Research Inventy: International Journal of Engineering And Science
Vol.15, Issue 6 (June 2025), PP 14-18
Issn (e): 2278-4721, Issn (p):2319-6483, www.researchinventy.com

Deepfake Identity Risks and Its Financial Impact in Vietnam's Digital Era

Thi-Khanh-My Nguyen[1], Thi-Thanh-Thao Vo[2]
[1,2] Faculty of Digital Economics and E-commerce, The University of Danang, Vietnam-Korea University of Information and Communication Technology, Danang, Vietnam

Abstract: *In Vietnam's fast-growing Fintech world, digital identity systems have become the backbone of secure online financial services. But with the rise of deepfake technology - AI-generated fake videos and voices—these systems are facing new and serious challenges. Deepfakes can trick even advanced security checks, leading to identity theft and financial fraud that can cost people and businesses dearly. While Vietnam has made great strides in building digital ID infrastructure and laws, there are still gaps in technology, legal protection, and public awareness that criminals can exploit. This paper looks closely at how digital identity works in Vietnam's Fintech sector, explores real cases of deepfake fraud, and discusses why current systems aren't enough to stop these threats. It also offers practical ideas for how the government, Fintech companies, and everyday users can work together - through better laws, smarter technology like multi-factor authentication and deepfake detection, and stronger digital education - to protect people and build trust in the digital economy. Only by joining forces can Vietnam create a safer, more reliable digital identity system that supports the country's ongoing digital transformation.*

Keywords: *Deepfake, Risks, Digital Identity, Financial Technology, Fintech, Vietnam.*

Date of Submission: 06-06-2025 Date of acceptance: 16-06-2025

I. INTRODUCTION

Over the past decade, the rapid advancement of financial technology as known as Fintech, has driven a profound digital transformation across the global financial and banking sectors. In the rapidly evolving fintech landscape of the Asia-Pacific region, Vietnam stands out as a dynamic center of innovation and expansion. The country is emerging as the second-largest fintech market in ASEAN, with its sector projected to reach an impressive US$18 billion by 2024 (Innolab Asia, 2024). This growth reflects ongoing advancements that are transforming financial services and contributing to sustainable economic development. According to United Overseas Bank (2022), the number of fintech companies in Vietnam has surged from just 39 in 2015 to over 200 by 2022, highlighting the sector's remarkable pace of growth and transformation.

Accompanying the expansion of Fintech services, digital identity has emerged as a critical enabler, serving as the foundational gateway for secure and seamless digital transactions. Digital identity refers to the process of collecting, verifying, and managing personal information in digital form to facilitate online transactions. A comprehensive digital identity may include personal details (such as full name, national ID number, and date of birth), biometric data (including facial recognition, fingerprints, and voice), device metadata, behavioral patterns, and historical interaction records across digital platforms. Fintech platforms that utilize digital identification systems have significantly broadened access to financial services for previously unbanked populations. In the last decade, 1.2 billion adults have gained access to financial services, with fintech serving as a major driver of this advancement (Sharmista Appaya, 2021). However, despite its operational efficiency and user convenience, the security and integrity of digital identification systems have not evolved at the same pace as technological innovation. In particular, the emergence of sophisticated AI-driven threats - most notably deepfake technologies, which enable the creation of highly realistic but fraudulent images, voices, or videos - poses growing risks to identity verification mechanisms and the broader Fintech ecosystem.

The emergence of deepfake technology - AI-generated images, voices, or videos that closely mimic real individuals - is increasingly threatening the integrity of digital identity systems. Unlike traditional fraud methods involving forged documents or manual impersonation, deepfakes can deceive automated eKYC systems and even bypass biometric authentication mechanisms, such as facial or voice recognition. A striking example occurred in Hong Kong in early 2024, where cybercriminals used a deepfake video impersonating the CFO of a major corporation to orchestrate a fraudulent transfer of over 25 million USD (Grace Noto, 2024). This case highlights the alarming potential of AI as a tool for financial exploitation, exposing significant vulnerabilities in current identity verification processes, particularly the lack of robust safeguards against synthetic media. In Vietnam, similar incidents have begun to surface. The introduction of mandatory biometric authentication for online transactions, mandated by Decision No. 2345/QĐ-NHNN and effective from July 1, 2024, was designed to strengthen digital banking security. However, fraudsters have taken advantage of the transitional phase. Posing as bank employees, scammers contact customers under the guise of assisting with biometric updates. They request sensitive information such as personal data, ID card images, and facial photos, and may even conduct video calls to capture voices and gestures. This collected data is then used to fabricate fake biometric profiles, granting criminals unauthorized access to victims' bank accounts (Techcombank, 2024). According to the Center for National Cybersecurity Monitoring under the Ministry of Information and Communications, Vietnamese internet users filed nearly 10,000 reports of online fraud in the first half of 2024. These incidents frequently involved impersonation schemes, with scammers posing as government representatives, service providers, or familiar contacts to trick their victims. Increasingly, fraudsters are leveraging AI-generated contente - such as altered images, synthetic voices, and deepfake vídeos - to make their deception more convincing and difficult to detect (Huy Anh, 2024) These developments underscore an urgent need for regulatory, technological, and institutional responses to address the growing risks associated with deepfake-driven identity fraud in the Fintech sector.

Although there have been many studies about the growth of Fintech and how digital technology is changing our lives, research that looks closely at the weaknesses in digital identity systems - especially the risks from deepfakes and fake identities - is still very limited, particularly in Vietnam. Right now, rules and policies about digital identity are not keeping up with the fast development of smart fake technologies. At the same time, many Fintech companies, especially startups and non-bank platforms, do not have strong tools or systems to detect deepfakes. Most users also do not have enough knowledge or skills to spot the risks of identity theft or understand how their personal data might be misused. On top of that, the legal system still has many gaps, making it hard to properly handle or punish digital identity crimes. This article aims to give a clear and up-to-date view of the digital identity crisis in the Fintech world, with a focus on Vietnam. It will (1) Explain how digital identity is used in Fintech today; (2) Explore new kinds of identity fraud, especially deepfakes, and show where the current systems are weak; (3) Look at real cases to understand the financial and social impact; (4) Suggest practical solutions - both technical and legal - that could help Vietnam protect digital identity better.

II. CURRENT STATUS OF DIGITAL IDENTITY IN VIETNAM’S FINTECH SECTOR

1. Overview of digital identification process in Vietnam

In the context of the strong digital transformation taking place in Vietnam, Digital Identity plays a core role in ensuring safety, authenticating users and building a trusted foundation for activities in the digital environment. This is not only a prerequisite for the development of e-Government, but also the foundation for the operation of the digital economy and the digital financial ecosystem (Fintech), where all financial transactions - from payment, account opening to borrowing - need to verify user identity quickly, accurately and securely. Since 2020, Vietnam has promoted the implementation of a comprehensive digital identity system through three main pillars such as national identification technology, state-level digital applications and related legal framework.

In 2021, the Ministry of Public Security launched the project for producing, issuing, and managing chip-based Citizen Identity Cards (ID cards). These chip-based ID cards not only store basic personal information but also integrate biometric and digital identification data, significantly enhancing the reliability of user identity verification. By the end of 2023, over 80 million chip-based ID cards had been issued to Vietnamese citizens - covering nearly 90% of the population aged 14 and older (Ngoc An, 2023). These cards are integrated for use across various services, including banking, insurance, healthcare, transportation, education, and e-commerce.

The VNeID application, developed by the Ministry of Public Security, is considered the national digital identity platform. It enables citizens to verify their digital identity at Level 1 and Level 2 (either through online registration or in-person at a police office). It also allows users to log in with their ID cards to access and use public services such as administrative procedures, residence declarations, tax filings, and registration for insurance, banking, and healthcare services. The Ministry of Public Security has issued over 86 million chip-embedded citizen ID cards and received over 75.16 million electronic identification records, activating over 53.88 million accounts (the activation rate over the total number of records received reached 71.68%) via VneID application (Vuong Tran, 2024).

Moreover, several key legal policies between 2020 and 2024 have laid the legal foundation for the digital identity process. These include:

- Amended Law on Electronic Transactions (2023) which clearly defines the use of digital identity in administrative, financial, and commercial transactions, and extends its application to both individuals and organizations.

- Draft Law on Digital Identification and Authentication (2024) which was developed by the Ministry of Public Security, this law outlines the types of digital identity, levels of authentication, issuance authority, and responsibilities of involved parties.
- Decree No. 59/2022/NĐ-CP which Governs personal digital identification and authentication, applicable across all administrative activities and online public services.

These policies are progressively legalizing the concept of a "digital citizen" while also reinforcing the obligations of financial institutions, banks, and fintech companies in verifying and protecting user identities.

2. Current Status of Applying Digital Identity in Vietnam's Fintech Sector

In recent years, eKYC (Electronic Know Your Customer) has emerged as a core technology in the operations of financial institutions and Fintech companies in Vietnam. Unlike traditional KYC procedures that require customers to visit physical branches, eKYC enables users to open bank accounts, register e-wallets, and apply for loans entirely online using just a mobile device with internet access. This digital shift not only reduces time and operational costs but also expands access to financial services in remote and underserved areas where barriers to formal finance remain significant. The eKYC process incorporates several advanced technologies to ensure accuracy and security. OCR (Optical Character Recognition) automatically extracts data from images of citizen ID cards (CCCD) or passports, while facial recognition matches a user's selfie to their ID photo to verify identity. Liveness detection further strengthens authentication by confirming real-time facial movements to prevent fraud using static images or deepfakes. Additionally, AI and machine learning technologies analyze user behavior to detect anomalies that could indicate impersonation or fraudulent activity. Leading players in Vietnam's Fintech and banking sectors—such as MoMo, ZaloPay, VNPay, Cake by VPBank, Timo, TPBank, VPBank, MB, and Techcombank—have actively invested in and integrated eKYC into their digital onboarding processes. Currently, many banks in Vietnam have deployed eKYC such as HDBank, Tienphong Bank, MB, BIDV, Vietinbank, VPBank, ACB, etc. at varying levels of sophistication. eKYC has played a vital role in accelerating financial inclusion, particularly during the COVID-19 pandemic, which highlighted the urgent need for remote and contactless services. However, the swift adoption of eKYC also brings increased concerns regarding data privacy and the rising risks of identity fraud.

In 2023, Vietnam witnessed a significant rise in fraud involving deepfake technology used to impersonate individuals in financial transactions. Deepfakes can facilitate sophisticated scams - such as fake identity verification, voice phishing, and synthetic identity fraud. Criminals can mimic clients or bank officials to bypass security systems or deceive users into transferring money. In June 2023, multiple users had their e-wallet accounts compromised through deepfake video calls impersonating bank employees. In September 2023, over 200 bank accounts in Ho Chi Minh City were opened using fake citizen ID cards and used to receive funds from international scam call centers. Other cases in Hanoi and Can Tho involved students using stolen personal information to open Fintech accounts and resell them (Ministry of Science and Technology, 2024). Cybercriminals exploited artificial intelligence to create fake videos and audio recordings, tricking victims into believing they were communicating with relatives or authorities. These deepfake video calls were often used to request money transfers or extract sensitive personal information. According to a report by the Information Security Department under the Ministry of Information and Communications, such fraud tactics are becoming increasingly sophisticated and difficult to detect, especially as deepfake technology becomes more accessible (Union Générale des Vietnamiens de France, 2024)

Many current eKYC systems still lack advanced authentication layers such as multi-factor authentication (MFA) and liveness detection to ensure that users are real. This vulnerability makes it easier for cybercriminals to bypass security using deepfake or spoofing tools. Smaller Fintech platforms and startups often lack the resources to invest in advanced anti-fraud AI technologies, making them more susceptible to attacks. Additionally, the absence of a unified digital identity standard among financial institutions leads to fragmentation and poor data interoperability, weakening the overall effectiveness of fraud detection and prevention (Ministry of Science and Technology, 2024).

A major challenge in safeguarding the digital identity system lies in the limited awareness and digital literacy of users regarding personal information security. Many individuals unknowingly share citizen ID numbers and portrait photos through fake apps or phishing links without recognizing the risks. A lack of familiarity with fraud schemes—such as phishing, fake banking chatbots, or counterfeit Fintech websites—leaves users vulnerable. The most at-risk groups include the elderly, students, and people in rural areas, where knowledge of digital safety remains limited.

Although the Law on Electronic Transactions has been amended, regulations concerning the handling of impersonation and digital account hijacking remain vague. There is also no standardized technical supervision framework for Fintech companies regarding identity security, increasing exposure to cyber threats. The limited data-sharing mechanisms between state agencies and private enterprises further hinder efforts to cross-verify and detect fraudulent activity. The Draft Law on Identification and Electronic Authentication, proposed by the Ministry of Public Security in 2024, aims to address these gaps, but it is still under development and not yet widely implemented. These incidents highlight the urgent need to raise public awareness and strengthen the legal framework to protect users in the digital environment.

III. DISCUSSIONS AND CONCLUSIONS

3.1. Discussion

Vietnam has made many achievements in deploying digital identification, especially in the field of Fintech. However, potential risks from deepfake technology, technical vulnerabilities and low user awareness are becoming serious challenges. To effectively address the growing risks from deepfake technology, technical vulnerabilities, and low user awareness in digital identification, a coordinated approach involving the Government, Fintech enterprises, and users is essential.

A robust legal framework is foundational to securing digital identification. Vietnam needs clear, comprehensive laws that specifically address identity verification, data protection, and cybercrime related to digital identities. For example, the upcoming Digital Identification and Electronic Authentication Law should clearly define what constitutes identity fraud, the responsibilities of Fintech companies, and the rights of consumers. Mandatory security standards and regular technical audits should be required for all Fintech providers to ensure compliance with best practices in identity verification and fraud prevention. Additionally, the government should improve the mechanisms for data sharing between different state agencies and financial institutions to enable reliable cross-checking of user identities, while respecting privacy regulations. By closing legal loopholes and ensuring clear penalties for violations, this framework will create a safer environment and deter fraudsters.

Promoting advanced technical solutions is crucial in combating identity fraud within the Fintech sector, as technology can be both a vulnerability and a defense. Fintech companies need to implement cutting-edge tools such as multi-factor authentication (MFA), which requires multiple forms of verification like passwords, fingerprints, or SMS codes to strengthen security. Real-time deepfake detection leveraging AI algorithms can analyze facial movements, voice patterns, and biometric signals to identify manipulated videos or audio during onboarding or transactions. Additionally, liveness detection techniques, which verify live user responses such as blinking or head movements, help prevent fraudsters from using static images or videos. Behavioral analytics powered by machine learning can monitor user behavior patterns—such as typing speed or location—to detect anomalies and flag suspicious activities early. However, many startups and smaller Fintech firms face financial and technical challenges in adopting these advanced technologies, so government incentives, subsidies, and partnerships are essential to democratize access and ensure high security standards across the entire industry.

Users are often the weakest link in digital security, frequently falling victim to phishing scams, unknowingly sharing sensitive information, or failing to recognize fraudulent platforms. Therefore, a broad-based digital literacy campaign is essential to educate the public on how to identify phishing emails, fake websites, and scam calls, as well as the importance of protecting personal data such as ID cards and biometric information. The campaign should also guide users on the necessary steps to take if they suspect their identity has been compromised. To be effective, this effort must leverage multiple communication channels—including social media, television, community outreach programs, and schools—and focus especially on vulnerable groups like the elderly, rural residents, and students. Additionally, Fintech applications themselves can play a role by integrating educational content and real-time alerts to help users make safer decisions on a daily basis.

Digital identity security requires a collective effort involving regular coordination forums and working groups that bring together government agencies, Fintech companies, cybersecurity experts, and consumer organizations. These platforms enable the sharing of threat intelligence and early warnings about emerging fraud techniques, allowing stakeholders to stay ahead of new risks. They also provide a space to develop industry-wide standards and best practices that promote consistent and effective security measures across the sector. Furthermore, such collaboration ensures a coordinated response to major incidents or system vulnerabilities, improving the speed and effectiveness of mitigation efforts. This cooperative approach fosters greater trust among participants and enhances the overall agility in combating fast-evolving threats like advanced deepfake technologies and increasingly sophisticated phishing campaigns.

Despite all precautions, identity fraud incidents will still occur. Creating clear, accessible channels for users to report suspected fraud quickly is essential to limit damage. This includes hotlines, online portals, and mobile app reporting features. Further, the government and industry should set up efficient processes for investigating these reports, providing victims with legal assistance, identity restoration services, and fraud remediation support. Quick and effective response builds consumer confidence and mitigates financial and reputational losses.

Implementing these solutions holistically will strengthen the trust and resilience of Vietnam’s digital identification system within the Fintech ecosystem, contributing to safer financial services and sustainable digital transformation.

3.2. Conclusion

In the context of strong digital transformation and the rapid development of the Fintech industry in Vietnam, the digital identification system plays a key role in ensuring security, authenticating users, and building trust in digital financial transactions. However, the emergence of deepfake technology and new forms of fraud have posed serious challenges to the integrity of the digital identification system, increasing the risks of information insecurity and financial losses.

Although Vietnam has made significant progress in building technical infrastructure and improving the legal framework related to digital identification, technical loopholes, limited user awareness, and the lack of synchronization in applying modern security measures remain weaknesses that are easily exploited. To effectively respond to these risks, close coordination is needed between the State, Fintech businesses, and users through perfecting legal policies, promoting the application of advanced technological solutions such as multi-factor authentication and real-time deepfake detection, along with raising awareness and digital literacy within the community.

Only through the cooperation of multiple parties can the digital identification system in Vietnam become safe and reliable, contributing to the sustainable development of both the Fintech industry and the digital economy in the future.

REFERENCES

[1]. Innolab.asia (2024). Unlocking The Rise of Fintech in Vietnam – The Promising 18 Billion USD Market by 2024. Available at: https://innolab.asia/2024/04/05/unlocking-the-rise-of-fintech-in-vietnam-2024/

[2]. United Overseas Bank. (2022). FinTech in ASEAN 2022: Finance, reimagined report | UOB. Available at: https://www.uobgroup.com/techecosystem/news-insights-fintech-in-asean-2022.html.

[3]. Ministry of Science and Technology (2024). Warning of increasing fraud using Deepfake technology. Available at: https://mic.gov.vn/canh-bao-gia-tang-lua-dao-bang-cong-nghe-deepfake-197240719153600292.htm

[4]. Union Générale des Vietnamiens de France (2024). Deepfake và những nguy cơ với an toàn thông tin tại Việt Nam. Available at: https://www.ugvf.org/vi/deepfake-va-nhung-nguy-co-voi-an-toan-thong-tin-tai-viet-nam/

[5]. Sharmista Appaya (2021). On fintech and financial inclusion. Available at: https://blogs.worldbank.org/en/psd/fintech-and-financial-inclusion

[6]. Grace Noto (2024). Scammers siphon $25M from engineering firm Arup via AI deepfake 'CFO'. Available at: https://www.cfodive.com/news/scammers-siphon-25m-engineering-firm-arup-deepfake-cfo-ai/716501/

[7]. Techcombank (2024). Warning of biometric update exploit scam. Available at: https://techcombank.com/en/information/updates/warning-of-biometric-update-exploit-scam

[8]. Huy Anh (2024). Rising threat: How online scams harm vulnerable Vietnamese. Available at: https://hanoitimes.vn/rising-threat-how-online-scams-harm-vulnerable-vietnamese-328313.html

[9]. Ngoc An (2023) Nearly 80 million citizen identification cards have been issued. Available at: https://tuoitre.vn/da-cap-gan-80-trieu-the-can-cuoc-cong-dan-20230426212807922.htm

[10]. Vuong Tran (2024). The Ministry of Public Security has activated over 53.88 million electronic identification accounts. Available at: https://laodong.vn/thoi-su/bo-cong-an-da-kich-hoat-tren-5388-trieu-tai-khoan-dinh-danh-dien-tu-1351074.ldo