Legal Gaps and Challenges in Prosecuting Cyber Fraud in Thailand's Online Banking System

Thailand's rapid digitization of financial services has created both opportunities for inclusive access to banking and growing vulnerabilities to cyber-enabled financial crime. This conceptual research study examines the direction of justice in cyber fraud cases within Thailand's online banking environment through the lenses of procedural justice theory and institutional theory. Drawing on empirical reports, legal and regulatory documents, and academic literature, the study identifies gaps in victims' experiences, institutional responses of banks, and law enforcement practices and sets research objectives. It proposes a qualitative triangulated study in three phases (victims, bank managers, and police officers) to probe how legal processes, institutional incentives, and perceptions of fairness shape case outcomes and victims' trust. The analysis discusses the implications for theory and practice, proposes actionable interventions, and outlines limitations and directions for future research. Throughout, the study situates the Thai case in global debates about the governance of online financial crime and the legitimacy of justice institutions in the digital age.

Keyword: *cyber fraud, online evidence, admissibility, online banking, access to Justice*

Introduction

Online banking and mobile financial services have become central to everyday economic life in Thailand. The convenience of digital payment channels and fast interbank transfers has substantially expanded access to financial services, but they have also created new attack surfaces for fraudsters and organized scam networks (Taeratanachai and Wiriyakitjar 2025). Recent governmental and civil society reports indicate that online and digital scams are a significant and growing problem in Thailand, with thousands of incidents reported and aggregate losses running into the billions of baht annually (Nation 2023). National-level responses, including draft guidelines by the Bank of Thailand (BOT), enforcement actions to freeze accounts suspected of use as mule accounts, and public campaigns, indicate recognition of the problem, but systemic difficulties in prevention, detection, victim redress, and cross-institutional coordination remain salient (Jenweeranon 2020). Empirical assessments show that scam operators often move stolen funds within minutes, while victims frequently do not realize losses for many hours, which complicates recovery and law enforcement action. These dynamics expose both technical and institutional weaknesses in Thailand's systemic response to financial cybercrime and raise important questions about the direction of justice, including how victims navigate formal legal pathways, how banks can balance regulatory compliance, customer protection, and operational constraints, and how police interpret and implement legal rules in the digital environment (Stefan 2025).

Recent policy interventions by the Bank of Thailand and related authorities signify a shifting landscape, but scholarly understanding of the interplay among victims' experiences, bank institutional behaviour, and law enforcement practices in Thailand's online banking environment remains limited and fragmented (Thongmeensuk 2025). Existing documentation and reporting provide robust descriptive accounts of the scale and patterns of online fraud in Thailand, as well as policy responses such as draft online fraud management guidelines and account-freezing operations. However, essential gaps remain in scholarly and policy-oriented research. First, much reporting is aggregative and statistical, offering limited insight into victims' lived experiences with reporting, bank remediation, and justice outcomes (such as restitution, criminal prosecution, or administrative relief). Second, although literature on procedural justice and institutional theory offers powerful frameworks for understanding perceptions of legitimacy and organizational behavior, these frameworks have not been systematically applied in the Thai online-fraud context to integrate micro-level perceptions (victims), meso-level institutional practices (banks), and macro-level legal structures (law enforcement and regulators). Third, there is limited qualitative research that triangulates perspectives across victims, banking professionals, and police officers within a single research design to illuminate procedural bottlenecks, institutional incentives, and normative expectations that shape justice trajectories in cyber fraud cases. Finally, the legal and administrative reforms that Thailand has introduced in recent years (including central bank guidelines and tactical enforcement measures against mule accounts) raise novel institutional dynamics and compliance pressures that require empirical investigation to evaluate their effect on procedural fairness and institutional isomorphism in the financial sector. Addressing these gaps is necessary to generate evidence-based reforms that strengthen both the effectiveness and legitimacy of justice processes for online-fraud victims (Tilleke & Gibbins 2025).

This study sets out to conceptualize how justice is directed in cyber fraud cases in Thailand's online banking environment by synthesizing the literature on procedural justice and institutional theory. Secondly, to identify institutional and legal features that shape victims' experiences and case outcomes. Third, to propose a robust qualitative, triangulated research design to probe victims, bank managers, and police officers empirically. Fourth, to derive theoretical and practical recommendations for improving justice direction, meaning the allocation, accessibility, and perceived fairness of remedial, investigative, and prosecutorial responses to online financial crime.

Literature Review

Online Banking and Cyber Frauds Worldwide

Recent global literature emphasizes that fraud in digital payments, online banking, and related financial technologies has been rising and that institutions are responding with technological, regulatory, and behavioural measures

(Laxman et al. 2024). A prominent recent work in the global domain explained by Vanini et al., (2023), this study analyzes transaction data spanning three years, proposing a combined framework of machine learning-based detection, economic optimization of machine learning decisions, and a risk model that considers countermeasures. The study shows that their machine learning model alone reduces expected and unexpected losses by about 15%, and when combined with optimization and risk modeling, up to 52%, while maintaining very low false positive rates (0.4%). This reflects how more sophisticated detection methods are necessary to manage fraudulent behavior in the digital banking (Vanini et al. 2023). Also relevant study is the explored by Aschi et al., (2022), which discusses the limitations of classical rule-based systems and describes how AI/machine learning based systems are increasingly used to detect risky transactions in real-time, with streaming architectures, data preprocessing, and continuously updated models. This work underscores that even small improvements in fraud detection rates can generate significant savings, given the scale of digital transactions (Chiarella and Borgese 2025). This review synthesizes three aspects: (a) empirical and policy research on cyber fraud and digital financial crime in Thailand; (b) procedural justice and legitimacy in policing and regulatory contexts; and (c) institutional theory as it applies to organizational responses in regulated environments, such as banks and police forces. Further, the objectives of this study are to map and analyze the procedural steps followed by Thai banks when customers report cyber fraud, including reporting, freezing, investigation, decision, and appeal processes. Additionally, the study aims to measure and compare outcomes for victims across a representative sample of Thai banks by examining reimbursement rates, time to resolution, and the proportion of cases requiring police reports.

Cyber Fraud and Digital Banking in Thailand: Patterns, Impacts, and Institutional Responses

Thailand has experienced an acceleration of online financial crime in line with global trends of increased online financial transactions. Studies and financial reports document a wide spectrum of fraudulent modalities, including online purchase scams, investment frauds, fake job and call-center scams, and account takeovers that exploit both technological vulnerabilities and social-engineering tactics to trick victims into transferring funds (Ingkathawornwong 2020). Literature on Thailand's perspective indicates significant psychological and social effects on victims, including shame, financial loss, and reduced trust in formal institutions. At the systemic level, the speed with which scammers launder funds through mule accounts and quickly move money across accounts complicates recovery and prosecution (Chayanon, Phoraksa, and Thitalampoon 2025). The Bank of Thailand and related agencies have recognized the scale of the problem; in recent years, they have published guidelines and executed large-scale interventions to close suspect mule accounts and propose new online fraud management frameworks for financial institutions. These interventions have included technical measures, regulatory guidance, and operational collaboration

with law enforcement, but their effectiveness depends on timely detection, information-sharing, and the willingness of banks to freeze and reverse transactions under legal and reputational constraints (Bank of Thailand 2023). Academic and practitioner reports stress that prevention and victim recovery require coordination across banks, regulators, and police, but empirical evidence on how these actors actually coordinate and how victims experience those processes is limited (Lertsatitpirote and Kanyajit 2023).

Several documents highlight the urgency and scale of the problem, including investigative reporting and NGOs' daily reports of hundreds of online fraud incidents, bank supervisory reports note the prevalence of mule accounts and deliberate laundering conduits, and the BOT has circulated draft guidelines for digital fraud management aimed at harmonizing banks' prevention and response protocols. Nonetheless, statistics also reveal a troubling time-lag problem. Scam operators often complete fund transfers within minutes, while victims may take many hours to detect fraudulent transactions. The asymmetry between attacker speed and institutional response time underscores structural obstacles to recovery and prosecution (Titus and Gover 2001). The literature, therefore, frames cyber-fraud challenges not only as technical or criminological issues but as institutional coordination problems requiring legal clarity, operational capacity, and procedural fairness to maintain public trust (Zayas 2023).

Cyber-Fraud Complaint Handling Issues in Thailand

Thailand-specific studies confirm these general patterns while adding local institutional detail. Qualitative work involving Thai police investigators and victims found that common fraud types (sale scams, account takeovers via social messaging platforms, and romance and investment scams) are widespread, and that victims' inexperience, over-optimism, and acquisitiveness were repeatedly identified as drivers of victimization. Importantly, interviews with officers revealed they perceive resource and technical gaps when managing high volumes of online fraud complaints, a situation that contributes to victim dissatisfaction and discourages reporting (Lertsatitpirote and Kanyajit 2023).

From the policing side, international policing literature emphasizes two interrelated problems affecting complaint handling: (1) organizational capacity (skills, digital forensics, case backlog) and (2) procedural legitimacy (how victims experience police response). The study shows that when police lack cyber expertise or show procedural indifference, victim satisfaction falls and future reporting declines, creating feedback that weakens official statistics and hampers prevention efforts (Stephan, 2025). These findings explain why victims in Thailand, facing similarly strained cyber units, may opt for bank dispute channels or third-party recovery efforts rather than lodging police complaints (Curtis and Oxburgh 2023). Banks in Thailand have responded with a mix of detection/ monitoring technologies, customer-notification systems, and coordination protocols with law enforcement and central authorities, such as the anti-online scam operation center and central fraud registry initiatives. Industry and government

reports show banks improving automated transaction monitoring and customer outreach. However, academic analyses note tensions between rapid fraud containment, such as account freezes and transaction holds, and consumer rights, including mistaken freezes and delays in customer redress, which damage trust and prompt formal complaints to both regulators and, in some cases, the police. This operational friction the bank's dual role as gatekeeper and service provider shapes how and whether customers escalate incidents to police (Tilleke & Gibbins 2025).

Theoretical Background

This study integrates procedural justice theory and institutional theory as complementary lenses for understanding the direction of justice in cyber fraud cases. Procedural justice provides the micro-level account of how victims perceive fairness and legitimacy in the handling of their cases. Institutional theory provides meso- and macro-level explanations for why banks and police organizations adopt particular policies and procedures and how coercive, mimetic, and normative forces shape these.

Procedural Justice Theory: Fairness, Legitimacy, and Cooperation

Procedural justice theory argues that individuals' perceptions of the fairness of processes used by authorities, rather than instrumental assessments of outcomes or deterrence, substantially influence their acceptance of decisions, willingness to cooperate with authority, and compliance with rules. Classic contributions from Sunshine & Tyler, (2003) show that when citizens perceive authorities (police, courts, regulators) as procedurally fair through respectful treatment, neutrality, voice, and trustworthy motives, they are more likely to view the institutions as legitimate and to cooperate voluntarily with legal processes (e.g., reporting crimes, providing information, complying with requests) even if outcomes are unfavorable.

Procedural fairness matters in policing because legitimacy can substitute for costly enforcement and fosters trust and information-sharing, which are crucial in complex investigations. In the context of cyber fraud, procedural justice suggests that victims' willingness to report incidents, engage with bank investigation teams, and cooperate with police may be strongly conditioned by how fairly they are treated during complaint intake, the transparency and timeliness of investigation updates, and perceptions of whether institutions prioritize victim welfare. Conversely, experiences of bureaucratic indifference, blame, or opaque processes can erode trust and discourage cooperation, reducing the likelihood of successful investigation and restitution. Thus, understanding victims' perceptions of fairness and legitimacy is essential to explain case trajectories and designing reforms that incentivize cooperative behavior (Tyler, Goff, and MacCoun 2015). Applied to the Thai context, procedural injustice can exacerbate underreporting, impede cross-institutional coordination, and hinder

asset recovery, producing both social harms (loss of trust) and operational inefficiencies. Empirical work on procedural justice in policing and regulatory interactions emphasizes the causally significant role of perceived fairness. This emphasis transfers readily to digital-fraud contexts where cooperation is crucial to tracing funds across accounts and jurisdictions (Sroeurn and Kohsuwan 2025).

Institutional Theory: Coercive, Mimetic, and Normative Pressures

Institutional theory explains organizational behavior as a response not merely to efficiency considerations but to pressures for legitimacy and survival in an institutional field. Applied to banks and policing organizations, institutional theory explains why financial institutions might adopt similar compliance and fraud-risk management practices in response to central bank guidance, peer practices, or professional norms among risk managers. It also explains how law enforcement agencies may converge on investigative models due to resource constraints, the diffusion of training programs, or national policy directives. In the digital fraud domain, coercive pressure from regulators, mimetic pressure arising from peer banks' implementation of advanced transaction monitoring, and normative pressure from legal-professional communities can produce isomorphic responses that shape the availability and quality of victim remediation. However, institutional theory also warns that such isomorphic convergence does not guarantee substantive effectiveness. Organizations may adopt similar rituals to signal compliance or legitimacy without materially improving outcomes (Chiarella and Borgese,2025). In Thailand, institutional theory helps analyze how banks and police might align their practices with regulatory templates while facing resource, technical, and legal constraints that blunt effective action. It further illuminates potential conflicts such as banks' risk-avoidance incentives versus customer-protection duties and the legitimacy consequences of formal compliance that do not translate into victims' perceived fairness (DiMaggio and Powell 1983).

Procedural Justice Theory Applied to Cyber Fraud

Procedural justice theory foregrounds four core elements of fair process: voice (opportunity to be heard), neutrality (impartiality in decision-making), respect (dignified treatment), and trustworthy motives (perception that authorities act with benevolent intentions) (Sunshine and Tyler 2003). In cyber-fraud cases, victims' access to timely information (voice) during complaint intake and investigation, consistency in bank and police procedures (neutrality), respectful communication by bank officers and police investigators, and the perception that institutions prioritize victim welfare over institutional convenience shape whether victims report incidents, persist with investigations, and cooperate with evidence collection. Procedural justice affects both subjective outcomes (victims' trust, satisfaction) and objective outcomes (cooperation necessary for investigations). Applied to the Thai context, procedural injustice can exacerbate underreporting, impede cross-institutional

coordination, and hinder asset recovery, producing both social harms (loss of trust) and operational inefficiencies. Empirical work on procedural justice in policing and regulatory interactions emphasizes the causally significant role of perceived fairness. This emphasis transfers readily to digital-fraud contexts where cooperation is crucial to tracing funds across accounts and jurisdictions (Sroeurn and Kohsuwan 2025).

From these theories, the study derives several integrative practices to guide empirical inquiry. First, higher perceived procedural fairness in bank and police interactions predicts greater victim cooperation and higher rates of case escalation to formal investigation. Second, coercive regulatory pressure without adequate resources or clear operational protocols produces isomorphic but superficial compliance among banks, which may not translate to improved victim outcomes. Third, discrepancies between institutional narratives of compliance and victims' experiences would predict reduced trust in both banks and law enforcement and lower reporting rates, thereby creating a negative feedback loop that impedes effective justice.

Integrative Observations and Need for Triangulated Qualitative Research

The literature above converges on several analytical points. First, victims' perceptions of procedural fairness are central to whether they seek and persist with formal justice channels. Second, institutional responses are shaped by regulatory pressure, peer imitation, and professional norms, which may lead to formalized yet uneven practices. Third, the rapid pace of technological change in digital banking creates timing and evidentiary challenges that complicate both institutional responses and perceptions of fairness. A triangulated, phase-based qualitative approach is therefore necessary to illuminate the micro–meso–macro dynamics that determine the direction of justice in cyber fraud cases. The following theoretical framing and proposed methodology respond directly to this need (Lertsatitpirote and Kanyajit 2023).

Methodology

This study proposes a qualitative, triangulated research design to generate in-depth, contextualized knowledge about how justice is administered in cyber fraud cases. A qualitative approach is suited to exploring perceptions, meanings, and institutional logics that quantitative methods may not capture. The research goal is exploratory and interpretive, seeking to understand how procedural fairness is experienced and enacted and how institutional pressures shape organizational responses. Semi-structured interviews allow open-ended exploration while maintaining comparability across respondents. Document analysis of bank policies, BOT guidelines, and police manuals complements interviews by providing background to stated practices and revealing formal institutional frames. The study aims to use thematic analysis to code interview transcripts and documents, iteratively developing categories that reflect procedural-justice dimensions (voice,

neutrality, respect, trustworthiness) and institutional-theory constructs (coercive, mimetic, and normative pressures). The design foregrounds purposive sampling, semi-structured interviews, document analysis, and thematic content analysis across three phases corresponding to the study's core populations, which are victims, bank managers/staff, and police officers. The research employs a multi-phase, qualitative case study design that triangulates data from three distinct but interconnected stakeholder groups.

Phase 1 involves in-depth interviews with victims of digital banking fraud to capture experiences of victimization, reporting decisions, interactions with banks and police, satisfaction with processes, and perceived barriers to justice. Phase 2 engages bank managers and frontline staff to elicit institutional policies, decision rationales, perceived legal constraints, and inter-organizational coordination practices. Phase 3 interviews police officers assigned to cybercrime and economic crime units to explore investigative practices, legal interpretations, evidentiary challenges, and perspectives on cooperation with banks and victims. Each phase includes purposive sampling to ensure diversity of experiences across urban and provincial sites, bank types (large commercial banks and regional banks), and law-enforcement units. The interview would be conducted face-to-face to avoid ambiguity, and it is expected to last 30 to 40 minutes with each interviewee. Firstly, to identify the actual victims, the screening questionnaire will be distributed to the interviewees. Secondly, before data collection, the bank's managers and police officers will be asked to provide the meeting time. Triangulation across stakeholder groups enables the study to identify convergent and divergent accounts, procedural bottlenecks, and institutional incentives shaping case trajectories.

Data Collection Methods

Semi-structured interviews will be conducted in Thai or the participant's preferred language by trained interviewers. Interview guides will be tailored to each population. Still, they will include core modules aligning with the theoretical framework, perceptions of fairness (voice, neutrality, respect, trust), procedural experiences (reporting, timelines, information flows), institutional responsibilities and constraints (legal duties, resource limitations), inter-organizational coordination, and suggestions for reform. Interviews will be audio-recorded (with consent), transcribed verbatim, and anonymized for analysis. Document analysis will include both guidelines and public statements from the Bank of Thailand, internal bank policy documents (where accessible), police procedural manuals, and relevant legal statutes governing money transfers, bank secrecy, and cybercrime procedures. Where possible, observation of complaint-intake processes at bank branches or call centers will be conducted to cross-validate self-reports.

Analytical Strategy

Transcripts and documents will be coded using NVivo software for qualitative analysis, following an iterative coding procedure. Initial codes will derive from theory (procedural-justice elements and institutional pressures), while inductive coding will allow emergent themes (e.g., time lags, technical evidentiary constraints, and fear of reputational harm). Cross-case matrices will be constructed to identify patterns across victims, banks, and police. Special attention will be paid to temporal sequences (when victims report relative to transaction timing), information asymmetries (what banks and police can access and share), and institutional narratives that justify certain practices. The analytic objective is to map the causal pathways by which institutional structures and perceived fairness produce particular justice trajectories ranging from successful recovery and prosecution to stalled investigations and victimization. Further, validity will be enhanced through triangulation, reliability through transparent coding schemes and inter-coder checks, and reflexivity through the documentation of researchers' positionality. Participants will be informed of the study purpose, use of data, and their right to withdraw.

Discussion Based on Documented Literature

The proposed triangulated qualitative study promises to yield a nuanced picture of how justice is directed in Thailand's cyber-fraud cases. Several likely themes emerge from integrating existing literature, policy documents, and the study's conceptual understanding advanced here.

Timing and Evidence Asymmetry: A Cross-Sector Challenge

One pervasive theme is the temporal asymmetry between attacker speed and institutional response. Scammers often move funds within minutes, victims commonly detect loss hours later, banks and police must then act in a compressed time window to freeze and trace funds. This timing challenge creates an asymmetry in evidence. Perpetrators exploit speed and use mule accounts or cross-jurisdictional transfers that fragment transaction trails. Victims and investigators face an uphill battle to produce timely, actionable information. Institutional reforms such as BOT guidelines on digital fraud management and system-level controls on rapid transfers seek to mitigate this but face implementation and legal hurdles (e.g., privacy and transaction confidentiality). The literature and policy reports underscore that without tighter technical and operational coordination and clearer legal channels for rapid data-sharing, many cases will remain unresolved (Zayas 2023).

Procedural Fairness as an Operational Asset, Not Only a Normative Ideal

Applying procedural justice theory reframes customer service and victim

outreach as instrumental to effective investigations. When victims are given a voice, transparent timelines, and respectful communication, they are more likely to provide corroborating information (multiple device logs, conversations, and screenshots) and to remain engaged throughout lengthy investigations. Conversely, bureaucratic indifference or blaming victims for carelessness can lead to underreporting, withdrawal, and loss of evidentiary leads. These dynamics suggest that improving procedural fairness is not merely normative but operationally productive. It increases cooperation, which in turn raises the probability of successful tracing and recovery. This insight supports investments in victim-facing processes (fraud hotlines, dedicated case managers) as part of the broader anti-fraud architecture. The procedural justice literature supports this causal channel between fairness, legitimacy, and cooperation (Tyler, Goff, and MacCoun 2015).

Institutional Isomorphism and the Risk of Ritual Compliance

Institutional theory warns that banks and law-enforcement agencies may adopt similar anti-fraud measures in response to regulatory pressure or peer imitation without necessarily solving root problems. For instance, banks may publicize state-of-the-art monitoring tools to signal compliance while failing to integrate processes across customer-facing units and law-enforcement liaison offices. Similarly, police units may adopt cybercrime rhetoric and create specialized units without sufficient training or interagency data-sharing protocols in place. Such ritual compliance can create the appearance of activity while victims continue to experience procedural unfairness and poor outcomes. This critique suggests that regulators and policy-makers should emphasize substantive performance metrics (timeliness of freeze actions, proportion of funds recovered, and victim satisfaction) rather than mere adoption of standard operating procedures (DiMaggio and Powell 1983).

Legal and Regulatory Complexity: Privacy, Liability, and the Need for Clear Protocols

Legal frameworks governing bank secrecy, personal data protection, and evidence rules can create friction between the need for rapid data sharing and obligations to protect privacy. Banks may be reluctant to release logs without explicit legal authorization. Police may be uncertain about the admissibility of certain digital traces, and victims may be deterred from cooperating due to stigma or fear of retribution. BOT draft guidelines and recent policy measures indicate awareness of these legal tensions, translating guidance into operational protocols requires explicit legal clarifications (e.g., emergency data disclosure mechanisms under judicial or administrative fiat) and safe harbors for banks that share data in good faith with authorized investigators. Without clear legal instruments that balance privacy and investigatory needs, interinstitutional cooperation will remain ad hoc and inconsistent (Tilleke & Gibbins 2025).

Organizational Incentives and Victim-Centered Metrics

Banks' incentives rooted in reputational risk, operational efficiency, and regulatory compliance can sometimes conflict with victim-centered practices that demand time-consuming case management. For example, immediate freezing of accounts can reduce short-term transaction volumes and lead to customer complaints in wrongful-freeze cases. Conversely, delaying freezes to obtain higher surety can reduce the chances of recovery. Designing incentives that align institutional self-interest with victim outcomes is therefore crucial. Possible mechanisms include regulator-mandated victim-recovery KPIs, supervised central registries to expedite tracing, and liability frameworks that protect banks acting in good faith to freeze funds. The institutional literature implies that coercive regulation (clear rules), normative professionalization (training and standards), and mimetic diffusion (sharing examples of effective models) can jointly encourage substantive improvements rather than token compliance (DiMaggio and Powell 1991).

Information Asymmetry and the Role of Trust

Trust emerges as a cross-cutting factor. Victims need to trust banks and police to report and cooperate; banks need to trust that sharing data with police will not create regulatory or reputational liabilities; police need to trust that banks' technical traces are reliable and timely. Building inter-institutional trust may require formal mechanisms memoranda of understanding, joint task forces, and legal frameworks that create predictable pathways for collaboration. Procedural fairness contributes to trust by making processes transparent and accountable; institutional reforms can anchor trust by specifying roles and liabilities. Together, these mechanisms can shorten response times, increase cooperation, and improve justice trajectories.

Implications and Contribution of the Study

This study proposes several theoretical contributions. By integrating procedural justice and institutional theory in the context of digital financial crime, the research extends procedural justice scholarship beyond traditional policing and court settings to financial institutions and hybrid regulatory environments. It demonstrates that perceptions of procedural fairness apply equally to corporate actors (banks) when they act as gatekeepers to legal redress. The study also expands institutional theory by showing how rapid technological change interacts with institutional isomorphism. Under uncertainty, mimetic pressures may favor the adoption of similar technical solutions (e.g., transaction-monitoring algorithms) even while organizational routines, customer service, police liaison, and legal disclosure remain heterogeneous. Finally, by emphasizing the temporal dimension (attacker speed vs. institutional response speed), the study adds a dynamic element to both theories, including procedural justice and institutional isomorphism, which must be understood in their

temporal contexts, where timing affects both legitimacy and the efficacy of isomorphic practices.

The research suggests several practical recommendations for policymakers, banks, and law enforcement. Establish legally authorized rapid-data pathways and emergency disclosure mechanisms that balance privacy with investigatory needs. Clear statutory instruments or emergency administrative orders can reduce banks' fear of liability when sharing transaction logs with authorized investigators. Further, institutionalize victim-centered complaint processes within banks, such as dedicated fraud case managers and standardized communication protocols that operationalize procedural-justice principles (voice, respect, neutrality, and transparent motives). Empirical evidence suggests that procedural fairness increases victim cooperation, which is operationally critical. More, develop inter-organizational performance metrics focused on substantive outcomes (time to freeze, proportion of funds recovered, victim satisfaction), and publish aggregated performance indicators to create accountability and drive improvement beyond superficial compliance. Another recommendation is to create joint task forces or liaison units with clear roles and standard operating procedures between banks and police to reduce time lags and evidentiary frictions. These units should include technical specialists who can translate bank logs into usable investigative leads. Further, to provide targeted training for police and bank staff on digital evidence, conversational interviewing of victims (trauma-informed methods), and legal frameworks to reduce procedural injustice arising from victim-blaming and misinformation. The other recommendation is to encourage the central bank to continue and refine its digital-fraud guidance through stakeholder consultation, emphasizing both technical measures and victim-protection obligations, and to consider a central fraud registry to expedite tracing and pattern detection measures, consistent with BOT draft initiatives already in circulation.

Implementing these recommendations requires coherent governance and political will. However, combining legal clarifications, procedural reforms, and institutional incentives increases the probability that victims will experience timely, fair, and effective justice.

Limitations and Future Research Directions

This conceptual study proposes a qualitative, triangulated empirical design but also acknowledges limitations that future research should address. First, the proposed qualitative design emphasizes depth over breadth, and findings would be richly contextual yet not statistically generalizable. Complementary quantitative studies, large-scale victim surveys, administrative data analyses of complaint outcomes, and cross-bank performance benchmarking would strengthen external validity and enable causal inference about the effectiveness of specific reforms. Second, access constraints may limit the availability of internal bank documents or in-depth police case studies due to confidentiality and reputational concerns. Building partnerships with banks and law-enforcement agencies, including data-sharing agreements that protect privacy

while enabling research access, will be necessary. Third, the rapidly evolving nature of technology and criminal tactics means that any empirical snapshot may quickly become dated. Longitudinal research that tracks changes over time, particularly following policy interventions such as BOT guidelines or legislative reform, would provide stronger evidence on reform efficacy. Fourth, cross-jurisdictional dynamics (offshore mule-account networks, international money movements) are increasingly central to digital fraud. Future research should incorporate comparative and transnational perspectives, including regional flows and cooperation with foreign law enforcement. Finally, while this study focuses on Thailand, comparative work across jurisdictions with different legal traditions and banking sectors would illuminate how institutional configurations shape the direction of justice in varied contexts, thereby refining theoretical generalizations.

References

Aschi, Massimiliano, Susanna Bonura, Nicola Masi, Domenico Messina, and Davide Profeta. 2022. "Cybersecurity and Fraud Detection in Financial Transactions." In *Big Data and Artificial Intelligence in Digital Finance: Increasing Personalization and Trust in Digital Finance Using Big Data and AI*, 269–78. Springer.

Bank of Thailand. 2023. "The Bank of Thailand Issues Additional Measures to Combat Financial Fraudulent Activities."

Chayanon, Sunthan, Trynh Phoraksa, and Siriporn Thitalampoon. 2025. "การ หลอกลวง ทาง ดิจิทัล: การ สำรวจ ช่อง โหว่ ทาง สังคม ต่อ การ ถูก หลอกลวง และ การ ฉ้อโกง ออนไลน์." *Dhammathas Academic Journal* 25 (1): 357–70.

Chiarella, Maria Luisa, and Manuela Borgese. 2025. "Platform-to-Business Contracts in Light of European Laws in the Digital Society." *Athens JL* 11: 129.

Curtis, Joanna, and Gavin Oxburgh. 2023. "Understanding Cybercrime in 'Real World'Policing and Law Enforcement." *The Police Journal* 96 (4): 573–92.

DiMaggio, Paul J, and Walter W Powell. 1983. "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields." *American Sociological Review*, 147–60.

———. 1991. "Introduction. The New Institutionalism in Organizational Analysis." *The New Institutionalism in Organizational Analysis, University of Chicago Press, Chicago, IL*, 1–38.

Ingkathawornwong, Pornchai. 2020. "Internet Banking Security: Human-Centered Issues in the Context of Thailand." *Humanities, Arts and Social Sciences Studies*, 163–218.

Jenweeranon, Pawee. 2020. "Thai Regulatory Approaches to Technology-Driven Innovation in Financial Services." *Regulating FinTech in Asia: Global Context, Local Perspectives*, 97–114.

Laxman, Vishnu, Nithyashree Ramesh, Senthil Kumar Jaya Prakash, and Ravi Aluvala. 2024. "Emerging Threats in Digital Payment and Financial Crime: A Bibliometric Review." *Journal of Digital Economy* 3: 205–22.

Lertsatitpirote, Krisada, and Sunee Kanyajit. 2023. "Causes and Types of Online Fraud Victimization in Thailand." *International Journal of Criminal Justice Sciences* 18 (2): 387–400.

Nation, The. 2023. "Eight Thai Banks Set up Hotline Centres for Reporting Online

Fraud Cases," 2023.
Sroeurn, Chhunheng, and Phanasan Kohsuwan. 2025. "The Effect of Service Fairness and Service Quality on Customer Satisfaction and Loyalty: A Case of Mobile Financial Applications in Phnom Penh." *Human Behavior, Development & Society* 26 (1).
Stefan, Elena Emilia. 2025. "Administrative Law Approach on Digitalisation." *Athens JL* 11: 415.
Sunshine, Jason, and Tom R Tyler. 2003. "The Role of Procedural Justice and Legitimacy in Shaping Public Support for Policing." *Law & Society Review* 37 (3): 513–47.
Taeratanachai, Chanin, and Rawida Wiriyakitjar. 2025. "Cybersecurity Analysis in Thailand: Trends, Challenges, and Policy Insights from Case Studies of SMEs, Mobile Banking, and Port Infrastructure." *National Defence Studies Institute Journal* 16 (1): 43–61.
Thongmeensuk, Saliltorn. 2025. "Online Fraud and Scams in Thailand."
Tilleke & Gibbins. 2025. "Bank of Thailand Releases Draft Guidelines for Digital Fraud Management."
Titus, Richard M, and Angela R Gover. 2001. "Personal Fraud: The Victims and the Scams." *Crime Prevention Studies* 12: 133–52.
Tyler, Tom R, Phillip Atiba Goff, and Robert J MacCoun. 2015. "The Impact of Psychological Science on Policing in the United States: Procedural Justice, Legitimacy, and Effective Law Enforcement." *Psychological Science in the Public Interest* 16 (3): 75–109.
Vanini, Paolo, Sebastiano Rossi, Ermin Zvizdic, and Thomas Domenig. 2023. "Online Payment Fraud: From Anomaly Detection to Risk Management." *Financial Innovation* 9 (1): 66.
Zayas, Edgar. 2023. "Thailand Shuts down 200K Mule Accounts in Two Months: A Good First Step but Much More Needed." *BioCatch*, 2023.