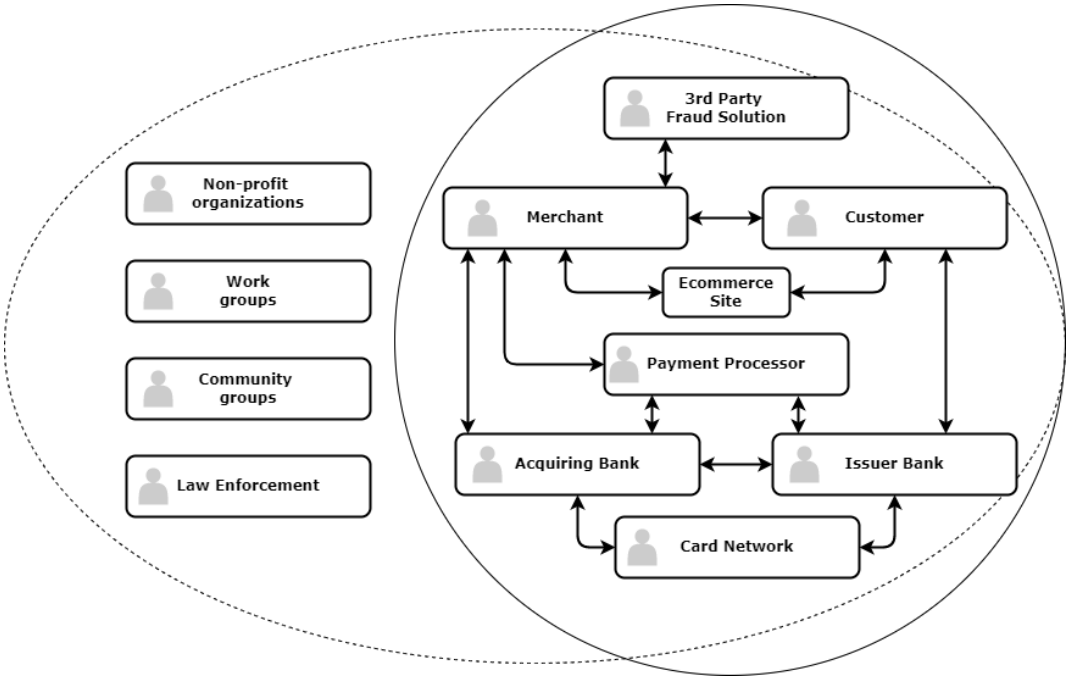

Figure 4. Potential stakeholder collaboration and information sharing

Fraud Incidents

The last finding was participants experienced complex fraud incidents. The research participants identified 13 types of fraud incidents that they consistently encounter in their role in fraud planning, prevention, detection, and response (Table 10).

Table 10. Qualitative coding types of fraud incidents

Initial coding	*Frequency*	*Category*	*Storyline*
Account takeover (ATO)	19	Fraud incidents	Ecommerce organizations face various everchanging, sophisticated, and complex fraudulent attacks.
Credit card fraud	6		
Credit card testing	8		
Gift card fraud	16		
Subscription fraud	9		
Money laundering	9		

Initial coding	*Frequency*	*Category*	*Storyline*
Money mule/triangulation fraud	7		
3D secure fraud	2		
Social engineering	5		
Credential stuffing	9		
Romance scams	1		
Policy abuse / 1st Party Misuse	30		
Identity theft	9		

Merchants and other ecommerce organizations are defending against complex and sophisticated fraud attacks. Specific types of ecommerce fraud incidents were discussed 130 times during the interviews. One attack could utilize multiple methods. These hybrid attacks contribute to the sophistication and complexity of cyber fraud incidents. Research Participant 1 suggested, "Fraudsters are unique in their efforts, right? They each have their own different MOs. Fraudsters want to be anonymous and will create standalone accounts within our networks with no common features." Research Participant 2 explained, "Fraudsters are no longer just attacking one silo or one channel [website]; they will attack the customer." Research Participant 3 suggested, "We've experienced a pretty significant diversity of the types and fraud and misuse that comes with that basically any way they can make money from us with all costs to them as possible.

ECOMMERCE FRAUD INCIDENT RESPONSE FRAMEWORK

The aim of this study is to explore the phenomena and develop a grounded theory framework to help define an ecommerce fraud incident response process, roles and responsibilities, systems, stakeholders, and incident types to help organizations respond to ecommerce fraud. The culmination of findings in this study resulted in an ecommerce fraud incident response framework that identifies significant areas from ecommerce fraud practitioners' perspectives.

Figure 5 illustrates the common incident response process, the common hybrid tools and systems, and roles and responsibilities for fraud prevention. Additionally, the figure showcases potential identification fraud incidents and information sharing conducted between the ecommerce fraud team, internal stakeholders, and external stakeholders. Information about the incidents is potentially shared between these three groups.

Ecommerce fraud incidents can be identified and detected by an ecommerce fraud team, internal stakeholders such as the cyber security team, or external stakeholders such as payment service providers or banks. Then the fraud can be shared between the relevant stakeholders for appropriate analysis and response. To facilitate appropriate ecommerce fraud response, a fraud team should have fraud prevention analysis, collaboration, leadership, management, reporting, and tool development skills and capabilities. Additionally, the ecommerce fraud team should have a mix of tools and systems to aid in the ecommerce fraud response process, such as rule-based detection, OSINT, and third-party software. Planning and improvement process activities can be completed before, during, and after a fraudulent incident. In the next section, this framework is broken down and discussed by each finding and then compared with the academic literature.

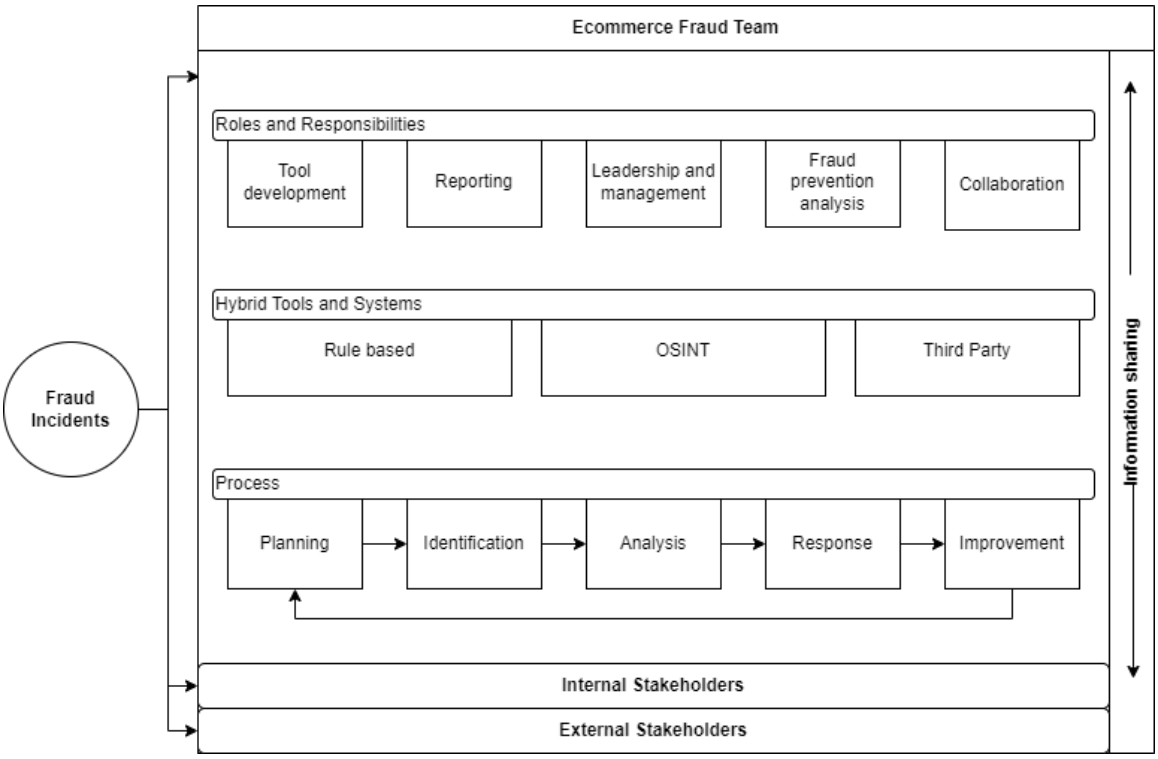

Figure 5. Ecommerce fraud incident response framework

DISCUSSION

The objective of this study was to explore the phenomena and develop a grounded theory framework to help define an ecommerce fraud incident response process, roles and responsibilities, systems, stakeholders, and incident types. First, this section conducted a comparison between the components ecommerce fraud incident response framework and the academic literature. Next, this section presents the academic and practical contributions of the study. Finally, limitations and implications for future research are reviewed and described.

PROCESSES, SYSTEMS, AND ROLES

The study aimed to help define processes, systems, roles, and responsibilities in ecommerce fraud incident response. This section compares the findings of the study with the academic literature. The findings were able to expand on the literature. The empirical incident response process differed in the containment phase between the processes. Academic literature only identified rule-based systems, whereas the findings of this study identified a multitude of tools, including rule-based systems. Roles and responsibilities were undefined in the literature, but key roles and responsibilities were identified in the findings of this study.

Processes

The first key finding was fraud practitioners described using planning, identification, analysis, response, and improvement phases of the cyber incident response. There were several similarities and differences between the academic literature and the perspectives of ecommerce industry fraud experts. The literature review identified an incident response model that included preparation, discovery, containment, analysis, response, and improvement phases (Adamov & Carlsson, 2016; Al-Dhaqm et al., 2020; Jalal et al., 2018; Lamis, 2010; Pilitsky et al., 2021; Pinto & Talley, 2006; Rollason-Reese, 2003; Ruefle et al., 2014; Sadik et al., 2020,). The five cyber incident phases of the empirical model

were similar to the literature model's preparation, discovery, analysis, response, and improvement phases. This finding diverged from the literature as many incident response models utilized a containment phase.

The second finding was research participants did not experience the containment phase of the cyber incident response model. Based on the research participants' experiences, this divergence may be due to online ordering practices rather than cyber security practices. Based on the research participants' perspectives, online orders appear difficult to "contain" as many business transactions are frictionless and continuously move through the ecommerce process. The transactions appear to be investigated as they are being processed. Figuratively speaking, ecommerce fraud is being identified, analyzed, and mitigated on a non-stop electronic conveyor belt.

Systems and tools

The next finding described research participants utilizing hybrid tools and systems for ecommerce fraud prevention, detection, and response. Overall, the research participants expressed using tools including rule-based, third-party, and OSINT fraud analytical tools. Fraud practitioners developed their own tools as well as used third-party developed tools. The majority of research participants noted their organizations utilized a combination of methods and tools for fraud prevention and detection. The use of hybrid tools and tool development could possibly be due to budgetary or utility reasons. Small-to-medium businesses may find commercial rule-based software expensive and may have to rely on open-source tools for specific fraud detection and investigation functionality. Additionally, rule-based detection software may not comprehensively address all areas of ecommerce fraud. However, more research would be needed to explore this facet.

In comparison, the academic research focused only on rule-based detection methods that may use machine learning and artificial intelligence (Diadiushkin et al., 2019; Kawase et al., 2019; Yasaka, 2020). Rule-based automation tools can be used for the detection and discovery of incidents. The rules look for specified patterns and can trigger different actions, such as sending notifications to the incident response team or preventing an attack (Pilitsky et al., 2021). Both the academic and empirical findings show the use of rule-based detection systems. However, the empirical findings differ and suggest that ecommerce fraud prevention goes beyond rule-based fraud detection. Ecommerce fraud prevention, detection, and response need a multitude of tools to uncover sophisticated fraud incidents, attacks, and schemes.

Roles and responsibilities

Another key finding of this empirical research defined five common roles and responsibilities. The research participants described tool development, reporting, leadership, and fraud prevention as the main roles and responsibilities. Tool development is the creation of internal and external fraud prevention tools. Reporting is the metrics and key performance indicators related to fraud prevention. Leadership and management focused on managing and developing people. Lastly, fraud prevention analytical capabilities included responding to fraudulent activity.

The literature differed from the empirical findings. The literature review did not specify roles and responsibilities but noted the challenges. Fraud prevention roles and responsibilities in organizations are murky, and it is unclear who should assume the role (Krambia-Kapardis & Zopiatis, 2010). Private and public organizations struggle to define and allocate team members' roles, responsibilities, and expertise, including outside groups and organizations involved in incident response (Simola, 2019; Van der Kleij et al., 2017). Organizations can use this finding to serve as a baseline for initial roles and responsibilities for hiring and developing personnel.

Organizational Alignment, Collaboration, & Stakeholders

This qualitative analysis aimed to identify stakeholders, information sharing, and collaboration practices. The major themes of the analysis and discussion are centered around organizational alignment, information sharing, and stakeholders. These areas present some challenges to ecommerce fraud response activities. Organizational alignments varied from each participant's perspective. Collaboration and information sharing may be challenging due to the level of maturity in interaction and trust between stakeholders. Lastly, many stakeholders may be involved in the detection and response efforts which adds to the complexity of the response.

Stakeholders

The fifth finding was research participants experienced information sharing and identified internal and external stakeholders. The next key finding was the research participants identified key stakeholders. The research participants identified nine internal stakeholders and eleven external stakeholders. The participants discussed various levels of interaction and the types of data and information that are shared or wanted to be shared. The research participants noted more stakeholders than in the academic literature. The academic literature identified only seven types of external stakeholders. In comparison, the research participants noted eleven types of external stakeholders. The academic literature appeared to only discuss external stakeholders rather than internal stakeholders where fraud was concerned. The cyber incident response literature specified vaguely about working with other organizational units.

Collaboration, information sharing, and holistic view

Collaboration and information-sharing capabilities are beneficial for internal and external stakeholders. Research Participant 1 noted a practical perspective for engaging in the fraud community. The participant suggested, "I think it is good for fraud teams to be able to share their experiences with that [fraud] community. I think that would help the fraud community as a whole". Research Participant 1 explained obtaining information for fraud prevention from the fraud community, "Even if we see things externally, like things in the news that happen or someone communicates on LinkedIn from the fraud community." The interaction between stakeholders and participants seemed to vary. One participant noted having good interaction with law enforcement, and the other participants had a negative sentiment toward law enforcement. Some were closely aligned with cyber security, and others with business units. More research is needed to explore the maturity levels of interaction that occur between internal and external stakeholders.

Another key finding was stakeholders do not have a holistic view of the data and information to make some connections about fraudulent behavior. The literature did not focus specifically on the holistic view of data and information. However, academia did specify there many unfamiliar and undefined areas in ecommerce and cyber incident response.

Organizational alignment

The sixth finding is that research participants experienced different organizational alignments. A major finding that occurred in the empirical study was organizational alignment. Three of the research participants noted their respective departments being reorganized several times. The participants noted their fraud team was reorganized several times under different departments until they were positioned in appropriate areas of collaboration and decision-making. However, it appeared that the organizational structures varied between participants. One participant specified the team moved from operations to IT to payments departments. Another participant specified their team moved from customer service to financial crimes. There does not appear to be a common organizational alignment. This could be due to the hybrid nature of the position that requires expertise in cyber security and financial payment systems. Additionally, since ecommerce fraud is a relatively new field, there may be

some maturity challenges. Further research can be conducted to explore this aspect. These gaps make it even more difficult to determine the complexity and sophistication of fraud.

Fraud Sophistication

The finding of the qualitative study highlighted the sophistication and complexity of fraud incidents. The research participants experienced 13 types of fraudulent incidents. The fraud incidents are account takeover, credit card fraud, credit card testing, gift card fraud, subscription fraud, money laundering, triangulation fraud, 3DS fraud, social engineering, credential stuffing, romance scams, policy abuse (1st party misuse), identity theft, and chargebacks. Many research participants noted one fraudulent incident could utilize multiple attack methods. These multi-faceted cyber attacks suggest fraudsters are using sophisticated and complex methods against organizations.

The literature review identified four types of ecommerce fraud incidents that hinder organizations. These were identity theft, mandate fraud, credit card fraud, and digital wallet fraud. Online payments and ecommerce have significantly increased in use and adoption globally (Ali et al., 2018; Marchal & Szyller, 2019; Singh & Jain, 2019; Wickramanayake et al., 2020). With the surge in global ecommerce, online transactions have become increasingly fraudulent, complex, and borderless (Kolodiziev et al., 2020; Minastireanu & Mesnita, 2019). Both the literature and empirical findings noted fraud sophistication. However, the fraud participants' experiences with fraudulent incidents were more nuanced than the incidents identified in the literature review. This study did not evaluate the types of fraud, but further research using methods like attack graph generation, crime script analysis, and attack trees can be used to help develop response playbooks, plans, and metrics.

Ecommerce Fraud Incident Response Framework

The aim of this research was to explore ecommerce fraud stakeholders' experiences with fraud and cyber incident response to help define areas such as the ecommerce fraud incident response process, roles and responsibilities, systems, stakeholders, and types of incidents. It is recommended to adopt the ecommerce fraud response framework to help ecommerce fraud and security professionals develop an awareness of cyber fraud activities and/or help mitigate cyber fraud activities.

This baseline framework serves as a starting point for ecommerce organizations that may struggle to respond to ecommerce fraud or are unaware of the number of stakeholders, types of incidents, tools, roles, and processes involved in fighting ecommerce fraud. Ecommerce organizations can customize the framework to their specific situation. Much of the academic literature on cyber incident response did not focus on aspects of ecommerce fraud. Additionally, the academic literature on ecommerce fraud was limited and did not incorporate many facets identified in this qualitative study. Table 11 provides a summary comparison of the main areas of the framework and the academic literature.

Table 11. Framework comparison

	Academic Literature	*Fraud Practitioners Experiences*
Process	Preparation, detection, containment, analysis, response, and improvement	Planning, identification, analysis, response, improvement
Systems	Rule-based	Rule-based, OSINT, third-party
Roles & responsibilities	Undefined	Tool development, fraud prevention analysis, reporting, leadership, management, and collaboration.

	Academic Literature	*Fraud Practitioners Experiences*
Stakeholders	Merchant, customer, issuing bank, acquiring bank, card network, payment processor, and law enforcement.	Merchants, customers, issuing banks, acquiring banks, card networks, payment processors, law enforcement, 3rd party fraud solution provider, work groups, community groups, and non-profit organizations. Customer service, information security, legal, shipping, warehouse, data, IT, payments, accounting, and product.
Ecommerce fraud incidents	Identity theft, mandate fraud, credit card fraud, and digital wallet fraud	Account takeover, credit card fraud, credit card testing, gift card fraud, subscription fraud, money laundering, triangulation fraud, 3DS fraud, social engineering, credential stuffing, romance scams, policy abuse (1st party misuse), identity theft, and chargebacks

Academic and Practical Contributions

This research study provided contributions to both the academic realm and practical industry. Based on the Constructivist Grounded Theory quality criteria, this qualitative study provides practical and theoretical contributions to the academic field and professional industry. The quality criteria are credibility, originality, resonance, and usefulness (Charmaz & Thornberg, 2020).

Credibility

Credibility refers to having sufficient relevant data for asking intelligent questions about the data, making systematic comparisons throughout the research process, and developing a thorough analysis (Charmaz & Thornberg, 2020). This qualitative analysis was credible because an initial literature review was conducted deductively to generate some initial themes. Next, an experienced ecommerce professional conducted a Grounded Theory analysis to develop an ecommerce incident response model iteratively. The comparison of the models contributed to a thorough analysis of the study.

Originality

Originality refers to whether the theory offers new insights into a problem and establishes the significance of the analysis (Charmaz & Thornberg, 2020). The primary contribution was the development of an original Grounded Theory of ecommerce fraud incident response model called the ecommerce fraud incident response framework. This original framework was developed to address the gaps presented in the academic literature, which did not define many areas of ecommerce fraud. Additionally, this research showcases the difficulty and sophistication of mitigating ecommerce fraud.

Resonance

Resonance is whether the theory and researcher have constructed concepts to represent the research participants' experiences and provide insights to others (Charmaz & Thornberg, 2020). This study constructed an ecommerce fraud incident response framework based on research participants' experiences. The ecommerce fraud incident response framework has the potential to provide insights to academia and practitioners in the field. The ecommerce fraud incident response framework provides a baseline model for practical use in organizations to help mitigate fraud in a systematic fashion. As commerce continues to grow and migrate online, more cyber incidents related to the ecommerce order/transaction lifecycle, such as fraud, are important to identify and define in order to respond to in an orderly manner.

Usefulness

Usefulness focuses on whether the research clarifies the research participants' experience, forms foundations for the policy or practical applications, contributes to a new line of research, and reveals pervasive processes and practices (Charmaz & Thornberg, 2020). The ecommerce fraud incident response framework provides useful applications to industry professionals who may struggle to mitigate fraud or are unaware of fraudulent attacks and incidents. Additionally, the research showcases many stakeholders involved in ecommerce fraud prevention. It is recommended that industry professionals adopt and adapt the framework to their specific environment. This study identified common areas that can be applied to help identify gaps in their own processes, systems, and people.

The results of this research study also potentially contribute to new lines of research. See the implications for the future study section. Even though this study and framework meet the quality criteria, there are still some limitations.

Limitations of the Study

Ecommerce fraud and cyber incident response are fascinating and complex research areas. As with any inquiry into complicated phenomena, there may be some limitations to this qualitative study. The extent to which the study's findings may be generalized and applied to other situations must be left to the reader's judgment.

The first limitation is that many stakeholders are involved in mitigating ecommerce fraud. There are many different stakeholders who may be involved in helping fight fraudulent activity. This study may not have identified and captured all central, significant concepts and themes associated with the area of inquiry due to the time and resource constraints of the study. The research participant interviews and analysis were conducted over 15 weeks in 2022.

Another limitation is that the use of online teleconference platforms for interviews may reduce the quality of the interviews. Online interviews are great for convenience and social distancing for COVID-19. However, online interviews through Internet teleconferencing are susceptible to technical difficulties, non-verbal cues identification issues, security issues, and privacy issues (Thunberg & Arnell, 2021). Thunberg and Arnell (2021) note that online interviews may not be appropriate for some research participants due to the security of the teleconference platform such as Zoom.

The last limitation is the participation of experts willing to share knowledge about sensitive business processes and information. Internal operations regarding fraud and cyber security are sensitive business areas. Some of the research participants noted that even they had difficulty sharing information about fraud with other organizations. Information leakage is a significant concern and can cause repercussions to the organization.

Implications for Future Study

This study provided credible, original, resonant, and useful insights for future research studies. The study constructed a foundational ecommerce fraud incident response framework that provides many avenues to explore. Future research could entail conducting a quantitative analysis by surveying the industry on the different components such as processes, systems, and responsibilities of the ecommerce fraud incident response framework. Other areas of research to explore and evaluate are the maturity models and organizational alignment, collaboration, information sharing, and stakeholders. Lastly, further research can be pursued on the nuances of ecommerce fraud incidents using frameworks such as attack graph generation, crime scripts, and attack trees to develop ecommerce fraud response playbooks, plans, and metrics.

CONCLUSION

With a surge in global ecommerce, online transactions have become increasingly fraudulent, complex, and borderless. The aim of this research study was to explore the experiences of industry fraud experts to define an ecommerce fraud incident response process, roles and responsibilities, systems, stakeholders, and types of incidents. This paper culminated and constructed a novel ecommerce fraud response framework based on the Constructivist Grounded Theory method to help organizations improve ecommerce fraud response and collaboration activities. The framework established an ecommerce fraud incident response process of planning, identification, analysis, response, and improvement. The framework constructed common systems of rule-based, OSINT, and third-party. The framework outlined common roles and responsibilities of tool development, reporting, management, leadership, collaboration, and fraud prevention analysis. The framework identified many types of fraudulent incidents, internal stakeholders, and external stakeholders.

This study provided practical and academic contributions through credibility, originality, resonance, and usefulness. The novel baseline framework can help mitigate attacks and minimize organizational loss, theft, and disruptions, by illustrating roles, responsibilities, processes, systems, incidents, and stakeholders. Future research can be conducted on areas in this ecommerce fraud incident response study and further explore the processes, systems, roles, responsibilities, organizational alignment, collaboration, stakeholders, and sophisticated fraud incidents.

ACKNOWLEDGMENT

The author would like to thank his family, the University of the Cumberlands, the Royal Melbourne Institute of Technology, the Merchant Risk Council, and the Informing Science Institute for their support.

REFERENCES

Adamov, A., & Carlsson, A. (2016, October). Cloud incident response model. *Proceedings of the 2016 IEEE East-West Design & Test Symposium*, *Yerevan, Armenia* (pp. 1–3, https://doi.org/10.1109/EWDTS.2016.7807665

Alammar, F., Intezari, A., Cardow, A., & J. Pauleen, D. (2019). Grounded theory in practice: Novice researchers' choice between Straussian and Glaserian. *Journal of Management Inquiry*, *28*(2), 228–245. https://doi.org/10.1177/1056492618770743

Albakri, A., Boiten, E., & De Lemos, R. (2018). Risks of sharing cyber incident information. *Proceedings of the 13th International Conference on Availability, Reliability, and Security* (pp. 1–10). Association for Computing Machinery. https://doi.org/10.1145/3230833.3233284

Al-Dhaqm, A., Razak, S. A., Siddique, K., Ikuesan, R. A., & Kebande, V. R. (2020). Towards the development of an integrated incident response model for database forensic investigation field. *IEEE Access*, *8*, 145018–145032. https://doi.org/10.1109/ACCESS.2020.3008696

Ali, M. A., Groß, T., & van Moorsel, A. (2018). Investigation of 3-D secure's model for fraud detection. *Proceedings of the 8th Workshop on Socio-Technical Aspects in Security and Trust* (pp. 1–11). Association for Computing Machinery. https://doi.org/10.1145/3361331.3361334

Amasiatu, C. V., & Shah, M. H. (2018). First party fraud management: Framework for the retail industry. *International Journal of Retail & Distribution Management*, *46*(4), 350–363. https://doi.org/10.1108/IJRDM-10-2016-0185

Artikis, A., Katzouris, N., Correia, I., Baber, C., Morar, N., Skarbovsky, I., Fournier, F., & Paliouras, G. (2017). A prototype for credit card fraud management: Industry paper. *Proceedings of the 11th ACM International Conference on Distributed and Event-Based Systems* (pp. 249–260). Association for Computing Machinery. https://doi.org/10.1145/3093742.3093912

Bednar, P. M., Katos, V., & Hennell, C. (2014). On the complexity of collaborative cyber crime investigations. *Digital Evidence and Electronic Signature Law Review*, *6*, 214. https://doi.org/10.14296/deeslr.v6i0.1894

Charmaz, K. (2006). *Constructing grounded theory: A practical guide through qualitative analysis*. Sage.

Charmaz, K., & Thornberg, R. (2020). The pursuit of quality in grounded theory. *Qualitative Research in Psychology*, *18*(3), 305–327. https://doi.org/10.1080/14780887.2020.1780357

Chen, A. N., Zeltmann, S. M., Griffin, K., Rubach, M., & Ellis, M. E. (2019). Trends and technology in e-payment. *Competition Forum*, *17*(2), 402–412. https://www.proquest.com/scholarly-journals/trends-technology-e-payment/docview/2343015805

Cross, C. (2018). Victims' motivations for reporting to the "fraud justice network." *Police Practice & Research*, *19*(6), 550–564. https://doi.org/10.1080/15614263.2018.1507891

Diadiushkin, A., Sandkuhl, K., & Maiatin, A. (2019). Fraud detection in payments transactions: Overview of existing approaches and usage for instant payments. *Complex Systems Informatics and Modeling Quarterly*, *20*, 72–88. https://doi.org/10.7250/csimq.2019-20.04

Doeland, M. (2017). Collaboration and the sharing of information help reduce payment transactions fraud. *Journal of Payments Strategy & Systems*., *11*(1), 81–85. https://hstalks.com/article/2822/collaboration-and-the-sharing-of-information-help-/?business

Donegan, M. (2019). Crime script for mandate fraud. *Journal of Money Laundering Control*, *22*(4), 770–781. https://doi.org/10.1108/JMLC-03-2019-0025

Dsouza, Z. (2018). Are cyber security incident response teams (CSIRTs) redundant or can they be relevant to international cyber security? *Federal Communications Law Journal*, *69*(3), 201–226. http://www.fclj.org/volumes/volume-69-2016-2017/issue-3/

Dwight, J. (2022). *Role of ecommerce fraud analytics in cyber incident response* [Doctoral dissertation, University of the Cumberlands].

Eappen, N. J. (2019). Mobile wallet adoption in India: Impact of trust and information sharing. *South Asian Journal of Management*, *26*(1), 32–49. https://www.proquest.com/scholarly-journals/mobile-wallet-adoption-india-impact-trust/docview/2251594419

Evers, J., Caprioli, M. U., Nöst, S., & Wiedemann, G. (2020). What is the REFI-QDA standard: Experimenting with the transfer of analyzed research projects between QDA software. *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research*, *21*(2). https://doi.org/10.17169/fqs-21.2.3439

Fadhilah, A. L., Ruldeviyani, Y., Prakoso, R., & Arisya, K. F. (2021). Measurement of information security awareness level: A case study of digital wallet users. *IOP Conference Series. Materials Science and Engineering*, *1077*, 12003. https://doi.org/10.1088/1757-899X/1077/1/012003

Glaser, B. G., & Strauss, A. L. (1967). *The discovery of grounded theory: Strategies for qualitative research*. Aldine Transaction. https://doi.org/10.1097/00006199-196807000-00014

He, M., Devine, L., & Zhuang, J. (2018). Perspectives on cybersecurity information sharing among multiple stakeholders using a decision-theoretic approach. *Risk Analysis*, *38*(2), 215–225. https://doi.org/10.1111/risa.12878

He, Y., Inglut, E., & Luo, C. (2022). Malware incident response (IR) informed by cyber threat intelligence (CTI). *Science China Information Sciences*, *65*, 179105. https://doi.org/10.1007/s11432-019-2774-4

Huang, K., Siegel, M., & Madnick, S. (2018). Systematically understanding the cyber attack business: A survey. *ACM Computing Surveys*, *51*(4), 1–36. https://doi.org/10.1145/3199674

Huang, T., & Huang, C. (2019). Fraud payment research: Payment through credit card. *Proceedings of the 10th International Conference on e-Business, Management and Economics* (pp. 189–194). Association for Computing Machinery. https://doi.org/10.1145/3345035.3345059

Hwang, Y.-W., Lee, I.-Y., Kim, H., Lee, H., & Kim, D. (2022). Current status and security trend of OSINT. *Wireless Communications and Mobile Computing*, *2022*. https://doi.org/10.1155/2022/1290129

Jalal, I., Yusof, M. M., Shukur, Z., & Mokhtar, M. R. (2018). A model for Afghanistan's cyber security incident response team. *International Journal on Advanced Science, Engineering and Information Technology*, *8*(6), 2620–2626. https://doi.org/10.18517/ijaseit.8.6.6692

Kawase, R., Diana, F., Czeladka, M., Schüler, M., & Faust, M. (2019). Internet fraud: The case of account take-over in online marketplace. *Proceedings of the 30th ACM Conference on Hypertext and Social Media* (pp. 181–190). Association for Computing Machinery. https://doi.org/10.1145/3342220.3343651

Kemp, S. (2020). Fraud reporting in Catalonia in the Internet era: Determinants and motives. *European Journal of Criminology*, *19*(5), 994–1015. https://doi.org/10.1177/1477370820941405

Kolodiziev, O., Mints, A., Sidelov, P., Pleskun, I., & Lozynska, O. (2020). Automatic machine learning algorithms for fraud detection in digital payment systems. *Eastern-European Journal of Enterprise Technologies*, *5*(9 (107)), 14–26. https://doi.org/10.15587/1729-4061.2020.212830

Krambia-Kapardis, M., & Zopiatis, A. (2010). Investigating incidents of fraud in small economies: The case for Cyprus. *Journal of Financial Crime*, *17*(2), 195–209. https://doi.org/10.1108/13590791011033890

Lamis, T. (2010). A forensic approach to incident response. *Proceedings of the 2010 Information Security Curriculum Development Conference* (pp. 177–185). Association for Computing Machinery. https://doi.org/10.1145/1940941.1940975

Levi, M., Doig, A., Gundur, R., Wall, D., & Williams, M. (2017). Cyberfraud and the implications for effective risk-based responses: Themes from UK research. *Crime, Law, and Social Change*, *67*(1), 77–96. https://doi.org/10.1007/s10611-016-9648-0

Levitin, A. J. (2018). Pandora's digital box: The promise and perils of digital wallets. *University of Pennsylvania Law Review*, *166*(2), 305–376. https://doi.org/10.2139/ssrn.2899104

Liu, H., Gegov, A., & Cocea, M. (2016). Rule-based systems: A granular computing perspective. *Granular Computing*, *1*, 259–274. https://doi.org/10.1007/s41066-016-0021-6

Marchal, S., & Szyller, S. (2019). Detecting organized ecommerce fraud using scalable categorical clustering. *Proceedings of the 35th Annual Computer Security Applications Conference* (pp. 215–228). Association for Computing Machinery. https://doi.org/10.1145/3359789.3359810

Midi, D., Sultana, S., & Bertino, E. (2016). A system for response and prevention of security incidents in wireless sensor networks. *ACM Transactions on Sensor Networks*, *13*(1), 1–38. https://doi.org/10.1145/2996195

Minastireanu, A., & Mesnita, G. (2019). An analysis of the most used machine learning algorithms for online fraud detection. *Informatica Economica*, *23*(1), 5–16. https://doi.org/10.12948/issn14531305/23.1.2019.01

Moreno, J., Serrano, M. A., Fernandez, E. B., & Fernández-Medina, E. (2020). Improving incident response in big data ecosystems by using blockchain technologies. *Applied Sciences*, *10*(2), 724. https://doi.org/10.3390/app10020724

Mugari, I. (2017). Cyberspace enhanced payment systems in the Zimbabwean retail sector: Opportunities and threats. *International Journal of Economics and Financial Issues*, *7*(3), 760–767. https://www.econjournals.com/index.php/ijefi/article/view/4988

Onwubiko, C., & Ouazzane, K. (2020). SOTER: A playbook for cybersecurity incident management. *IEEE Transactions on Engineering Management*, *69*(6), 3771–3791. https://doi.org/10.1109/TEM.2020.2979832

Park, J., Cho, D., Lee, J. K., & Lee, B. (2019). The economics of cybercrime: The role of broadband and socio-economic status. *ACM Transactions on Management Information Systems*, *10*(4), 1–23. https://doi.org/10.1145/3351159

Pilitsky, A. V., Prokopenko, O. E., & Halizev, V. N. (2021). General approach to automating the process of responding to computer security incidents. *IOP Conference Series. Materials Science and Engineering*, *1069*(1), 12023. https://doi.org/10.1088/1757-899X/1069/1/012023

Pinto, C. A., & Talley, W. K. (2006). The security incident cycle of ports. *Maritime Economics & Logistics*, *8*(3), 267–286. https://doi.org/10.1057/palgrave.mel.9100159

Rollason-Reese, R. (2003). Incident handling: An orderly response to unexpected events. *Proceedings of the 31st Annual ACM SIGUCCS Fall Conference* (pp. 97–102). Association for Computing Machinery. https://doi.org/10.1145/947469.947496

Ruefle, R., Dorofee, A., Mundie, D., Householder, A. D., Murray, M., & Perl, S. J. (2014). Computer security incident response team development and evolution. *IEEE Security & Privacy*, *12*(5), 16–26. https://doi.org/10.1109/MSP.2014.89

Sadik, S., Ahmed, M., Sikos, L., & Islam, A. (2020). Toward a sustainable cybersecurity ecosystem. *Computers*, *9*(3), 74. https://doi.org/10.3390/computers9030074

Simola, J. (2019). Comparative research of cybersecurity information sharing models. *Information & Security*, *43*(2), 175–195. https://doi.org/10.11610/isij.4315

Singh, A., & Jain, A. (2019). An empirical study of AML approach for credit card fraud detection – Financial transactions. *International Journal of Computers, Communications & Control*, *14*(6), 670–690. https://doi.org/10.15837/ijccc.2019.6.3498

Smith, R. (2008). Coordinating individual and organisational responses to fraud. *Crime, Law, and Social Change*, *49*(5), 379–396. https://doi.org/10.1007/s10611-008-9112-x

Statista. (2022). *E-commerce fraud* [Dossier]. https://www.statista.com/study/110998/e-commerce-fraud/

Stojanović, B., Božić, J., Hofer-Schmitz, K., Nahrgang, K., Weber, A., Badii, A., Sundaram, M., Jordan, E., & Runevic, J. (2021). Follow the trail: Machine learning for fraud detection in fintech applications. *Sensors*, *21*(5), 1594. https://doi.org/10.3390/s21051594

Sun, N., Zhang, J., Rimba, P., Gao, S., Zhang, L., & Xiang, Y. (2019). Data-driven cybersecurity incident prediction: A survey. *IEEE Communications Surveys and Tutorials*, *21*(2), 1744–1772. https://doi.org/10.1109/COMST.2018.2885561

Thunberg, S., & Arnell, L. (2021). Pioneering the use of technologies in qualitative research: A research review of the use of digital interviews. *International Journal of Social Research Methodology*, *25*(6), 757–768. https://doi.org/10.1080/13645579.2021.1935565

Tie, Y., Birks, M., & Francis, K. (2019). Grounded theory research: A design framework for novice researchers. *SAGE Open Medicine*, *7*. https://doi.org/10.1177/2050312118822927

Vakulenko, Y., Shams, P., Hellström, D., & Hjort, K. (2019). Service innovation in e-commerce last mile delivery: Mapping the e-customer journey. *Journal of Business Research, 101*, 461-468. https://doi.org/10.1016/j.jbusres.2019.01.016

Van der Kleij, R., Kleinhuis, G., & Young, H. (2017). Computer security incident response team effectiveness: A needs assessment. *Frontiers in Psychology*, *8*, 2179–2179. https://doi.org/10.3389/fpsyg.2017.02179

Wang, H., Wang, Z., Zhang, B., & Zhou, J. (2018). Information collection for fraud detection in P2P financial market. *MATEC Web of Conferences*, *189*, 6006. https://doi.org/10.1051/matecconf/201818906006

Wickramanayake, B., Geeganage, D. K., Ouyang, C., & Xu, Y. (2020). *A survey of online card payment fraud detection using data mining-based methods.* arXiv:2011.14024. https://doi.org/10.48550/arXiv.2011.14024

Wilks, S. (2019). Private interests, public law, and reconfigured inequality in modern payment card networks. *Dickinson Law Review*, *123*(2), 307–362. https://ideas.dickinsonlaw.psu.edu/dlr/vol123/iss2/2

Yasaka, N. (2020). Global knowledge management of suspicious transaction reporting system in Japan. *Journal of Money Laundering Control*, *23*(1), 55–63. https://doi.org/10.1108/JMLC-04-2019-0032

Yu, M., & Smith, S. M. (2021). Grounded theory: A guide for a new generation of researchers. *International Journal of Doctoral Studies*, *16*, 553–568. https://doi.org/10.28945/4836

Zibak, A., & Simpson, A. (2019). Cyber threat information sharing: Perceived benefits and barriers. *Proceedings of the 14th International Conference on Availability, Reliability, and Security* (pp. 1–9). Association for Computing Machinery. https://doi.org/10.1145/3339252.3340528

APPENDIX A. SAMPLE OF CODING

Coding	*Participant's statements*
Planning activities	RP1 - "We have our insights, and we spot the patterns, we see the developments, we keep our ears to the ground and our eyes on the data, and we can see what's happening and what's coming about oftentimes before it even happens. We know that there's a potential risk and vulnerability there. We want to patch that hole"
Identification activities	RP4 - "Sometimes someone will trigger fraud rules, but it's in their habit. They always do it. They trigger a bunch of alerts. So that was the first step. Make sure it's actually an outlier for that particular individual"
Analysis activities	RP3 - "We've got a range of different types of data that we're looking to…then we have manual search tools where we can pull specific data points from that order"
Response activities	RP3 - "We can cancel an order … if it's a good order, we're processing [the order]"
Improvement activities	RP1 - "When we do come up with our results and whatnot, then we're able to implement rules that will help the machine learning build to better protect, detect, and prevent these baddies [fraudsters],"
Roles and responsibilities	RP2 - "We could really see that this [fraud] is getting more and more sophisticated. We developed some tools, and they really worked well"
Systems	RP6 – "So we have search tools in the back end of our system that we search for email addresses, we search for different device traits pretty much everything that our system is doing on the front end with our filtering. We are then doing on the back end once we find fraud to make sure that our system didn't miss anything, which when you have a rules-based system, it is easy to miss, especially new fraud rings that we see"
Organizational structure	RP1 – "In the last three years, we have been bounced around like crazy. We started off in the operations department, you know, working with customer service, career success, restaurant success, you know, being part of general day-to-day operations. Then we got moved into the fintech pillar. Then we got moved into the general I.T. pillar."
Information sharing	RP2 – "I have been working with card schemes for 15 years, something like that. And I think we have very good collaboration"

APPENDIX B. INTERVIEW QUESTIONS

Interview questions

- What is your current role and responsibility in your organization?
- Why do you think this role is responsible for mitigating ecommerce fraud?
- What is your experience combating ecommerce fraud?
- Can you describe some of the fraud attacks you have experienced?
- Can you describe your experience with the investigation process?
- What are your experiences with tools or processes to prevent or mitigate fraud?
- How well do you think your organization handles ecommerce fraud?
- How do you think ecommerce fraud prevention can be improved in your organization?
- Can you describe your experience collaborating with individuals in your organization when trying to mitigate fraud? How about outside of your organization?
- How do you share information within your organization?
- How do you share information outside of your organization?
- Is there anything else you would like to add?

AUTHOR

Joshua Dwight is a Lecturer in the School of Science, Engineering, and Technology at the Royal Melbourne Institute of Technology (RMIT) in Vietnam. He obtained his Ph.D. in Information Technology from the University of the Cumberlands, Kentucky, USA. Additionally, attained an MBA from Louisiana State University and an MSc in Information Systems Management from Seattle Pacific University. He previously worked at the City University of Seattle as an associate faculty member. Prior to academia, he worked for over a decade in the ecommerce, banking, aerospace, and government industries in various business and technology roles.