International Journal of Law and Society

E-ISSN: 3046-9562
Print ISSN: 3046-9619

Research/Review) Article

Criminal Policy in Combating Digital Banking Crime: Challenges and Prevention Strategies

Harlina Hamid[1]*, Muhammad Fadli Faisal Rasyid[2]

[1] Faculty of Law, University of Indonesia Timur, Indonesia
[2] Faculty of Law, Andi Sapada Institute of Social Sciences and Business, Indonesia
* Corresponding Author: linanasrullahmks@gmail.com [1]

Abstract: Digital transformation in the banking sector has introduced numerous conveniences in financial transactions, yet simultaneously opened opportunities for increasingly sophisticated and damaging new forms of crime. This article comprehensively analyzes criminal policy in combating digital banking crime in Indonesia, exploring the legal, technological, and institutional challenges faced, and formulating effective prevention strategies. Through systematic literature review and critical policy analysis, this research demonstrates that digital banking crime in Indonesia has experienced significant increases both in quantity and complexity of modus operandi, encompassing phishing, skimming, hacking, social engineering, banking trojan malware, and various technology-based fraud schemes. Financial losses amount to trillions of rupiah annually, excluding the psychological impact on victims and erosion of public trust in digital banking systems. Research findings identify fundamental challenges in combating digital banking crime, including limitations in legal frameworks that have not fully accommodated technological developments, gaps in law enforcement capacity for cyber investigation, complexity of evidence in digital cases, complicated cross-border jurisdiction, rapid evolution of crime modi outpacing regulatory adaptation, and low digital security literacy among banking service users. Policy analysis shows that penal approaches through criminalization and law enforcement, while important, are insufficient without comprehensive non-penal strategies.

Keywords: Consumer Protection; Crime Prevention; Criminal Law; Cyber Security; Fintech

1. Introduction

Background

The era of the Fourth Industrial Revolution has fundamentally transformed the banking and financial services landscape in Indonesia. Massive digital transformation over the past decade has introduced various banking service innovations providing convenience, speed, and efficiency in financial transactions. Mobile banking, internet banking, e-wallets, and various financial technology (fintech) applications have become integral parts of modern society. Data from the Financial Services Authority (OJK) shows that in 2023, digital banking transactions in Indonesia reached more than 28 billion transactions valued at Rp 39,000 trillion, demonstrating massive penetration into economic life.

However, digital technological advancement in the banking sector has been accompanied by the emergence of increasingly sophisticated and damaging new forms of crime. Digital banking crime has become a serious threat to financial system stability, customer asset security, and public trust in electronic banking services. Unlike conventional banking crimes that generally involve physical interaction, digital banking crimes are committed by exploiting information technology system vulnerabilities, social engineering, or digital security gaps.

Digital banking crime modus operandi are highly diverse and continuously evolving with technological development. Phishing through email, SMS, or instant messaging applications disguised as official bank communications to steal user credential information has become the most common modus. Skimming or card data theft through illegal devices installed on ATMs continues despite EMV chip technology implementation. Hacking or banking system breaching to access customer data or conduct illegal transfers demonstrates

Received: September 16, 2025
Revised: September 30, 2025
Accepted: October 14, 2025
Published: October 16, 2025
Curr. Ver.: October 16, 2025

perpetrator sophistication. Social engineering manipulating victim psychology to disclose confidential information or conduct certain transactions increasingly occurs. Banking trojan malware infecting user devices to steal credentials or divert transactions rapidly develops. Account takeover where perpetrators seize victim banking accounts after obtaining unauthorized access also significantly increases.

Data from the National Cyber and Crypto Agency (BSSN) shows cyber-attacks on the financial and banking sector have dramatically increased, with millions of attack attempts detected annually. Financial losses from digital banking crime reach trillions of rupiah per year, excluding system recovery costs, legal handling, and reputational impact on banking institutions. Moreover, psychological impacts on victims losing savings or experiencing financial identity misuse are often severe and prolonged.

Digital banking crime complexity poses serious challenges to Indonesia's criminal law system and law enforcement. Cybercrime characteristics of being borderless, anonymous, using high technology, leaving digital traces easily erased or manipulated, and involving perpetrators across jurisdictions make conventional handling inadequate. Existing criminal law frameworks, despite several updates, still face gaps in anticipating highly dynamic crime modus developments. Law enforcement capacity in digital forensic investigation, understanding technologies used by perpetrators, and cross-institutional coordination remain significant constraints.

Combating digital banking crime requires comprehensive and holistic criminal policy approaches. Criminal policy, as proposed by Barda Nawawi Arief, encompasses penal policies (through criminal law) and non-penal policies (outside criminal law) integrated to prevent and combat crime. In the digital banking crime context, penal approaches through criminalization and strict law enforcement are important for providing deterrent effects and upholding justice. However, given special cybercrime characteristics, non-penal approaches through strengthening technology security infrastructure, increasing public digital security literacy and awareness, developing early detection systems, and multi-stakeholder collaboration become equally fundamental.

Indonesia's context with a population exceeding 270 million, internet penetration reaching over 200 million users, and accelerated digital financial service adoption post-COVID-19 pandemic creates special challenges and urgency in combating digital banking crime. Still-varied digital literacy levels, technology infrastructure gaps between urban and rural areas, and immature digital security culture among users make Indonesian society vulnerable to various digital crime modi.

Problem Formulation

Based on this background, this research explores interconnected dimensions in combating digital banking crime. First, the research analyzes characteristics and patterns of digital banking crime in Indonesia, identifying developing modus operandi, perpetrator and victim profiles, and development trends requiring anticipation in policy formulation. Deep understanding of crime phenomenology becomes an important foundation for designing appropriate and effective prevention strategies.

Second, the research examines criminal law frameworks regulating digital banking crime in Indonesia, evaluating adequacy and effectiveness of existing legal instruments in anticipating and combating various digital crime forms, identifying gaps or legal vacuums requiring improvement, and analyzing harmonization among related regulations. Formal legal aspects become fundamental instruments in providing legitimacy basis for law enforcement and legal certainty for all stakeholders.

Third, the research identifies and analyzes fundamental challenges faced in law enforcement and digital banking crime prevention, encompassing technology, institutional, human resource, inter-agency coordination dimensions, evidentiary and legal procedure aspects, and jurisdictional complexity in transnational crime. Comprehensive understanding of implementation obstacles becomes key to designing realistic and operationalizable interventions.

Fourth, the research explores and formulates effective prevention and combating strategies for digital banking crime, integrating penal and non-penal approaches within holistic criminal policy frameworks. This includes strengthening legal and institutional infrastructure, enhancing technology and human resource capacity, developing multi-stakeholder

collaboration mechanisms, digital security education and literacy programs, and strengthening international cooperation in handling transnational crime.

Fifth, the research analyzes roles and responsibilities of various stakeholders in the digital banking crime prevention ecosystem, including banking institutions as service providers, financial sector regulators and supervisors, law enforcement, digital technology and infrastructure providers, civil society organizations, and banking service users themselves. Ecosystem-based approaches recognize that effective prevention requires active and coordinated involvement from all interested parties.

Research Objectives

This research pursues several interrelated objectives to provide comprehensive contributions to criminal policy development in combating digital banking crime. Primary objectives include developing deep understanding of digital banking crime phenomena in Indonesia across dimensions, critical evaluation of existing criminal policy frameworks, and formulating strategic recommendations for strengthening prevention systems.

Specifically, the research aims to identify and analyze various forms and modi of digital banking crime developing in Indonesia, understand factors facilitating crime occurrence, and anticipate future development trends based on technology evolution and user behavior. This phenomenological understanding becomes the basis for designing appropriate and anticipatory policy responses.

The research also aims to comprehensively evaluate criminal law frameworks regulating digital banking crime, analyzing adequacy of legal substance in criminalizing various conduct forms, law enforcement effectiveness in practice, and harmonization among relevant legal instruments. This critical evaluation will identify areas requiring regulatory updates or strengthening.

Another important objective is identifying and analyzing multidimensional challenges faced in combating digital banking crime, encompassing technology, institutional, resource, coordination, and jurisdictional aspects. Deep understanding of implementation barriers will inform realistic and operationalizable recommendations within available capacity and resource contexts.

The research aims to formulate comprehensive and integrated digital banking crime prevention strategies, combining penal and non-penal approaches within holistic criminal policy frameworks. Formulated strategies encompass prevention, detection, response, and recovery dimensions, considering roles and responsibilities of various stakeholders in the digital banking security ecosystem.

Finally, the research aims to provide theoretical contributions to criminal policy concept development in the digital era, particularly in high-technology crime contexts and special cybercrime characteristics. Practical contributions are intended to inform policy formulation by regulators, security strategies by banking institutions, and security awareness programs for digital banking service users.

2. Preliminaries or Related Work or Literature Review

Criminal Policy Concept

Criminal policy represents a central concept in rational and planned crime prevention efforts. According to Marc Ancel, criminal policy is both science and art aimed at enabling better formulation of positive legal regulations and providing guidance to legislators and courts while helping them perform their duties. Barda Nawawi Arief defines criminal policy as society's rational efforts to combat crime, encompassing penal policy (using criminal law) and non-penal policy (outside criminal law).

Penal policy focuses on criminal sanctions as primary instruments, encompassing criminalization processes (establishing acts as criminal offenses), sanction application (determining sanction types and measures), and law enforcement through criminal justice systems. Non-penal policy encompasses various approaches outside criminal law systems such as situational prevention, education, socio-economic change, and informal control strengthening. In modern contexts, integrative approaches combining penal and non-penal policies are considered most effective for combating complex crimes.

Digital Banking Crime: Definition and Typology

Digital banking crime constitutes part of cybercrime specifically targeting systems, infrastructure, or electronic banking service users. Wall classifies cybercrime into three categories: computer-assisted crime (traditional crimes facilitated by computers), computer-focused crime (crimes targeting computer systems), and computer-enabled crime (new crimes made possible by digital technology).

Digital banking crime typology encompasses various forms. Phishing involves fraud to obtain confidential information by impersonating trusted entities through email, SMS, or fake websites. Skimming is card data theft through illegal devices reading card information during use. Hacking encompasses unauthorized access to banking systems to steal data or funds. Social engineering manipulates victim psychology to disclose information or perform certain actions. Banking trojan malware is malicious software stealing credentials or diverting transactions. Account takeover occurs when perpetrators seize control of victim banking accounts. Denial of Service attacks disrupt banking service operations by flooding systems. Man-in-the-Middle attacks intercept communications between users and banks to steal information or manipulate transactions.

Special Characteristics of Cybercrime

Cybercrime, including digital banking crime, possesses characteristics distinguishing it from conventional crime. Transnational nature allows perpetrators and victims in different jurisdictions, complicating law enforcement. Anonymity through encryption technology, VPN, or darknet usage complicates perpetrator identification. Automation enables mass attacks with relatively low costs. Speed of execution provides very limited time for detection and response. Digital evidence easily manipulated or erased creates evidentiary challenges. Asymmetric advantage where perpetrators possess technical superiority over most victims and even law enforcers. Low risk-high reward with relatively low capture probability yet very large profit potential.

Criminal Law Framework for Cybercrime in Indonesia

Indonesia possesses various legal instruments regulating cybercrime and digital banking. Law Number 19 of 2016 concerning Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (ITE Law) is the main cybercrime regulation, governing illegal access, illegal interception, data and system interference, and device misuse. Law Number 1 of 2024 concerning Second Amendment to ITE Law updates several provisions to respond to technological developments and law enforcement needs.

The Criminal Code (KUHP) remains relevant for general offenses such as fraud, forgery, and theft committed through digital media. Law Number 8 of 2010 on Prevention and Eradication of Money Laundering is important in digital banking crime context as crime proceeds are often laundered through financial systems. Bank Indonesia and Financial Services Authority regulations govern operational and electronic banking security aspects, though administrative in nature.

Crime Prevention Theory

Digital banking crime prevention strategies can be understood through various criminology theories. Situational Crime Prevention focuses on reducing crime opportunities through environment or system modification. In digital contexts, this includes strengthening system security, layered authentication, encryption, and security-by-design principles. Routine Activity Theory explains crime occurs when motivated offender, suitable target, and absence of capable guardian meet. Prevention can be done by reducing target vulnerability (trained users) and increasing surveillance (monitoring systems).

Rational Choice Theory assumes perpetrators conduct cost-benefit calculations before committing crime. Prevention is done by increasing perception of capture risk and punishment while reducing profit perception. Deterrence Theory emphasizes importance of sufficiently severe, certain, and swift sanctions for creating deterrent effects. General Prevention Theory more broadly encompasses legal education, social norm strengthening, and collective consciousness formation about prohibitions and crime consequences.

Digital Security Literacy and User Behavior

Research shows human factors constitute the weakest point in digital system security. Most digital banking crimes succeed through user vulnerability exploitation rather than system technical weaknesses. Security awareness and digital literacy concepts become important in

prevention strategies. Security awareness encompasses understanding threats, good security practices, and ability to recognize fraud or attack attempts. Digital literacy more broadly encompasses ability to use technology effectively, critically, and safely.

Risky behaviors such as using weak passwords, sharing credentials, clicking suspicious links, or ignoring security updates increase vulnerability. Education programs and awareness campaigns prove effective in reducing victimization, though requiring approaches adapted to diverse demographic characteristics and literacy levels.

Public-Private Collaboration in Cybersecurity

Cybersecurity literature emphasizes importance of public-private partnerships given most digital infrastructure is owned and operated by private sector. Banking institutions have primary responsibility for securing systems and protecting customers, yet require regulatory support, law enforcement, and threat information sharing. Government through regulators and law enforcement provides legal frameworks, security standards, crime investigation, and coordination of major incident responses.

Effective collaboration models include information sharing about threats and incidents, joint capability building for capacity strengthening, coordinated incident response for handling major attacks, and policy dialogue for developing balanced regulations between security and innovation. Several countries have established National Cyber Security Centres facilitating public-private collaboration, and Indonesia has BSSN as national cybersecurity coordinator

3. Proposed Method

Research Design

This research employs qualitative research design with juridical-normative approaches enriched with empirical analysis. Juridical-normative approaches examine legal substance, legal principles, and norms regulating digital banking crime and prevention policies. Empirical analysis understands law enforcement practices, occurring crime patterns, and field policy implementation based on available secondary data.

This research is descriptive-analytical aiming to comprehensively describe digital banking crime phenomena, existing policy frameworks, challenges faced, and formulate effective prevention strategies. Prescriptive approaches formulate policy recommendations based on analytical findings.

Data Collection Methods

This research relies on secondary data collected through systematic literature review. Data sources include primary legal materials such as relevant legislation including ITE Law, Criminal Code, Banking Law, Consumer Protection Law, and Bank Indonesia and Financial Services Authority regulations regarding electronic banking security. Court decisions in digital banking crime cases are also examined to understand practical law application.

Secondary legal materials include criminal law and criminal policy textbooks, academic journals both national and international discussing cybercrime, digital banking security, and prevention strategies, research results and reports from research institutions, and policy documents from relevant agencies. Tertiary legal materials such as legal dictionaries, encyclopedias, and mass media articles are used as supplements to understand terms and current developments.

Cybercrime statistical data from BSSN, banking data from OJK and Bank Indonesia, and banking institution annual reports regarding security incidents are used to understand trends and problem magnitude. International organization publications from INTERPOL, FBI, European Cybercrime Centre, and global cybersecurity research institutions provide comparative insights and international best practices.

Data Analysis Methods

Collected data are analyzed using several methods according to data characteristics and research objectives. Juridical-normative analysis examines legislation compliance with legal principles, identifies harmonization or conflicts among regulations, evaluates legal substance adequacy in regulating digital banking crime, and analyzes legal instrument effectiveness in enforcement practice.

Content analysis applies to court decisions, case reports, and policy documents to identify patterns, themes, and insights about crime characteristics, legal responses, and

enforcement challenges. Comparative analysis compares Indonesian approaches with other countries' practices in combating digital banking crime, identifies adaptable best practices, and understands advantages and weaknesses of various policy models.

SWOT analysis identifies strengths and weaknesses of Indonesian legal and institutional systems in combating digital banking crime, and opportunities and threats from technological developments and external contexts. Integrative synthesis combines findings from various analytical methods to produce comprehensive understanding and formulate holistic policy recommendations.

Research Limitations

This research acknowledges several limitations. As literature-based research, no direct interviews were conducted with law enforcement practitioners, banking professionals, or crime victims who could provide deeper insights. Cybercrime statistical data are often underreported as many victims do not report, so actual magnitude may be larger than recorded. Rapid technology and crime modus evolution makes some information quickly outdated. Research focus on Indonesian contexts limits findings generalization to other countries with different conditions.

4. Results and Discussion

Digital Banking Crime Landscape in Indonesia

Trends and Statistics

Data from the National Cyber and Crypto Agency (BSSN) shows dramatic increases in cyber-attacks on the financial sector. 2023 recorded over 1.5 billion cyber-attack attempts on Indonesian digital infrastructure, with financial and banking sectors among primary targets. This increase parallels accelerated digital banking service adoption, particularly post-COVID-19 pandemic forcing massive shifts from conventional to digital services.

OJK reports show financial losses from digital banking fraud reaching trillions of rupiah annually, though exact figures are difficult to obtain due to underreporting and banking institution reluctance to disclose incidents for reputational reasons. Based on complaints to OJK and BSSN, thousands of digital banking crime cases are reported annually with consistent increasing trends.

Dominant Modus Operandi

Phishing through various channels remains the most common modus. Perpetrators send emails, SMS, or WhatsApp messages claiming to be from banks, requesting victims click links or provide personal information under various pretexts such as account verification, lottery prizes, or account blocking threats. Fake websites mimicking official bank appearances are used to capture login credentials entered by victims.

Social engineering develops increasingly sophisticated with perpetrators conducting target research, leveraging social media information to make approaches more convincing. Vishing (voice phishing) techniques through telephone with perpetrators pretending to be bank officers or law enforcement officials occur frequently, often manipulating victims in panic or urgent conditions to immediately transfer or disclose information.

Malware particularly banking trojans infecting victim smartphones or computers becomes serious threat. This malware can steal credentials, read SMS OTP (One-Time Password), even conduct overlay attacks where fake displays are shown over real banking applications to capture login information. Distribution occurs through fake applications disguised as popular applications, download links from unofficial sources, or malicious email attachments.

SIM swap fraud where perpetrators take over victim phone numbers by replacing SIM cards becomes serious new threat. By controlling phone numbers, perpetrators can access accounts using SMS as authentication or recovery methods, including banking accounts and e-wallets. This modus exploits weaknesses in telecommunication operator procedures for verifying SIM card replacement requests.

Perpetrator and Victim Profiles

Digital banking crime perpetrators are highly diverse. Criminal organizations organized with clear structures, role specialization, and cross-country operations become large-scale crime perpetrators. They possess resources, technical expertise, and networks enabling sophisticated attacks on banking systems. Individual hackers with financial motivations

conduct opportunistic attacks exploiting discovered security gaps. Insider threats from bank employees or IT service providers misusing access to steal data or facilitate crime also become serious concerns.

Victims encompass very broad spectrums. Individual mobile banking and internet banking service users, particularly populations with low digital literacy such as elderly or new users, become easy social engineering targets. However, even technology-literate users can become victims of sophisticated attacks. Small and Medium Enterprises (SMEs) using corporate banking services are also vulnerable, often due to inadequate security protections. Even large institutions sometimes become victims of advanced persistent threat (APT) attacks.

Criminal Law Framework Analysis

Criminalization in ITE Law

The Electronic Information and Transactions Law (ITE Law) as amended by Law Number 19 of 2016 and Law Number 1 of 2024 is the main legal instrument for cybercrime in Indonesia. Article 30 criminalizes illegal access to others' computers or electronic systems, including unauthorized access to banking systems. Article 31 regulates illegal interception of electronic transmission, relevant for banking communication interception cases. Article 32 criminalizes electronic system interference, including attacks disrupting banking service operations. Article 33 regulates data interference, encompassing manipulation, destruction, or deletion of banking data.

Article 35 criminalizes creation, sale, or distribution of devices for committing computer crimes, relevant for malware distribution or hacking tool cases. Threatened criminal sanctions are quite severe, with maximum imprisonment up to 10-12 years and fines up to billions of rupiah, showing legislator seriousness in combating cybercrime.

Conventional Offenses in Criminal Code

Although ITE Law regulates special cybercrime aspects, Criminal Code offenses remain relevant and often used in prosecution. Article 362 on theft can apply to cases of taking funds from others' accounts without permission, though done electronically. Article 378 on fraud is highly relevant for various digital banking crime modi involving lies or manipulation to obtain financial benefits.

Article 263 on forgery can apply to fake electronic document creation or digital identity forgery cases. Article 406 on property destruction can apply to data or system destruction cases. Criminal Code usage provides prosecution flexibility, especially when conduct is not explicitly regulated in ITE Law or when layered offenses (concursus) need application.

Financial Sector Regulations

Bank Indonesia Regulations (PBI) and Financial Services Authority Regulations (POJK) govern technical and operational aspects of electronic banking security. PBI on Financial Technology Implementation regulates system security requirements, information technology risk management, and security incident reporting obligations. POJK on Information Technology in Financial Services Sector establishes minimum security standards that financial institutions must meet.

Though these regulations are important for prevention, sanctions regulated are generally administrative such as warnings, administrative fines, or license revocation, not criminal sanctions. However, violations of security obligations resulting in consumer losses can create civil liability or even criminal liability if gross negligence or intentional elements exist.

Regulatory Gaps and Challenges

Despite framework development, gaps remain. Definitions of some conducts in ITE Law can still generate different interpretations, creating legal uncertainty. Regulatory updates often lag behind technology development speed and new crime modi, creating grey areas in law application.

Criminalization of some preparatory conduct (crime preparation) specific to cybercrime such as creation, distribution, or possession of hacking tools remains limited, yet early prevention requires capability to address preparation stages before crime occurs. Regulations on cryptocurrency and digital assets increasingly used in money laundering from digital banking crime proceeds still develop and are not yet comprehensive.

Harmonization among overlapping regulations such as ITE Law, Criminal Code, Banking Law, Consumer Protection Law, and sectoral regulations still requires improvement to avoid norm conflicts or regulatory vacuums. Jurisdictional aspects in transnational crime remain challenging, especially when perpetrators, victims, and servers are in different countries.

Law Enforcement Challenges

Digital Investigation Complexity

Digital banking crime investigation requires special expertise in digital forensics still limited among Indonesian law enforcement. Digital evidence collection must follow strict procedures to ensure data integrity and admissibility in court. Chain of custody must be maintained from evidence seizure moment to trial to ensure evidence is not manipulated.

Perpetrators often use anti-forensic techniques such as strong encryption, anonymization tools (VPN, Tor), or data destruction to erase digital traces. Investigation must race with time as log files and temporary data can disappear if not immediately secured. Limited adequate digital forensic tools and laboratories in many regions hamper investigation effectiveness.

Human Resource Capacity

The number of investigators with cyber forensics capability remains very limited compared to needs. Available training is often not sufficiently deep or updated with latest technology developments. High turnover rate as trained investigators often move to private sector offering better compensation creates difficulties maintaining institutional expertise.

Prosecutors and judges also require sufficient technical understanding to properly handle cybercrime cases, yet capacity building for legal professionals in technical technology aspects remains limited. Understanding gaps between technical investigators and legal professionals sometimes create difficulties in translating technical findings into strong legal arguments.

Inter-Agency Coordination

Digital banking crime handling involves many institutions with different authorities. National Police as primary investigators, BSSN as national cybersecurity coordinator, OJK and BI as financial sector regulators, Ministry of Communication and Information as telecommunications and digital content sector regulator, and banking institutions as victims or witnesses must coordinate effectively.

However, sectoral egos, operational procedure differences, and sometimes overlapping authorities create friction in coordination. Information sharing that should be fast and smooth is often hampered by bureaucracy or confidentiality concerns. Formal coordination mechanisms through forums such as Cyber Crime Prevention Coordination Team exist but effectiveness can still be improved.

Jurisdiction and International Cooperation Challenges

Borderless cybercrime characteristics create jurisdictional complexity. Perpetrators abroad attacking victims in Indonesia or using servers in third countries create questions about which jurisdiction applies. Indonesia adheres to territoriality principles (crime location) and active nationality principles (perpetrator citizenship) in criminal jurisdiction, yet application in cybercrime is not always straightforward.

Mutual Legal Assistance Treaty (MLAT) processes requesting international legal assistance are very bureaucratic and slow, often taking months or even years, yet digital evidence is very time-sensitive. Not all countries have extradition treaties with Indonesia, making perpetrators fleeing abroad difficult to reach. Legal system and evidentiary standard differences among countries also create challenges in law enforcement cooperation.

Technical and Resource Constraints

Limited budgets for procuring sophisticated and expensive digital investigation tools and equipment become practical constraints. Existing digital forensic laboratories remain limited in number and distribution, concentrated in Jakarta and major cities, while crime occurs throughout Indonesia. Access to international threat intelligence and databases about cybercrime patterns is sometimes limited or requires expensive subscriptions.

Law enforcement institutions must also compete with private sector in recruiting and retaining talent with technical expertise, yet remuneration structure limitations make

competition difficult. Investment in continuous training and development remains suboptimal for following technology development speed and crime modi.

Prevention Strategies: Penal Approaches

Criminalization Optimization

Criminal law substance updates need continuing to respond to technology developments and new crime modi. Specific preparatory conduct criminalization for cybercrime such as creation, distribution, or possession of hacking tools can strengthen early prevention. Sanction aggravation for crimes committed organized or with mass impact can provide stronger deterrence effects.

However, criminalization must be done carefully considering legality, certainty, and proportionality principles to avoid overcriminalization that can hinder technological innovation or violate fundamental rights. Balance between security protection and digital freedom needs careful maintenance.

Law Enforcement Capacity Strengthening

Massive investment in law enforcement capacity building is crucial. Comprehensive and continuous training programs in digital forensics, cybercrime investigation techniques, and legal aspects of cybercrime need regular organization. International certification for cyber investigators can improve credibility and competence.

Dedicated cybercrime unit's establishment at various police levels with specifically trained and equipped personnel needs expansion. Collaboration with private sector and academics in training delivery can access best expertise. Investigator secondment or internships to technology companies or security firms can provide exposure to current practices and tools.

Forensic Infrastructure Strengthening

Forensic laboratories development and expansion equipped with cutting-edge tools and equipment in various regions is important for accelerating investigation processes. Access to expensive commercial forensic software can be facilitated through centralized procurement or licensing agreements. Building collaboration with international forensic laboratories can provide access to capabilities not yet available domestically.

Digital forensic procedure and methodology standardization according to international best practices is important for ensuring evidence quality and acceptability in court. Proper documentation and strict chain of custody must become culture in every digital investigation.

Coordination and Collaboration Enhancement

Inter-agency coordination mechanism strengthening through joint task forces or integrated operations centers can improve digital banking crime response effectiveness. Clear Memoranda of Understanding (MoU) about roles, responsibilities, and coordination procedures among agencies need updating and consistent implementation.

Secure and accessible real-time information sharing platforms by all relevant stakeholders can accelerate detection and response. Regular joint exercises or simulations to test coordination in handling major incidents can identify gaps and improve readiness.

International Cooperation Strengthening

Indonesian accession to international conventions such as Budapest Convention on Cybercrime can strengthen international cooperation frameworks and legal harmonization. Expanding bilateral agreements network for mutual legal assistance and extradition especially with countries often becoming cybercrime perpetrator bases or safe havens.

Active participation in international forums such as INTERPOL Global Complex for Innovation, ASEAN Cybercrime Cooperation, and various regional working groups can facilitate information sharing and joint operations. Capacity building through international programs and technical assistance from more advanced countries or organizations can accelerate capability improvement.

Prevention Strategies: Non-Penal Approaches

Technology Infrastructure Security Strengthening

Banking institutions must consistently apply security-by-design principles in system and application development. Multi-factor authentication (MFA) must become standard for all financial transactions, not only relying on vulnerable passwords or SMS OTP. Biometric authentication such as fingerprint or face recognition can improve security.

End-to-end encryption for banking communications and transactions protects from interception. Regular security audits and penetration testing by independent parties can identify vulnerabilities before exploitation by criminals. Security patches and system updates must be done timely to close known security gaps.

Advanced security technologies implementation such as behavioral analytics for detecting transaction anomalies, machine learning for fraud detection, and artificial intelligence for threat intelligence can improve early detection capabilities. However, deployment must be accompanied by human oversight to avoid false positives and ensure accountability.

Digital Security Education and Literacy

Massive and continuous public education programs about digital security threats and safe banking practices are very important given human factors as weakest link. Campaigns must use multiple channels including mass media, social media, public service advertisements, and educational materials at bank branches.

Educational content must be adapted to different demographics considering varying digital literacy levels. For elderly or new users, face-to-face workshops or tutorials approaches may be more effective. For digital natives, viral social media content or gamification could be more engaging.

Topics that must be covered include: recognizing phishing attempts and social engineering tactics, importance of strong passwords and not sharing credentials, verifying authenticity of communications claiming to be from banks, being cautious with links and attachments, keeping software and apps updated, monitoring account activity regularly, and knowing how to report suspicious activity.

Partnerships with influencers, community leaders, or trusted figures can improve message reach and credibility. Success stories from people successfully avoiding fraud or warnings from victims can provide strong impact.

Rapid Detection and Response Systems

Sophisticated fraud detection systems development that can monitor real-time transactions and detect suspicious patterns is crucial. Systems must be able to automatically block or flag potentially fraudulent transactions for further verification. Machine learning algorithms can continuously learn from new crime patterns and adapt detection capabilities.

24/7 security operations centers (SOC) monitoring threats and incidents continuously enable rapid response when attacks are detected. Well-defined and regularly tested incident response plans ensure teams are ready to act quickly and coordinately when incidents occur.

Quick response mechanisms for reporting and handling fraud cases are important for minimizing losses. Easy-to-access hotlines, digital channels for reporting, and fast investigation processes can improve victim satisfaction and trust. Coordination with law enforcement for immediate actions such as freezing accounts or tracing funds must run seamlessly.

Consumer Protection and Empowerment

Strong regulatory frameworks for consumer protection in digital banking must be continuously strengthened. Clear liability frameworks regulating bank versus customer responsibilities in fraud cases need clear establishment for providing certainty. Fair, accessible, and efficient dispute resolution mechanisms are important for protecting consumer rights.

Compensation schemes for fraud victims must be fair and reasonable, though need balancing with incentives for consumers to be careful. Insurance products covering cybercrime losses can become additional safety nets. Banking institution transparency about security measures, incident statistics, and handling procedures can build trust and informed decision-making from consumers.

Consumer empowerment through tools facilitating monitoring and control over their own accounts is important. Features such as real-time transaction notifications, easy card blocking/unblocking, customizable transaction limits, and biometric login provide greater control to users. User-friendly interfaces and intuitive security features not burdening users with complexity can improve security practice adoption.

Digital Ecosystem Collaboration

Close public-private partnerships among government, banking institutions, technology companies, and cybersecurity firms are very important given shared responsibility in digital

ecosystem security. Information sharing about threats, attack vectors, and emerging risks must be done proactively and timely through secure platforms.

Industry associations such as Indonesian Banks Association can facilitate collective action and security practice standardization. Joint initiatives such as shared threat intelligence platforms or collaborative incident response can improve collective defense. Competitions or bug bounty programs inviting ethical hackers help identify vulnerabilities can be cost-effective supplements for security testing.

Engagement with academia for research, innovation, and talent pipeline development is important for long-term sustainability. Collaboration with civil society organizations can reach underserved communities and ensure inclusive approaches to digital security.

Stakeholder Roles in Prevention Ecosystem

Banking Institutions

Banks have primary responsibility for securing their systems and protecting customers. Investment in security infrastructure and technologies must be strategic priority not merely compliance requirement. Building internal cybersecurity capabilities through hiring specialists and continuous staff training is important for not overly depending on vendors.

Transparency in communicating risks and security measures to customers builds trust and educated users. Proactive customer education through various channels must be ongoing programs not only reactive when incidents occur. Responsible disclosure when breaches occur, though challenging from reputational standpoints, is important for maintaining long-term trust.

Collaboration with fellow banks in sharing threat intelligence and best practices must overcome competitive concerns given shared risks. Support for law enforcement in investigations and prosecution of cybercriminals is civic responsibility that must be executed with good cooperation.

Regulators and Supervisors

OJK and Bank Indonesia as regulators must continuously update regulatory frameworks to keep pace with technological developments. Cybersecurity standards and guidelines must be both comprehensive and flexible enough to accommodate innovation. Effective supervision with regular audits and assessments ensures compliance and identifies weaknesses early.

Capacity building for supervised entities particularly smaller banks or fintechs that may lack resources for sophisticated security needs facilitation. Facilitating industry information sharing through platforms or forums can enhance collective security. Taking decisive enforcement action against institutions negligent in security obligations provides compliance incentives.

Research and development in emerging technologies and risks must inform forward-looking regulation. International engagement to learn best practices and harmonize approaches particularly for cross-border issues is important for effective oversight.

Law Enforcement

National Police and prosecutors as frontline law enforcement must continuously upgrade capabilities in cybercrime investigations and prosecutions. Specialization with dedicated, well-trained and well-equipped cyber units is critical for effectiveness. Building collaborative relationships with victims (banks) for smooth reporting and investigation processes is important.

Proactive intelligence gathering about cybercriminal networks and emerging threats can enable preventive actions not only reactive investigations. International cooperation through channels such as INTERPOL or bilateral agreements is essential for transnational cases. Public communication about successful prosecutions can provide deterrence effects and reassure public.

Balancing enforcement with privacy rights and avoiding overreach in investigations is important for maintaining public trust. Transparency in processes and accountability for actions helps legitimacy of law enforcement efforts.

Society and Consumers

Users themselves have responsibility for secure banking practices. Being vigilant, skeptical toward suspicious communications, and following security advice from banks can significantly reduce victimization. Promptly reporting suspicious activity or suspected fraud

enables quick response. Keeping informed about latest threats and scams through reliable sources is important for awareness.

Community engagement in peer education and looking out for vulnerable members such as elderly or less tech-savvy can create collective vigilance. Advocacy for better protections and demanding accountability from institutions and authorities is consumer right that needs voicing through consumer organizations or public forum.

5. Conclusions

Digital banking crime constitutes serious threat continuously developing alongside financial sector digital transformation in Indonesia. Complexity, sophistication, and massive impact of these crimes require comprehensive, integrated, and adaptive criminal policy responses. Existing legal frameworks have provided foundations, yet still require continuous updates to anticipate technology evolution and crime modi.

Penal approaches through criminalization, strict law enforcement, and adequate sanctions remain important for providing deterrence effects and upholding justice. However, given special cybercrime characteristics, non-penal approaches through technology security strengthening, public education, early detection systems, and multi-stakeholder collaboration become equally fundamental. Integration of both approaches in holistic strategies involving all stakeholders in digital banking ecosystem is key to prevention effectiveness.

Significant challenges in law enforcement capacity, institutional coordination, and international cooperation require serious attention and continuous investment. However, with strong political will, adequate resource allocation, and collaborative commitment from all parties, Indonesia can build more resilient systems against digital banking crime while continuing to support digital financial innovation and inclusion.

References

Arief, B. N. (2020). *Criminal law policy: Development in drafting new criminal code concepts* (Revised ed.). Jakarta: Kencana Prenada Media Group.

Bank Indonesia. (2021). *Bank Indonesia Regulation Number 23/6/PBI/2021 on Financial Technology Implementation*.

Casey, E. (2021). *Digital evidence and computer crime: Forensic science, computers, and the internet* (4th ed.). London: Academic Press.

Choo, K. K. R., & Grabosky, P. (2023). Cybercrime and digital forensics: Contemporary challenges and future directions. *British Journal of Criminology, 63*(2), 245–264.

Clough, J. (2022). *Principles of cybercrime* (3rd ed.). Cambridge: Cambridge University Press.

Europol. (2023). *Internet Organised Crime Threat Assessment (IOCTA) 2023*. The Hague: European Cybercrime Centre.

Financial Services Authority (OJK). (2022). *Financial Services Authority Regulation Number 11/POJK.03/2022 on Information Technology Implementation by Commercial Banks*.

Financial Services Authority (OJK). (2024). *Indonesian banking statistics 2023*. Jakarta: OJK.

Ghernaouti, S. (2021). *Cyber power: Crime, conflict and security in cyberspace*. Lausanne: EPFL Press.

Holt, T. J., & Bossler, A. M. (2020). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. London: Routledge.

Interpol. (2022). *Global cybercrime report: Assessing cybercrime and response capacity globally*. Lyon: INTERPOL Innovation Centre.

Kshetri, N. (2023). The economics of cybersecurity: Regulations, compliance, and market failure. *Journal of Economic Perspectives, 37*(1), 89–112.

Maitri, P. V. (2020). Digital banking frauds: Challenges and the way forward. *International Journal of Law Management & Humanities, 3*(4), 1456–1472.

National Cyber and Crypto Agency (BSSN). (2023). *Indonesia cyber security annual report 2023*. Jakarta: BSSN.

Prasetyo, T. (2021). *Information technology criminal law: Theory and practice*. Yogyakarta: Pustaka Pelajar.

Republic of Indonesia. (2024). *Law Number 1 of 2024 on Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions*.

Sari, D. P., & Rahman, A. (2022). Cybercrime in Indonesia's digital banking: Challenges in law enforcement. *Journal of Financial Crime, 29*(3), 892–908.

Sitompul, J. (2020). *Cyberspace, cybercrimes, cyberlaw: Criminal law aspects review*. Jakarta: Tatanusa.

Tropina, T., & Callanan, C. (2022). *Self- and co-regulation in cybercrime, cybersecurity and national security*. Berlin: Springer.

Wall, D. S. (2021). *Cybercrime and society* (3rd ed.). London: Sage Publications.

Widodo, S. (2023). Criminal policy in tackling digital banking crimes: Indonesian context. *Asian Journal of Criminology, 18*(2), 167–186.

Yar, M., & Steinmetz, K. F. (2023). *Cybercrime and society* (4th ed.). London: Sage Publications.