

Deepfake-Driven Financial Fraud In Indonesia: A Systematic Review Of Economic Impacts And Regulatory Challenges

Muhammad Arsalan Khan¹, Hidayatul Khusnah^{2*}, Emeraldalda Ayu Kusuma³, Mar'a Elthaf Ilahiyah⁴, Muhammad Zeeshan Khan⁵

¹Postdoctoral Fellow, Center for Data and Business Intelligence, Universitas Nahdlatul Ulama Surabaya, Indonesia

^{2*}Department of Accounting, Faculty of Business Economics and Digital Technology, Universitas Nahdlatul Ulama, Surabaya, Indonesia

³Department of Management, Sekolah Tinggi Ilmu Ekonomi Indonesia

⁴Department of Accounting, Faculty of Economic and Business, Sekolah Tinggi Ilmu Ekonomi Indonesia

⁵Department of Computer science, Islamia College Peshawar Khyber Pakhtunkhwa, Pakistan;

Corresponding Author: Hidayatul Khusnah

Abstract

Deepfake technology, utilizing advanced artificial intelligence to create hyper-realistic synthetic media, poses a significant threat to Indonesia's financial sector, exploiting the nation's rapid digital transformation. This study synthesizes over 50 secondary sources, including academic papers, industry reports, and regulatory documents from 2020 to October 2025, to assess the economic impact and regulatory responses to deepfake-enabled financial fraud. Findings reveal losses exceeding \$138.5 million, driven by a 1,550% surge in AI-driven fraud within fintech from 2022 to 2024, primarily through biometric spoofing and impersonation scams. These incidents undermine financial inclusion for 66 million unbanked Indonesians and erode trust in digital platforms. Regulatory efforts, led by the Financial Services Authority and Ministry of Communication and Digital Affairs, include ethical AI guidelines and enhanced biometric protocols, reducing fraud attempts by 20–30%. However, gaps in specific legislation and low digital literacy (42% proficiency) hinder enforcement. Limitations include underreported losses and reliance on potentially outdated secondary data. Future research should incorporate primary data and explore emerging fraud vectors. Recommendations advocate for a dedicated deepfake law, inter-agency coordination, advanced detection tools, and public education to ensure a resilient financial ecosystem.

Keywords: Deepfake, financial fraud, fintech, biometric spoofing, regulatory framework

JEL Classification Codes: G21, K24, O33, E26, G28, D18

INTRODUCTION

The emergence of the deepfake technology, in which sophisticated AI codes are applied to produce or modify audio and video and images and have the capacity to sound and appear very natural, has posed considerable challenges to the social confidence and economic well-being of the world community. Deepfakes are a result of the advancements in the area of generative adversarial networks and it is possible to create convincing synthetic media and utilize it to offer deception of different types, successfully representing a person. This technology renders the field of finance in the worse situation because it allows scammers to bypass firewalls, such as biometrical authentication, to perform unauthorized transactions and impersonation. As the digital economies expand, the intersection of deepfakes and financial fraud will become a burning topic in academic literature, particularly in the new economies, where regulation may lag behind technological progress.

Deepfakes activities in the world have been related to the rising cases of financial losses as it has been approximated that the fraud has led to losses estimated at one billion and eight hundred million dollars within the past few years. This blast has been fueled by the presence of AI technologies that make the creation of fake content democratic and enable inexperienced people to engage in frauds. High-profile cases of the use of deepfakes in Asia and others is an example of how cybercriminals have used deepfakes to impersonate executives in video calls, authorize multimillion-dollar deals, and other cases. The economic effects are not only on the direct financial losses but also on the loss of consumer confidence, increased costs of running the business to detect frauds and the integrity implication in the market. The instances of deepfakes have been increasing great heights in Asia-Pacific, where 1,530% increase in deepfakes during the years of 2022-2023 is reported, which can be taken as evidence of the vulnerability of the region to online products. These tendencies demonstrate that there is a desperate necessity to have interdisciplinary studies that would cut across technology, economics and policy to minimize such threats.

With a further focus on Indonesia, a country with the developing digital economy, the effects of the financial fraud, made possible with the help of deepfakes, are especially severe. Internet penetration is at 77% and mobile banking users are now more than 200 million, meaning that Indonesia has experienced a rapid increase in fintech services, which increase financial inclusion but also expose users to greater risks of cybercrime. The billions-worth fintech industry of the country has turned into a scam of the AI-enhanced scams, in which deepfakes are used to evade Know Your Customer (KYC) rules and impersonate someone to take illegal loans or transfers. Recent research findings indicate that 100 percent of Indonesian companies are worried about AI-generated fraud, and half of them have experienced synthetic identity theft, which weakens biometric systems and causes significant economic damages. The demographic profile of Indonesia, such as a significant number of unbanked people, only adds to this vulnerability, and social engineering attack with deepfake technology strengthens it.

The financial damages that deep fake fraud can cause in Indonesia are unbelievable, with reported cases reported above 138 million dollars in one-off cases of biometric spoofing (Group-IB, 2024). As an example, one of the biggest financial institutions has stated that it received over 1,100 instances of deepfakes in a month in 2024, costing the bank millions of dollars of fraudulent submissions. Greater surveys indicate that AI-motivated fraud within the fintech ecosystem is set to grow by 1,550 percent between 2022-2024, and deepfakes are going to make up a significant portion of financial scamming activity exercises. Such figures are not only the signs of direct costs but also indirect costs in the form of higher insurance rates, legal cost and the loss of reputation that discourages to invest in the sphere of digital services. Furthermore, it causes a psychological impact on the victims, like emotional misery related to identity loss, which is an immaterial, yet relevant weight to be put on the economic one. In comparison to the worldwide trends, the losses in Indonesia can be compared to the ones experienced in the Southeast, where the cyberfraud like deepfakes generated illegal income up to 37 billion dollars in the year 2023, and the area is truly connected with such threats.

Indonesia has been responding to these challenges by formulating regulatory responses that are in line with the challenges but still have a lot of gaps. Financial Services Authority (OJK) has also proposed ethical use of AI in fintech, such as transparency in algorithms and stronger biometric security. Along with this the Ministry of Communication and Digital Affairs (Kominfo) has already made circulars on ethics of AI, encouraging platforms to deploy detection devices and content moderation to prevent the spread of deepfakes. The recent future, including the OJK Regulation on digital financial assets No. 27/2024 and the 2025 AI Governance Book on Banking, is expected to enhance regulation

on AI misuse. Nevertheless, the current laws such as the Electronic Information and Transactions (ITE) Law and Personal Data Protection Law are insufficient in clearly dealing with deepfakes without definitions, sanctions, and enforcement that are specific to synthetic media. Such ambiguities in law have been observed by scholars to impede prosecution as seen in difficulties in proving deepfake involvement in online fraud cases. Globally, Indonesia is inspired by such a model as Deep Synthesis Provisions in China or the AI Act in the EU, which recommends vicarious liability on platforms and compulsory watermarking of AI-generated materials. Even with such initiatives, poor digital literacy whereby 42 percent of the citizens are skilled at detecting fake news and scarce technological means make it more challenging to enforce.

The study fills an important gap in research: the literature on deepfakes in the world is quite rich, but the specifics of the situation in Indonesia are underrepresented, and the interplay between the economic loss and the effectiveness of regulations is not thoroughly examined in the context of an emerging economy. Previous studies have mainly dwelled on technological detection or political connotations, and little has been done on the socioeconomic aspects of financial fraud. This study is meant to quantify the economic impacts and assess regulatory reaction and suggest actionable recommendations by synthesizing secondary data through the use of scholarly papers, industry reports, and regulatory documentations dating back to 2020 and 2025. The systematic literature review that follows PRISMA protocols is used to guarantee the comprehensive and rigorous analysis using more than 50 sources.

The objectives are threefold: first, to delineate the scale of economic losses from deepfake fraud in Indonesia's financial sector; second, to assess the adequacy of current regulatory frameworks; and third, to identify strategies for enhanced mitigation. This approach not only contributes to academic discourse but also informs policymakers and practitioners in fostering resilient digital ecosystems. The subsequent sections will explore methodology, detailed findings on economic losses, regulatory analyses, discussion of implications, and concluding recommendations.

METHODOLOGY

In order to fully evaluate the consequences of deepfake-enhanced financial fraud in Indonesia, the current research will employ a systematic literature review approach, which is facilitated by the PRISMA framework to guarantee rigor, transparency, and reproducibility. This methodology is quite appropriate in the case of secondary data analysis since it will allow synthesizing various sources to answer the research questions: What are quantified losses in the financial sector of Indonesia due to deepfake fraud and how effective are existing regulatory responses? Using the existing scholarly articles, industry reports, and regulatory documents, the methodology also circumvents the ethical and logistical issues of primary data collection in a sensitive area as financial fraud, and it captures the current trends up to 2025.

Data Collection

The process of data collection was conducted through a methodical search of academic databases and reliable online repositories to find the relevant secondary sources. Preference was given to such databases as Google Scholar, JSTOR, Researchgate, and institutional sources as the Financial Services Authority (OJK) and the Ministry of Communication and Digital Affairs (Kominfo). Search terms included "deepfake financial fraud Indonesia," "AI-driven scams fintech Indonesia 2020-2025," "deepfake economic losses Indonesia," and "deepfake regulatory frameworks Indonesia." Boolean operators (e.g., AND, OR) and filters for publication dates (2020–2025) refined the search to capture recent developments in AI-driven fraud. Additional searches on professional outlets, such

as reports from Group-IB, VIDA, and Surfshark, supplemented academic findings with industry perspectives.

Inclusion criteria were established to ensure source relevance and quality:

- **Time Frame:** Publications from 2020 to October 2025, reflecting the rapid evolution of deepfake technology and its financial applications.
- **Geographic Focus:** Studies and reports specific to Indonesia or inclusive of Southeast Asia, with explicit references to deepfake-related fraud.
- **Content Type:** Peer-reviewed articles, industry reports, government publications, and reputable news analyses containing empirical data (e.g., loss estimates, case studies) or policy evaluations.
- **Language:** English and Indonesian sources to encompass local regulatory documents and global comparisons.
- **Relevance:** Sources addressing economic impacts, regulatory responses, or case studies of deepfake fraud in financial contexts.

Exclusion criteria eliminated non-peer-reviewed blogs, opinion pieces lacking empirical backing, and studies unrelated to financial fraud or Indonesia. The search yielded over 50 sources, including 20 peer-reviewed papers, 15 industry reports, 10 regulatory documents, and 5 news articles from credible outlets like Forbes and Reuters. Cross-verification ensured source reliability, with preference given to publications from established organizations (e.g., OECD, World Economic Forum) and academic journals.

Data Extraction and Analysis

Data extraction was conducted systematically to categorize findings into three thematic areas: economic losses, regulatory responses, and case studies of deepfake fraud. A standardized template recorded key details from each source, including:

- Quantitative metrics (e.g., financial loss estimates, fraud incident rates).
- Qualitative insights (e.g., descriptions of fraud mechanisms, regulatory challenges).
- Contextual factors (e.g., sector-specific impacts, regional comparisons).

Thematic analysis was performed using NVivo software to code and organize data, identifying patterns such as prevalent fraud tactics (e.g., biometric spoofing, executive impersonation) and gaps in legal frameworks. Quantitative data, such as loss figures and fraud surge percentages, were aggregated to provide descriptive statistics, visualized through tables and charts for clarity. For instance, loss estimates were cross-referenced across sources to validate figures like the \$138.5 million in potential damages reported by Group-IB (2024). Qualitative data underwent content analysis to extract recurring themes, such as the inadequacy of the Electronic Information and Transactions (ITE) Law in addressing deepfakes (Huda & Rachman, 2025).

Ethical Considerations

As the study relies solely on secondary data, ethical concerns related to participant consent or data privacy were minimal. However, ethical rigor was maintained by ensuring accurate representation of source materials and avoiding selective reporting. Plagiarism was prevented through meticulous citation, and sources were evaluated for credibility to exclude misleading or unverified claims. The study also considered the ethical implications of discussing fraud cases, anonymizing specific institutional references where confidentiality was a concern, as noted in some industry reports.

Limitations

The reliance on secondary data introduces limitations, including potential gaps in unreported fraud incidents and regional variations in data availability. Indonesia-specific

studies on deepfake fraud are limited compared to global analyses, necessitating extrapolation from Southeast Asian trends. Additionally, the dynamic nature of AI technology means that some findings may become outdated as new detection methods emerge. These limitations were addressed by focusing on high-quality sources and acknowledging uncertainties in the discussion section.

LITERATURE REVIEW

Global Context of Deepfake Fraud Losses

To fully appreciate the scale of deepfake-enabled financial fraud in Indonesia, it is essential to situate it within the broader global context, where losses have surged exponentially with the democratization of AI tools. Worldwide, deepfake fraud has inflicted financial damages approaching \$900 million, with the first half of 2025 alone accounting for \$410 million, a marked increase from \$359 million in 2024 and \$128 million cumulatively prior (Surfshark, 2025). This trajectory reflects the accessibility of deepfake generation software, which allows even low-skilled actors to create convincing forgeries for scams such as voice cloning in wire transfer requests or video manipulations in investment frauds. For instance, the Wall Street Journal documented over \$200 million in losses to deepfake scams in the first quarter of 2025, predominantly targeting financial institutions through impersonation tactics (Oz Forensics, n.d.). The economic value of digital disruption further illustrates this escalation, as AI-driven technologies like deepfakes have created millions of new jobs while simultaneously enabling fraud that could account for nearly a quarter of global GDP by 2025, with surplus value calculations revealing the dual-edged nature of innovation (Kumar, 2023). In addition, the rise of generative AI has amplified these risks, leading to numerous incidents of financial loss through synthetic media, as noted in analyses of beyond-data-privacy threats where deepfakes contribute to severe economic harms (Du et al., 2025). The face of deception in financial markets further highlights how deepfake fraud undermines trust, with hyper-realistic manipulations causing significant market disruptions globally (Kumar et al., 2025).

In the Asia-Pacific region, the growth has been particularly pronounced, with a 1,540% increase in deepfake fraud incidents from 2022 to 2023, driven by rapid fintech adoption and varying regulatory maturity (VIDA, 2024a). Deloitte projections estimate that by 2027, such fraud could escalate to unprecedented levels, potentially costing the global economy tens of billions annually if unchecked (VIDA, 2024a). Southeast Asia, including Indonesia, has emerged as a hotspot, with cyber scamming operations generating over \$43.8 billion in illicit gains in 2023, a significant portion attributable to AI-enhanced frauds like deepfakes (Center for Strategic and International Studies [CSIS], 2024). These regional dynamics underscore how deepfakes exploit interconnected financial networks, where a single breach can cascade into widespread economic harm, including stock market manipulations and cross-border money laundering. The hybrid harm-centric model highlights how online fraud, including deepfakes, inflicts visceral victimization, with economic losses in the 1990s alone estimated at USD \$900 million annually, a figure that has ballooned with AI advancements (Cantin, 2025). The impact on Islamic banking trust and security further reveals emerging threats, as deepfake videos have compromised financial integrity, necessitating robust mitigation strategies (Kismawadi, 2025).

Deepfake Fraud in Indonesia: An Overview

Moving to the case of Indonesia, the country is highly vulnerable to the use of deepfakes due to its active digital economy that boasts a high internet penetration rate and a thriving

fintech market. Indonesia has more than 200 million mobile banking clients and a billions of dollar fintech valuations, so an AI-driven deception has fertile territory on its financial front (World Economic Forum, 2025). According to secondary sources, the deepfake fraud has increased exponentially, with the number of AI-related cases in the fintech sector growing 1,550 percent in the period between 2022 and 2024 (AuthMe, 2025). This increase is credited to the growth of fake media to evade the Know Your Customer (KYC) procedures, create fake loan applications, and pose as authorities in fraud schemes. Techno-optimism in innovation law and policy further exacerbates this, as rapid adoption of AI tools without adequate safeguards has stoked political polarization and deepfakes, leading to severe financial harms in emerging markets like Indonesia (Lee, 2025). Legal analysis from a fair and civilized humanity perspective highlights instances of deepfake fraud involving figures like President Prabowo Subianto and Finance Minister Sri Mulyani, emphasizing the societal impact of such manipulations (Pamungkas et al., 2025). Industry reports highlight that deepfakes primarily target biometric verification systems, which are integral to Indonesia's digital financial services. For example, criminals employ AI to generate synthetic identities, tricking facial recognition and liveness detection mechanisms, thereby enabling unauthorized access and transactions (VIDA, 2024b). A survey of Indonesian businesses revealed that 100% express concern over AI-generated fraud, with 56% reporting encounters with synthetic identity theft and 67% facing impersonation scams (VIDA, n.d.). These statistics illustrate the pervasive nature of the threat, where deepfakes not only cause immediate losses but also erode consumer trust, potentially stalling the country's financial inclusion goals for its 66 million unbanked population. The trends in computer science and information technology research further note that deepfakes, alongside other AI disruptions, have led to overheating and damage in financial systems, with economic growth changes in Indonesia linked to a 15% rise in such incidents (Kulkarni & Angurala, 2024). Legal gaps in the Electronic Information and Transactions (ITE) Law further complicate responses, as it lacks specific provisions for deepfake technology, posing challenges for regulatory enforcement (Rama et al., 2025).

Quantified Economic Losses

Secondary sources provide concrete estimates of the financial toll, painting a picture of escalating damages. In Indonesia alone, potential losses from deepfake fraud have been pegged at \$138.5 million, stemming from incidents involving biometric bypass and identity synthesis (Group-IB, 2024). One prominent financial institution reported detecting over 1,100 deepfake attempts in August 2024, resulting in losses exceeding \$135 million through fraudulent loan disbursements and account takeovers (Group-IB, 2024). Broader analyses from the OECD indicate that AI-generated deepfakes have caused widespread financial and identity harm, with individual and business losses in Indonesia aligning with regional patterns of exponential growth (OECD.AI, 2024). The economics of cryptocurrencies and AI further contextualize this, as blockchain and digital currency disruptions have mirrored deepfake trends, with generative AI contributing to conversion rate manipulations and customer satisfaction declines in fintech, leading to annual losses in the hundreds of millions (Agarwal et al., 2021).

Deepfakes account for approximately 31% of money-scramming incidents in the fintech sector, where they facilitate sophisticated schemes like voice-cloned investment pitches or video-forged endorsements (Intimedia, n.d.). The Safer Internet Lab's 2025 report on online fraud in Indonesia notes that most losses derive from deepfake videos exploiting public figures to promote malicious schemes, contributing to cumulative damages in the hundreds of millions (Safer Internet Lab, 2025). When contextualized regionally, Indonesia's experiences mirror those in Southeast Asia, where cyberfraud factories often leveraging deepfakes generate billions in illicit revenue, with Indonesia contributing

significantly due to its large digital user base (CSIS, 2024). The dignity and deepfakes discussion adds depth, as these technologies inflict dignitary harms beyond economics, with over 900 opinions citing related victimization in financial contexts (Goodyear, 2025). The break glass safeguards for social media emphasize that Telegram's 900 million users have amplified deepfake dissemination, leading to numerous advanced approaches needed for mitigation (Mishra & Fiske, 2025). Criminal liability studies further note the misuse of AI in deepfake crimes, with significant financial fraud cases highlighting the need for accountability frameworks in Indonesia (Sembiring & Firdaus, 2025). To illustrate these impacts, consider the following Table 1 summarizing key metrics from 2024–2025:

Table 1: Summary of key metrics from 2024–2025

Metric	Value	Source
Potential national losses from deepfake fraud	\$138.5 million	Group-IB (2024)
Losses from biometric bypass in one institution	>\$135 million	Group-IB (2024)
Surge in AI-driven fintech fraud (2022–2024)	1,550%	AuthMe (2025)
Businesses encountering synthetic identity fraud	56%	VIDA (n.d.)
Global deepfake losses (H1 2025)	\$410 million	Surfshark (2025)
Asia-Pacific deepfake surge (2022–2023)	1,540%	VIDA (2024a)
Southeast Asia cyberfraud illicit gains (2023)	>\$43.8 billion	CSIS (2024)

This data underscores the quantitative severity, yet it likely underestimates the true extent due to underreporting, as many victims and institutions avoid disclosure to preserve reputation.

Case Studies of Deepfake Fraud in Indonesia

Detailed case studies from secondary sources reveal the mechanics and consequences of deepfake fraud, offering insights into real-world applications. One notable incident involved deepfake videos of prominent public figures promoting fraudulent investment platforms, leading to widespread victim losses estimated in the millions (Safer Internet Lab, 2025). In this scheme, perpetrators used AI to superimpose celebrities' faces onto scripted endorsements, deceiving users into transferring funds to scam accounts. Similarly, in the financial sector, a 2024 case saw fraudsters employing deepfake video calls to impersonate bank executives, authorizing illicit transfers and causing institutional losses exceeding \$25 million in a single event, akin to global precedents (Intimedia, n.d.). Another example from fintech highlights how deepfakes sabotage inclusion efforts: criminals created synthetic identities to apply for loans, bypassing KYC with forged biometric data, resulting in non-performing loans and operational disruptions (VIDA, 2024b). The OECD documented multiple instances where deepfakes led to identity theft, with victims facing long-term financial recovery challenges, including credit score damage and legal fees (OECD.AI, 2024). These cases demonstrate not only direct losses but also the ripple effects, such as increased scrutiny from regulators and higher compliance costs for affected entities.

Sector-Specific Impacts

The economic burden varies across sectors, with fintech and traditional banking bearing the brunt. In fintech, deepfakes facilitate account takeovers and phishing, comprising a significant share of fraud cases (AuthMe, 2025). Projections indicate that without advanced detection, losses could hinder the sector's 16.8% annual growth rate through 2025 (Oliver Wyman, 2024). In banking, vulnerabilities include manipulated executive communications, as seen in impersonation scams that erode institutional trust and inflate insurance premiums (Group-IB, 2024).

Beyond finance, spillover effects impact related industries, such as insurance, where deepfake claims fraud increases processing costs, and e-commerce, where synthetic reviews manipulate markets (CSIS, 2024).

Indirect and Long-Term Economic Costs

While direct losses dominate headlines, indirect costs such as reputational damage, reduced investor confidence, and diminished financial inclusion amplify the economic impact. Deepfakes contribute to a "trust deficit" in digital services, potentially excluding vulnerable populations from fintech benefits (VIDA, 2024b). Operational expenses for enhanced security, including AI detection tools, add billions globally, with Indonesia facing proportional burdens (Oz Forensics, n.d.). Long-term projections suggest that unchecked deepfake fraud could stunt GDP growth in emerging markets by impeding digital economy expansion (Deloitte, as cited in VIDA, 2024a).

Projections and Implications

Looking ahead, secondary data forecast continued escalation, with Deloitte predicting a tripling of deepfake incidents by 2027 (VIDA, 2024a). For Indonesia, this implies potential losses in the billions if regulatory and technological gaps persist. The implications extend to national security, as deepfakes intersect with broader cyber threats, necessitating integrated responses.

In conclusion, the economic losses from deepfake-enabled financial fraud in Indonesia, as evidenced by secondary data, are profound and multifaceted, demanding proactive measures to safeguard the nation's digital future. The following section will explore regulatory responses in detail.

Regulatory Responses and Challenges

The regulatory landscape surrounding deepfake-enabled financial fraud in Indonesia reflects a proactive yet evolving effort to address the intersection of artificial intelligence, cybersecurity, and financial integrity. With the development of the deepfake technology, regulators have two roles to play: encouraging digital economy innovation and reducing consumer and institution risks. The responses to this situation in Indonesia are organized mainly by the Financial Services Authority (Otoritas Jasa Keuangan, OJK) and the Ministry of Communications and Digital Affairs (Kominfo) with support offered by the existent laws, including the Electronic Information and Transactions (ITE) Law and the Personal Data Protection Law. In this part, I will integrate secondary sources of data found in regulatory documents, scholarly reviews, and industry reports to determine the extent, practice, and efficacy of these measures. Through the analysis of major efforts, enforcement issues, case studies and international factors, it is possible to see the positive aspects of ethical rules, yet the lack of specificity and enforcement remains evident, and more resilient frameworks are required to address the threat of deepfakes in the financial industry. The legal issues in the fight against deepfake abuse also underline the necessity of comparative regulation of AI to improve privacy benefits and online safety basing on the world example (Doing et al., 2025).

Overview of Indonesia's Regulatory Framework

The strategy adopted by Indonesia to regulate AI and deepfakes in the financial sector is based on a set of laws that govern the digital sphere of the country, which had been developed in the early 2000s and modified with time in response to the new technologies. One of its cornerstones is the ITE Law (Law No. 11/ 2008 that was amended in 2016 and Law No. 19/ 2016) that criminalize the distribution of fake news that might cause harm or economic losses including manipulated media (Huda and Rachman, 2025). Nevertheless, this legislation was enacted before the proliferation of deepfakes, and it has no specific references to AI-generated content, considering deepblots as belonging to more extensive groups of electronic misinformation or fraud (Dentons HPRP, 2024). Biochemical information which is essential to financial checks is also better safeguarded by the Personal Data Protection Law (Law No. 27/2022) requiring consenting and protection against unauthorized use but does not specifically address synthetic media manipulations (Akhmad and Rachman, 2025). The step to improve digital security by enhancing e-law optimization and deeply regulating deepfakes can be considered in comparison with China and implied the urgency of the application of Indonesian-specific frameworks (Lestari et al., 2025).

As a reaction to the increasing threats of AI, OJK has published specifications on the financial sector. The Code of Responsible AI Use in Fintech (early 2024) of the OJK focuses on ethical use of AI, implying the transparency of the algorithms and the risks of various technologies, such as deepfakes (OJK, 2024). This is supplemented by the OJK Regulation No. 27/2024 on Digital Financial Assets that introduces controls to cryptocurrencies and digital wallets with deepfake scams that force them to improve KYC procedures and fraud detection (OJK, 2024). One of the most notable advances to date is the AI Governance Book of Indonesian Banking in April 2025 that is based on the Basel Committee standards and tries to specifically cover the deepfake risks in relation to the liveness detection, behavioral biometrics, and multi-factor authentication in transaction approvals (OJK, 2025). The documents will encourage the use of a risk-centric approach to promote AI forensics along with staff education in identifying synthetic impersonations. A sophisticated digital investment fraud prevention legal framework also complements these efforts and tackles the intricate fraud arrangements through deepfake technology (Napitupulu et al., 2025).

Kominfo is a key player in the enhanced regulation of digital content. As of 2024-2025, Kominfo created a circular on AI ethics, which requires online platforms to adopt content moderation algorithms, such as deepfake detection ones, and report suspicious users (Kominfo, 2024). The project is based on international best practices, which demand cooperating with technology companies to watermark AI-generated content; this is necessary and needs to promote awareness campaigns among the public (Rouse, 2025). Also, Kominfo organizes its collaboration with Bank Indonesia around consumer protection in digital payment, incorporating deepfake protection in the country and policies in cyberspace (Bank Indonesia, 2024). The crypto-based and AI-driven organized fraud research supports the digital activities of Bank Indonesia, proposing a series of practical countermeasures to help it mitigate the emerging risks (Lin, 2025).

The academic reviews note that the rules constitute a transition between reactive and active regulation of the financial system, and the frameworks of OJK contribute to the self-regulation of the financial institutions (Prabowo and Suryanto, 2023). An example of this is the AI Governance Book, which requires AI systems to be audited annually to understand the vulnerability to deepfakes that could minimize cases of fraud through the abilities to detect possible frauds (OJK, 2025). According to industry reports, 72% of surveyed fintech companies have already implemented these rules, and as a result, have better biometric protection and fewer attempted spoofing attacks after implementation

have claimed to have dropped to 20-30% (VIDA, 2024a). The lessons on cybersecurity in the European Union that relate to AI-cybercrimes provided valuable insights to Indonesia, stating the relevance of starting the regulation of AI development (Hussin and Ginano, 2023).

Key Challenges in Regulatory Implementation

Although these have been achieved, there are major issues that impede the efficiency of the Indonesian regulatory responses. One of them is the lack of specific legislation concerning deepfakes that can be enforced only through the interpretation of the current laws. Researchers state that current clauses of the ITE Law on misinformation are inadequate to prosecute the instances of deepfake, because in the case of AI-generated fraud, it is difficult to demonstrate intent and harm, which usually necessitates a high level of forensic skills that are generally unavailable to the judicial procedure (Huda and Rachman, 2025). Indicatively, the law punishes electronic fraud but fails to identify the term deep fake and specify the technical requirements of the admissibility of evidence leading to a low conviction rate and extended investigations (Rachman & Aditya, 2025). The lack of a legal framework in Indonesia concerning electronic information and transactions adds to the problems and presents more difficulties, which would require the recommendations to be made to the regulatory levels (Rama et al., 2025).

The lack of resources and cross-jurisdictions aggravates enforcement gaps. OJK and Kominfo are siloed organizations without a lot of inter-agency coordination, which results in inconsistent application across the sectors (Dentons HPRP, 2024). Digital literacy remains a hurdle, with surveys indicating that only 42% of Indonesians can distinguish real from fake content, complicating victim reporting and regulatory monitoring (Kusumawardani & Rachman, 2025). Furthermore, the transnational nature of deepfake fraud often orchestrated from overseas scam hubs in Southeast Asia challenges national borders, as perpetrators exploit encrypted platforms beyond Indonesian jurisdiction (CSIS, 2024). The haze of artificial intelligence's accountability based on international law further complicates deepfake fraud cases, particularly in online loan contexts (Davey & Sauerwein, 2023).

Technological lag poses another barrier. While OJK mandates detection tools, many financial institutions in Indonesia rely on outdated systems, with only larger banks affording advanced AI countermeasures (Group-IB, 2024). Small and medium-sized fintech firms, which dominate the market, face compliance burdens that could stifle innovation without adequate support (Oliver Wyman, 2024). Academic studies critique the reactive nature of regulations, noting that guidelines often follow major incidents rather than preempting them, allowing fraudsters to adapt faster than regulators (Aditya, 2023). Indonesia's readiness to face social engineering attacks with deepfake technology highlights these preparedness gaps, with negative consequences like financial fraud underscoring the need for action (Noval, 2023).

Case Studies in Regulatory Enforcement

Real-world enforcement cases illustrate both successes and limitations. In February 2025, Indonesian authorities, under Kominfo and police coordination, arrested individuals behind a deepfake scam using manipulated videos of President Prabowo to promote fraudulent investments, defrauding victims of Rp65 million across 20 provinces (Safer Internet Lab, 2025). This operation leveraged ITE Law provisions and Kominfo's reporting mechanisms, resulting in swift takedowns of scam platforms and public warnings. However, the case highlighted traceability issues, as perpetrators used VPNs and overseas servers, delaying full asset recovery (Rachman & Aditya, 2025). Legal analysis on the use of deepfake technology in banking institutions further notes the threat

to financial integrity, emphasizing the need for regulatory readiness (Gunawan & Janisriwati, 2023).

Another example involves OJK's intervention in a 2024 fintech fraud ring employing deepfakes for loan approvals. Following reports of synthetic identity theft, OJK imposed fines and mandated biometric upgrades on implicated platforms, aligning with Regulation No. 27/2024 (OJK, 2024). This led to the suspension of several apps and recovery of partial losses, demonstrating regulatory teeth in consumer protection. Yet, critics point out that such actions are post-hoc, with victims often bearing initial burdens due to inadequate preventive measures (Prabowo & Suryanto, 2023). Deep fakes in P2PL services highlight legal challenges and data privacy risks, with financial industry vulnerabilities underscoring the need for robust safeguards (Yuspin et al., 2025).

In the banking sector, the AI Governance Book's implementation has prompted audits revealing vulnerabilities in executive communication protocols. A 2025 case where deepfake video calls attempted to authorize transfers was thwarted due to mandated behavioral analysis, preventing potential multimillion-dollar losses (Group-IB, 2024). These instances underscore the value of sector-specific guidelines but also reveal enforcement disparities, with urban institutions faring better than rural ones. Criminal responsibility of AI committing deepfake crimes in Indonesia further emphasizes the need for accountability, with widespread attention to financial fraud cases (Hailtik & Afifah, 2023).

International Influences and Comparative Insights

Indonesia's regulations draw heavily from international models, enhancing their sophistication. The EU's AI Act (2024), which classifies deepfakes as high-risk and mandates transparency, has influenced OJK's ethical codes and Kominfo's circulars (Rouse, 2025). Similarly, China's Deep Synthesis Provisions require labeling of AI content, inspiring proposals for watermarking in Indonesia (Akhmad & Rachman, 2025). Global bodies like the OECD advocate for harmonized standards, with Indonesia participating in ASEAN discussions on cyberfraud to address cross-border deepfakes (OECD.AI, 2024). Addressing deepfake pornography and the right to be forgotten offers additional legal challenges, drawing lessons for AI-driven sexual abuse prevention (Nasution et al., 2025). Comparatively, Indonesia lags behind leaders like Singapore, which has dedicated deepfake laws with severe penalties, but outperforms neighbors like the Philippines in AI governance adoption (CSIS, 2024). Scholars recommend adopting vicarious liability for platforms, holding them accountable for hosting deepfakes, as in the EU model (Dentons HPRP, 2024). International collaboration, such as sharing detection tools via the World Economic Forum, could bolster Indonesia's efforts (World Economic Forum, 2025). The legal landscape on national cybersecurity capacity in combating cyberterrorism using deepfake technology further emphasizes the need for robust frameworks (Purwadi et al., 2022). Table 2 summarize key initiatives:

Table 2: Summary of key initiatives

Initiative	Description	Enactment/Implementation	Source
OJK Code of Conduct for AI in Fintech	Ethical guidelines for AI transparency and risk management	Early 2024	OJK (2024)
OJK Regulation No. 27/2024	Oversight of digital assets, including fraud monitoring	2024	OJK (2024)

Kominfo AI Ethics Circular	Platform accountability for content moderation and detection	2024–2025	Kominfo (2024)
AI Governance Book for Banking	Standards for deepfake risk management in banks	April 2025	OJK (2025)
ITE Law Amendments	Broader misinformation penalties, applied to deepfakes	2008/2016	Huda & Rachman (2025)

These measures signal commitment but require refinement for efficacy.

Implications for Future Regulatory Evolution

The outlined challenges have indicated that despite the fact that the responses of Indonesia are a foundation, fundamental reforms are crucial. One of the proposals is the creation of a specific Deepfake Law that is properly defined, has forensics in place, and has a system of international cooperation (Kusumawardani and Rachman, 2025). A better development of tool development and education regarding literacy gaps can help close the gaps and reduce fraud by 30-40 percent depending on the global counterparts (VIDA, 2024a). With the development of AI, agile regulations, which are updated each year, will become an essential aspect to remain in the lead over threats. The regulation of AI as an offender of deepfake crimes also highlights the necessity of special legal frameworks to focus on the responsibilities (Hailitik and Afifah, 2023).

Essentially, the regulatory framework in Indonesia shows that there is adaptive improvement in case of deepfakes, but it still has inconsistencies in specificity, enforcement, and resources. These findings will be incorporated in the discussion section and part will be coupled with economic impacts to deem comprehensive solutions. The problem of cybercrime and liability underlines the use of artificial intelligence in committing crimes via the Internet, and it is necessary to develop a detailed legal answer (Rasyid et al., 2024).

DISCUSSION

The production of secondary data on the use of deepfakes to commit financial fraud in Indonesia indicates that it is a complex problem that entangles changes in technology, economic weaknesses, and regulatory issues. In this section, the results of the economic and regulatory analysis are combined to analyze the implications of deepfake fraud on the Indonesia financial ecosystem critically, with references to the global trends and suggestions on strategic interventions. This discussion has highlighted the urgency of dealing with deepfake threats using concerted technological, legal and educational actions by analyzing the interplay between economic losses, responses by regulators, and larger socio-technical dynamics. The gap in the existing schemes is also noted, the future risks are outlined, and the practical suggestions are given to increase the resilience of the Indonesian fast-digitizing economy.

Economic Implications and Systemic Risks.

Deepfake-induced financial fraud in Indonesia, with an estimated economic impact of more than \$138.5 million in a single case, would be a major liability to the financial industry of the country, specifically in fintech and banking (Group-IB, 2024). These losses, driven by a 1,550% surge in AI-driven fraud from 2022 to 2024, reflect the vulnerability

of Indonesia's digital infrastructure, where widespread mobile banking adoption (over 200 million users) and biometric reliance amplify exposure (AuthMe, 2025; World Economic Forum, 2025). Beyond direct monetary impacts, indirect costs such as reputational damage, increased compliance expenses, and eroded consumer trust threaten to undermine Indonesia's fintech growth, projected at 16.8% annually through 2025 (Oliver Wyman, 2024). The targeting of the unbanked population, approximately 66 million individuals, exacerbates financial exclusion, as victims of deepfake scams may distrust digital platforms, stalling inclusion efforts (VIDA, 2024b).

Globally, Indonesia's experience aligns with a broader escalation, where deepfake fraud losses reached \$410 million in the first half of 2025, with the Asia-Pacific region witnessing a 1,540% incident surge from 2022 to 2023 (Surfshark, 2025; VIDA, 2024a). This regional context highlights systemic risks, as deepfakes facilitate cross-border scams, including money laundering and market manipulation, with Southeast Asia's cyberfraud generating \$43.8 billion in illicit gains in 2023 (CSIS, 2024). For Indonesia, these trends suggest a potential for escalating losses if current vulnerabilities remain unaddressed, particularly as generative AI becomes more accessible. The psychological impact on victims, including identity harm and financial distress, further compounds economic consequences, necessitating a holistic approach to mitigation (OECD.AI, 2024).

Regulatory Strengths and Limitations

Indonesia's regulatory framework, spearheaded by the Financial Services Authority (OJK) and the Ministry of Communication and Digital Affairs (Kominfo), demonstrates proactive adaptation to deepfake threats. Initiatives like the OJK Code of Conduct for AI in Fintech (2024), Regulation No. 27/2024, and the AI Governance Book for Banking (2025) establish ethical guidelines, mandate biometric enhancements, and align with global standards like the Basel Committee's risk management principles (OJK, 2024, 2025). The Kominfo AI Ethics Circular (2024–2025) further promotes platform accountability and public awareness, reflecting international influences from the EU's AI Act and China's Deep Synthesis Provisions (Kominfo, 2024; Rouse, 2025). These measures have yielded tangible results, with 72% of fintech firms adopting OJK guidelines, leading to a 20–30% reduction in spoofing attempts (VIDA, 2024a).

However, significant limitations persist. The absence of a dedicated deepfake law within the Electronic Information and Transactions (ITE) Law framework creates enforcement ambiguities, as existing provisions on misinformation lack specificity for AI-generated fraud (Huda & Rachman, 2025; Rachman & Aditya, 2025). Low digital literacy, with only 42% of Indonesians able to discern fake content, hampers victim reporting and public compliance with regulatory mandates (Kusumawardani & Rachman, 2025). Resource constraints further limit smaller institutions' ability to implement advanced detection tools, creating disparities in enforcement effectiveness between urban and rural financial entities (Group-IB, 2024). The transnational nature of deepfake scams, often orchestrated from regional hubs, complicates jurisdiction and traceability, as seen in the 2025 Prabowo deepfake case, where overseas servers delayed full resolution (Safer Internet Lab, 2025). Comparative analysis with global peers reveals mixed positioning. Singapore's dedicated deepfake legislation offers a model for explicit sanctions, while Indonesia's reactive approach often post-incident lags behind (CSIS, 2024). However, Indonesia's adoption of AI governance frameworks surpasses that of neighbors like the Philippines, positioning it as a regional leader in policy innovation (Dentons HPRP, 2024). The challenge lies in balancing regulatory agility with technological advancement, as fraudsters exploit gaps faster than regulators can adapt (Aditya, 2023).

Socio-Technical Dynamics and Future Risks

The socio-technical nature of deepfake fraud underscores the interplay between human behavior and technological vulnerabilities. Indonesia's high internet penetration (77%) and reliance on biometric systems create a fertile ground for social engineering attacks, where deepfakes leverage trust in familiar voices or faces (World Economic Forum, 2025). Academic studies emphasize that low digital literacy amplifies susceptibility, particularly among rural and unbanked populations, who are prime targets for scams involving fake endorsements or impersonated officials (Kusumawardani & Rachman, 2025). The rapid evolution of generative AI, projected to triple deepfake incidents by 2027, poses a looming threat, as tools become cheaper and more sophisticated (VIDA, 2024a).

Future risks include not only increased financial losses but also broader societal impacts, such as disinformation campaigns that destabilize markets or undermine public trust in governance (Prabowo & Suryanto, 2023). The integration of deepfakes with other cyber threats, like ransomware or phishing, could amplify economic harm, potentially reaching billions in losses if unchecked (Oz Forensics, n.d.). For Indonesia, these risks threaten national security, as deepfakes targeting public figures could incite social unrest or manipulate financial markets (Safer Internet Lab, 2025).

Strategic Recommendations

To address these challenges, a multi-pronged strategy is essential, combining technological innovation, legal reform, and public education. The following recommendations draw from secondary data insights and global best practices:

1. ***Enact a Dedicated Deepfake Law:*** Indonesia should develop legislation explicitly defining deepfakes, outlining forensic standards for evidence, and imposing penalties for creation and dissemination of fraudulent synthetic media. This could mirror Singapore's model, incorporating vicarious liability for platforms hosting such content (Rouse, 2025; Dentons HPRP, 2024).
2. ***Enhance Inter-Agency Coordination:*** Establishing a national task force involving OJK, Kominfo, Bank Indonesia, and law enforcement would streamline enforcement, improve data sharing, and address jurisdictional overlaps. ASEAN-level collaboration could tackle cross-border scams, leveraging shared detection tools (CSIS, 2024; OECD.AI, 2024).
3. ***Invest in Detection Technologies:*** Financial institutions should adopt advanced AI-based detection systems, including liveness detection and behavioral biometrics, as mandated by OJK's 2025 guidelines. Public-private partnerships with tech firms could subsidize these tools for smaller fintechs, reducing compliance burdens (Group-IB, 2024; OJK, 2025).
4. ***Scale Public Education Campaigns:*** Nationwide campaigns, led by Kominfo, should educate consumers on identifying deepfakes, using accessible formats like mobile apps or social media. Global studies suggest that improved literacy could reduce victimization by 30–40% (VIDA, 2024a). Targeting rural areas and unbanked populations is critical to support financial inclusion.
5. ***Adopt Global Standards:*** Incorporating elements of the EU's AI Act, such as mandatory watermarking and transparency for AI-generated content, would enhance traceability and accountability. Indonesia's participation in OECD and ASEAN forums could facilitate access to free detection tools from global tech providers (Rouse, 2025; World Economic Forum, 2025).
6. ***Agile Policy Updates:*** Regulations should be revisited annually to keep pace with AI advancements, incorporating predictive analytics to anticipate fraud trends. OJK's risk-based audits could integrate real-time threat assessments to preempt attacks (Prabowo & Suryanto, 2023).

CONCLUSION

This study underscores the critical threat of deepfake-enabled financial fraud in Indonesia, revealing substantial economic losses driven by sophisticated AI-driven scams targeting the nation's burgeoning digital economy. Among the most notable results, it is evident that deepfake fraud, specifically biometric spoofing and impersonation has caused considerable financial loss, which harmed the fintech sector badly and aided in losing trust among millions of users, including the 66 million unbanked population. Some of the risks have been mitigated by regulatory means, including ethical AI standards and improved biometrics, with significant progress in the reduction of fraud attempts. Nevertheless, there are still certain weaknesses, such as underreported cases since corporate confidentiality can be effective, secondary data usage that might not reflect the most recent technological innovations, and no study that is specific to Indonesia, which limits the overall understanding. Lack of specific deepfake laws and poor digital literacy only make the task of enforcement more difficult. Future studies need to focus on primary data gathering by conducting surveys on victims and interviewing regulators to reveal hidden effects and longitudinal research to examine novel policies and explore new vectors of fraud such as AI-driven cryptocurrency fraud. The consequences are extensive: in the absence of strong measures, growing losses may jeopardize the development of fintech, increase financial exclusion, and threaten the national security. To overcome these obstacles, Indonesia needs to implement specific deep-fake laws, enhance inter-agency cooperation, introduce the use of state-of-the-art detection tools, and introduce mass education efforts to enhance digital literacy, which will result in a robust and integrative financial ecosystem.

References

1. Aditya, P. (2023). Indonesia readiness to face social engineering attacks with deepfake technology. *Journal of Law and Sustainable Development*, 11(12), e727. Agarwal, J. D., Agarwal, M., Agarwal, A., & Agarwal, S. (2021). *Economics of cryptocurrencies: Artificial intelligence, blockchain, and digital currency*. World Scientific.
2. Akhmad, B., & Rachman, S. (2025). Implementation of ethical artificial intelligence law to prevent the use of AI in spreading false information (deepfake) in Indonesia. *Eastasouth Journal of Law and Human Rights*, 2(2), 120–130.
3. AuthMe. (2025). Deepfake fraud surges in Indonesia: Biometric technology as a shield. <https://authme.com/blog/deepfake-indonesia-fraud-fintech/>
4. Bank Indonesia. (2024). National strategy for digital payments security. <https://www.bi.go.id/en/publikasi/ruang-media/news-release/Pages/National-Strategy-for-Digital-Payments-Security.aspx>
5. Cantin, J. S. (2025). The hybrid harm-centric model: Realigning online harm regimes to reflect the visceral realities of victimisation. *ResearchSpace@Auckland*.
6. Center for Strategic and International Studies. (2024, December 12). Cyber scamming goes global: Unveiling Southeast Asia's high-tech fraud factories. <https://www.csis.org/analysis/cyber-scamming-goes-global-unveiling-southeast-asias-high-tech-fraud-factories>
7. Davey, O. M., & Sauerwein, L. (2023). Deepfake in online fraud cases: The haze of artificial intelligence's accountability based on the international law. *Sriwijaya Crimen and Legal Studies*.
8. Dentons HPRP. (2024, May 15). Regulating deepfake content: Protections and gaps under existing regulations. <https://dentons.hprplawyers.com/en/insights/articles/2024/may/15/regulating-deepfake-content-protections-and-gaps-under-existing-regulations>

9. Doing, M., Fitriani, Y., Alkadrie, S. M. R. R. M., & Others. (2025). Legal challenges in combating deepfake abuse: A comparative study of AI regulation in privacy protection and digital security. Proceeding.
10. Du, Y., Li, Z., Li, N., & Ding, B. (2025). Beyond data privacy: New privacy risks for large language models. arXiv preprint arXiv:2509.14278.
11. Goodyear, M. (2025). Dignity and deepfakes. Arizona State Law Journal.
12. Group-IB. (2024). Deepfake fraud threats to financial institutions. ASEAN Technology & Security Magazine. <https://aseantechsec.com/deepfake-fraud-threats-to-financial-institutions/>
13. Group-IB. (2024, December 4). Deepfake fraud. <https://www.group-ib.com/blog/deepfake-fraud/>
14. Gunawan, I. J., & Janisriwati, S. (2023). Legal analysis on the use of deepfake technology: Threats to Indonesian banking institutions. Law and Justice.
15. Hailtik, A. G. E., & Afifah, W. (2023). Criminal responsibility of artificial intelligence committing deepfake crimes in Indonesia. Asian Journal of Social and Humanities. <https://ajosh.org>
16. Huda, N., & Rachman, D. (2025). Interpretation of ITE Law in deepfake cases. Indonesian Legal Review.
17. Hussin, M. H., & Ginano, M. H. S. P. (2023). European Union cyber security in dealing with the threat of AI-cybercrimes: Lessons for Indonesia. Dinamika Global: Jurnal Ilmu Hubungan Internasional.
18. Intimedia. (n.d.). Deepfake is a serious threat in Indonesia: A collective strategy to counter it. <https://intimedia.id/read/deepfake-is-a-serious-threat-in-indonesia-a-collective-strategy-to-counter-it>
19. Kismawadi, E. R. (2025). The impact of deepfakes on trust and security in Islamic banking: Emerging threats and mitigation strategies. Deepfakes and Their Impact on Business.
20. Kominfo. (2024). Circular on AI ethics. <https://kominfo.go.id>
21. Kulkarni, M. D., & Angurala, M. P. (2024). Trends in computer science and information technology research. International Journal of Human Capital Management.
22. Kumar, P., Kaur, A., Pillay, S., & Rana, S. (2025). The face of deception: Unmasking deepfake fraud in financial markets. Mastering Deepfake Technologies.
23. Kumar, V. (2023). The economic value of digital disruption. Management Professional. Springer.
24. Kusumawardani, R., & Rachman, D. (2025). Digital literacy and deepfake detection in Indonesia. Journal of Cybersecurity Studies.
25. Lee, P. (2025). Techno-optimism in innovation law and policy. SSRN.
26. Lestari, W. T., Ramadani, R. F., Negara, Y. D., & Others. (2025). Enhancing digital security via e-law optimization and deepfake regulation: A comparative study of China. Jurnal: Journal of Law and Social Sciences.
27. Lin, L. S. F. (2025). Cryptocurrencies and AI-enabled organised fraud: Emerging risks and countermeasures. Journal on Risk and Financial Management: Big Data Analytics.
28. MEA Integrity. (2025, June 9). How deepfakes are undermining biometric identity checks in 2025. <https://www.mea-integrity.com/how-deepfakes-are-undermining-biometric-identity-checks-in-2025/>
29. Mishra, S., & Fiske, J. (2025). Break glass: Structural safeguards for social media. Harvard DASH. h
30. Napitupulu, J. H., Panggabean, M. L., & Others. (2025). An integrated legal framework for digital investment fraud prevention in Indonesia. Journal of Contrarius Actus.

31. Nasution, A. V. A., Suteki, & Lumbanraja, A. D. (2025). Addressing deepfake pornography and the right to be forgotten in Indonesia: Legal challenges in the era of AI-driven sexual abuse. *International Journal for the Semiotics of Law*.
32. Noval, S. M. R. (2023). Indonesia readiness to face social engineering attacks with deepfake technology. *Journal of Law and Sustainable Development*.
33. OECD.AI. (2024). AI-generated deepfakes cause financial and identity harm in Indonesia. <https://oecd.ai/en/incidents/2024-04-23-f5ff>
34. OJK. (2024). Code of conduct for responsible AI in fintech. Financial Services Authority Indonesia. <https://www.ojk.go.id/id/kanal/perbankan/Pages/Code-of-Conduct-AI-Fintech.aspx>
35. OJK. (2025). AI Governance Book for Indonesian Banking. Financial Services Authority Indonesia. <https://www.ojk.go.id/id/kanal/perbankan/Pages/AI-Governance-Book-2025.aspx>
36. Oliver Wyman. (2024, October). Decoding the potential of AI-driven growth in Indonesia. <https://www.oliverwyman.com/our-expertise/insights/2024/oct/unlocking-potential-of-ai-driven-growth-in-indonesia.html>
37. Oz Forensics. (n.d.). The deepfake surge: Why liveness detection is the answer. <https://www.ozforensics.com/blog/articles/the-deepfake-surge-why-liveness-detection-is-the-answer>
38. Pamungkas, A. A., Sutarni, N., & Others. (2025). Legal analysis of deepfake technology in Indonesia from the perspective of fair and civilized humanity. *Pena Justisia: Media Komunikasi Fakultas Hukum*.
39. Prabowo, A., & Suryanto, Y. (2023). Legal analysis on the use of deepfake technology: Threats to financial institutions in Indonesia. *Legal Analysis Journal*, 5(2), 112–125.
40. Purwadi, A., Serfiyani, C. Y., & Others. (2022). Legal landscape on national cybersecurity capacity in combating cyberterrorism using deep fake technology in Indonesia. *International Journal of Cyber Criminology*.
41. Rachman, S., & Aditya, P. (2025). Crimes involving deepfake in online fraud and the challenges of proving them. *Journal of Criminal Law*, 15(4), 200–215.
42. Rama, A., Lofandri, W., & Saputra, A. F. (2025). Legal gaps in Indonesia's electronic information and transactions law in addressing deepfake technology: Challenges and regulatory recommendations. *Indonesian Journal of School Counseling*.
43. Rasyid, M. F. F., SJ, M. A., Mamu, K. Z., & Paminto, S. R. (2024). Cybercrime threats and responsibilities: The utilization of artificial intelligence in online crime. *Jurnal Ilmiah Mizani Hukum*.
44. Rouse. (2025, June 13). Navigating the deepfake dilemma: Legal challenges and global responses. <https://rouse.com/insights/news/2025/navigating-the-deepfake-dilemma-legal-challenges-and-global-responses>
45. Safer Internet Lab. (2025). Online fraud and scams in Indonesia. <https://saferinternetlab.org/wp-content/uploads/2025/05/Online-Fraud-and-Scams-in-Indonesia.pdf>
46. Sembiring, J., & Firdaus, S. U. (2025). Criminal liability for misuse of artificial intelligence (AI) in deepfake crimes. *International Journal of Multi-Disciplinary*.
47. Surfshark. (2025, July 8). Deepfake fraud caused financial losses nearing \$900 million. <https://surfshark.com/research/chart/deepfake-fraud-losses>
48. T20 Indonesia. (2022). Deepfakes and security in the information environment: Challenges for governments, society, and business. https://www.t20indonesia.org/wp-content/uploads/2022/11/TF2_Deepfakes-and-Security-in-the-Information-Environment_Challenges-for-Governments-Society-and-Business-1.pdf

49. VIDA. (2024a, August 26). Four emerging AI-generated fraud in Indonesia. <https://vida.id/en/blog/four-emerging-ai-generated-fraud-in-indonesia>
50. VIDA. (n.d.). 100% of businesses in Indonesia worry about AI-generated fraud. <https://vida.id/pressrelease/100-bisnis-di-indonesia-khawatir-penipuan-berbasis-ai>
51. World Economic Forum. (2025, February 17). The rise of AI in Indonesia is expanding financial inclusion. <https://www.weforum.org/stories/2025/02/rise-of-ai-in-indonesia/>
52. Yuspin, W., Afnan, H. A., Wardiono, K., Budiono, A., & Others. (2025). Deep fakes in P2PL services: Assessing legal challenges and data privacy risks. WSEAS Transactions on Computer Research.