International Journal of Social Science and Human Research

ISSN (print): 2644-0679, ISSN (online): 2644-0695

Volume 08 Issue 05 May 2025

DOI: 10.47191/ijsshr/v8-i5-77, Impact factor- 8.007

Page No: 3503-3514

Banking Crime in The Digital Age: Tackling Emerging Challenges

Manotar Tampubolon

Fakulti Undang-Undang, Universiti Teknologi MARA. Malaysia

ABSTRACT: The rapid advancement of technology has significantly changed the banking industry, allowing for quicker transactions, improved customer experiences, and worldwide connectivity. However, this technological progress has also opened the door to complex banking crimes, including cyberattacks, data breaches, and identity theft. This research examines the intricate challenges that come with integrating technology in banking, focusing on how financial institutions manage the delicate balance between innovation and security. Using a multidisciplinary approach, the study incorporates case studies, regulatory frameworks, and technological safeguards to identify vulnerabilities in digital banking systems. It also evaluates the effectiveness of current legal and institutional measures in tackling emerging threats. The findings indicate that while technology-driven solutions can provide potential defenses, shortcomings in cross-border collaboration and adaptive regulation impede effective crime prevention. Recommendations stress the importance of unified global policies, advanced threat detection systems, and ongoing staff training to address these evolving challenges.

KEYWORDS: Banking crime, technology, cybersecurity, regulation

I. INTRODUCTION

The rapid advancement of technology has dramatically changed the financial landscape, providing unmatched conveniences and efficiencies in banking operations. Digital banking platforms, online transactions, and mobile payment apps have transformed how individuals and institutions engage with financial systems. However, these advancements have also led to a rise in complex crimes targeting financial institutions and their customers. Banking crime in the technological age presents a multifaceted challenge that requires a thorough understanding of the relationship between technological innovation, criminal activity, and regulatory frameworks. This introduction seeks to delve into the complexities of this issue, highlighting its implications for contemporary society.

At the heart of banking crime in this digital era is the growing dependence on online platforms, which has unintentionally created vulnerabilities within financial systems. Cybercriminals take advantage of these weaknesses through sophisticated tactics like phishing attacks, ransomware, and identity theft. For example, a report from the Financial Action Task Force (FATF) points out that cybercriminals are increasingly using advanced technologies to commit fraud and launder money across borders (FATF, 2023). Likewise, Statista reports that over 65% of financial cybercrimes documented involve ransomware attacks within digital banking systems (Petrosyan, 2024). These crimes often cross- national borders, making it more challenging to identify and prosecute the offenders.

The anonymity provided by technology has allowed criminals to operate with increased sophistication and precision. The use of cryptocurrency in illegal activities, such as money laundering and fraud, illustrates this trend. Research from the United Nations Office on Drugs and Crime (UNODC) estimates that around $2.22 trillion and $5.54 trillion, about 2% to 5% of global GDP of the global GDP is laundered each year through digital means, including cryptocurrency platforms (United Nations Office on Drugs and Crime, 2024). As technology evolves, the tactics used by criminals become more elusive, creating significant challenges for law enforcement agencies and financial institutions.

In response to these challenges, governments and regulatory bodies around the world have stepped up efforts to bolster cybersecurity measures and improve regulatory frameworks. Initiatives like the European Union's General Data Protection Regulation (GDPR) and the United States' Cybersecurity Information Sharing Act (CISA) highlight the increasing focus on safeguarding sensitive financial data from cyber threats (Interface, 2024). However, despite these efforts, the fast-paced nature of technology often outstrips regulatory progress, leaving financial systems continuously exposed to new threats. The Reserve Bank of India reported a 27% rise in banking fraud cases during the first half of the financial year 2024-2025, increasing from 14,480 cases in the same period last year (The Economic Times, 2025). This highlights the urgent need for adaptable regulatory approaches.

The societal implications of banking crime in today's technological era go far beyond just financial losses. These crimes can significantly damage public trust in financial institutions and destabilize economies. According to a study by the World Bank, countries with high levels of banking crime often see a decline in foreign investments and slower economic growth (World Bank, 2024). Additionally, the psychological toll on victims, such as increased stress and a loss of security, is significant. As our society becomes more interconnected, tackling the root causes of banking crime requires a collaborative effort from various stakeholders, including those in technology, law enforcement, and academia.

The technological age has undoubtedly transformed the banking sector, presenting both opportunities and challenges. While advancements have improved efficiency and accessibility, they have also created new vulnerabilities that criminals can exploit. This complex nature of technological progress highlights the importance of a comprehensive strategy to combat banking crime. By encouraging innovation, reinforcing regulatory frameworks, and fostering international cooperation, we can better navigate the challenges of banking crime in this evolving landscape and protect the resilience of our financial systems.

II. LITERATURE REVIEW

In recent years, the growing dependence on technology has dramatically changed the banking industry, bringing both innovative solutions and unique challenges. Researchers have thoroughly examined the evolution of banking practices, pointing out how digitalization has improved operations, enhanced customer experiences, and expanded access to financial services (Cyber Management Alliance, 2024). However, this technological shift has also introduced new vulnerabilities, especially concerning banking crime. Despite significant research into banking crime and cybersecurity, there are still gaps in our understanding of the complex and evolving nature of these threats. This literature review delves into the current knowledge on banking crime in the technological era, emphasizing areas that need further exploration.

Cybercrime aimed at the banking sector has become a widespread concern, with financial institutions increasingly targeted by advanced attacks like phishing, ransomware, and Distributed Denial-of-Service (DDoS) assaults (Asmar & Tuqan, 2024). Research conducted by Lallie et al., highlights the rising financial and reputational damages caused by cyberattacks on banks (World Economic Forum, 2024). Furthermore, the rise of cryptocurrencies has brought about new types of financial crime, such as money laundering and fraud, which are made easier by the anonymity provided by blockchain technology (Saha et al., 2024). While some studies have looked into the technical aspects of these crimes, there has been insufficient focus on their socio-economic effects and the regulatory measures needed to address them.

A critical aspect of banking crime involves insider threats, where employees misuse their access to defraud institutions or customers (Yaseen, 2024). Although insider fraud has been around for a long time, the digitalization of banking has significantly increased the scale and scope of these activities. Research by Whitelaw, J. Riley, and N. Elmrabit (2024) indicates that many insider threats take advantage of weak internal controls and insufficient monitoring systems. However, current studies often fail to consider the psychological and organizational factors that drive insider fraud. This gap in understanding hinders the development of effective preventive measures.

Artificial intelligence (AI) and machine learning (ML) have become essential tools in the fight against banking crime, as banks increasingly adopt these technologies for fraud detection and risk assessment (Bello & Olufemi, 2024). These systems sift through large volumes of data to spot unusual transactions and forecast potential risks. However, some critics contend that the effectiveness of AI-driven solutions is compromised by biases present in data and algorithms, leading to false positives and negatives (Akter et al., 2021). Moreover, criminals have started leveraging AI to create more sophisticated attack methods, such as deepfake identity fraud (Meda, 2024). This dual use of AI in banking crime highlights the necessity for a deeper understanding of its consequences.

The regulatory framework for tackling banking crime in the digital era remains inconsistent and fragmented across different jurisdictions. While international organizations like the Financial Action Task Force (FATF) have set guidelines to combat money laundering and terrorist financing, adherence varies significantly among nations (FATF, 2024). Financial Crime Academy points out the difficulties posed by cross-border banking crimes, where differences in jurisdiction impede effective enforcement (Financial Crime Academy, 2024). Additionally, there is a lack of studies exploring the role of public-private partnerships in improving regulatory compliance and facilitating information sharing among stakeholders.

Another important issue is how banking crime affects customer trust and financial inclusion. Research indicates that frequent cyberattacks and data breaches undermine public confidence in financial institutions, which can deter people from using digital banking services (Natalucci, Qureshi & Suntheim, 2024). This lack of trust particularly impacts vulnerable groups, such as low-income individuals and the elderly, who may not have the digital skills necessary to navigate online banking safely (Msweli & Mawela, 2020). While studies have highlighted these trends, there is a noticeable absence of longitudinal research that explores the long-term consequences of banking crime on consumer behavior and financial inclusion.

Despite significant advancements in understanding the various aspects of banking crime, there are still considerable gaps. For example, there is a scarcity of research on the psychological effects of banking crime on victims, especially in cases of identity theft and financial scams (Alashwali, Chandrashekar, Lanyon & Cranor, 2024). Additionally, the rapid pace of

technological change often outstrips the ability of regulatory frameworks to keep up, leaving both banks and consumers vulnerable to new threats. Future studies should aim to create flexible legal frameworks and comprehensive strategies that consider the relationship between technology, regulation, and human behavior. Addressing these gaps is crucial for protecting the integrity of the banking sector and enhancing public trust in the digital economy..

III. FINDINGS

A. Increased Cyberattacks on Financial Institutions

In recent years, financial institutions have seen a significant rise in cyberattacks, which pose serious risks to global financial stability. The attacks have become more sophisticated and frequent, making it essential for organizations to implement strong cybersecurity measures and regulatory actions. A prominent example of this trend occurred between September 30 and November 18, 2024, when Chinese hackers gained access to over 3,000 unclassified files from the U.S. Treasury Department, including documents related to Secretary Janet Yellen (Bloomberg, 2025). This breach took advantage of a vulnerability in a third-party vendor, BeyondTrust, impacting 419 Treasury computers and compromising sensitive data (Medium, 2025). This incident highlights the increasing danger of cyberattacks aimed at third-party vendors, as hackers look for weaknesses in associated contractors to circumvent strong institutional defenses.

The financial sector has seen a dramatic increase in ransomware attacks. In 2024, around 65% of financial organizations globally reported being targeted by these attacks, up from just 34% in 2021 (Help Net Security, 2024). Furthermore, 46% of financial companies indicated they had experienced a data breach in the last two years (Heiding, Schneier & Vishwanath, 2024). These figures underscore the growing cyber threats confronting the financial industry and the urgent need for improved security measures. Table 1 displays the attacks on global financial institutions that took place in 2024.

Table 1: Financial institution attacks in 2024

Year 2024	Location	Institution	Type of attack	Impact
January	United States	Bank of America	Cyberattack	Data breach resulting in compromised customer information.
February	EU Countries	European Central Bank	Phishing Scam	Fake communications tricked employees into disclosing information
March	India	State Bank of India	Ransomware	Services halted due to malware encryption
April	Brazil	Banco do Brazil	Distributed Denial of Service (DDoS) Attack	Website and online services offline for 24 hours
May	Australia	Commonwealth Bank	Account Takeover	Multiple accounts hacked using social engineering tactics
June	South Korea	KB Kookmin Bank	Insider Trading Leak	Sensitive financial data leaked by a former employee
July	Japan	Mitsubishi UFJ Financial Group	Data Breach	Attack exposed confidential client data
August	United Kingdom	HSBC	Malware Attack	Disruption of mobile banking services for 48 hours
September	Canada	RBC (Royal Bank of Canada)	Fraudulent Transactions	Large-scale unauthorized transactions
October	South Africa	Standard Bank	ATM Skimming	Hackers install devices to steal card info from ATMs
November	UEA	Emirates NBD	Data Breach	Personal data of customers exposed online
December	Russia	Sberbank	Ransomware	Systems locked and ransomed with customer data at risk

In response to these increasing threats, regulatory bodies have introduced new measures to enhance cybersecurity. The European Union's Digital Operational Resilience Act (DORA) took effect, setting uniform standards for digital operational resilience within the financial sector. DORA focuses on managing technological risks, incident reporting, and monitoring ICT providers, with the goal of safeguarding financial entities from cyber threats. Financial institutions were given a two-year timeframe to adjust their structures and processes to meet the regulation, marking a significant advancement in strengthening the digital infrastructure of Europe’s financial sector.

The rise of artificial intelligence (AI) in cyberattacks has further complicated the cybersecurity landscape. AI enables more advanced phishing attacks, allowing less experienced criminals to carry out scams with greater accuracy (Zhang & Tenney, 2024). The introduction of "Phishing-as-a-Service" (PaaS) made it possible to rent or purchase complete phishing kits, reducing the entry barriers for attackers (Swayne, 2025). This trend has resulted in a surge of banking trojans and cryptocurrency scams, prompting financial institutions to implement advanced security measures to combat AI-driven threats.

Government actions have been initiated to tackle these challenges. In January 2025, President Biden released a detailed executive order focused on cybersecurity, which includes securing federal communications against foreign threats, addressing risks posed by AI and quantum computing, and enhancing software supply chain security (Selena, 2024). The order stipulates stricter cybersecurity requirements for companies that collaborate with the federal government and requires the implementation of AI for cyber defense, along with the development of quantum-resistant encryption. This initiative is designed to strengthen America's digital security framework and ensure strong federal cybersecurity standards in the future. The rising number and complexity of cyberattacks on financial institutions highlight the urgent need for improved cybersecurity measures, regulatory compliance, and international collaboration. As cyber threats continue to advance, financial institutions must take proactive steps to protect their operations and uphold the trust of their stakeholders.

B. Emergence of Cryptocurrency-Related Fraud

The rise of cryptocurrency has transformed the global financial landscape, providing unique advantages like decentralized control, anonymity, and transactions without borders. However, these same features have also made cryptocurrencies a prime target for fraudulent activities. The prevalence of cryptocurrency-related fraud has surged, fueled by the swift adoption of digital currencies and the absence of robust regulatory frameworks. This essay delves into the main types of cryptocurrency fraud, the reasons behind its rise, and the wider implications for individuals, businesses, and regulators around the world. Cryptocurrency fraud takes many forms, including Ponzi schemes, initial coin offering (ICO) scams, phishing attacks, and ransomware (Hetler, 2024). Ponzi schemes, for example, are fraudulent investment operations that promise high returns with minimal or no risk. In these schemes, earlier investors are paid with the money from newer investors until the operation ultimately collapses. ICO scams represent another common type of fraud, where malicious individuals create fake cryptocurrency projects to attract investments, only to vanish once they have collected the funds (Desetty, Jangampet & Pulyala, 2020). Additionally, phishing attacks, which use deceptive methods to steal users' private keys or wallet information, have become more sophisticated (Upadhyay & Upadhyay, 2025). Likewise, ransomware attacks demand cryptocurrency payments to unlock essential systems, targeting both businesses and individuals.

In addition to these methods, cryptocurrency fraud has also ventured into newer areas like non-fungible tokens (NFTs). Scammers take advantage of the NFT market by creating fake digital assets or employing wash trading tactics to artificially boost prices (Tamébé, Owen & Nizzero, 2024). Such actions undermine trust in the cryptocurrency market and negatively impact genuine users and investors. Several factors contribute to the rise of cryptocurrency fraud. The decentralized and pseudonymous characteristics of cryptocurrencies eliminate intermediaries like banks and regulators, allowing fraudsters to operate without detection. Unlike traditional financial systems, cryptocurrency transactions are permanent and cannot be reversed, leaving victims with little recourse after a fraudulent transaction. Additionally, the global and borderless nature of cryptocurrencies makes it challenging to trace and recover funds, as offenders often work across various jurisdictions (Octavia, 2021).

The lack of regulatory oversight makes the situation even worse. While some countries have put strict regulations in place to oversee cryptocurrency activities, many areas still lack comprehensive frameworks, resulting in a fragmented regulatory environment. This inconsistency gives fraudsters the opportunity to take advantage of regulatory gaps or operate from places with weak enforcement (Millett et al., 2025). Furthermore, since cryptocurrencies are relatively new, many users do not know the best practices for securing their digital assets, which leaves them open to scams and cyberattacks. The increase in cryptocurrency fraud has serious consequences for both individuals and businesses. For individuals, the financial losses can be catastrophic, especially for those who invest their life savings in deceitful schemes. Victims often experience psychological effects, such as stress and a loss of trust in financial systems. For businesses, cryptocurrency fraud brings operational and reputational challenges. Companies that are targeted by ransomware attacks frequently deal with costly disruptions and may need to spend more on improving their cybersecurity measures (Mulligan, Morsfield & Cheikosman, 2024). Additionally, businesses that accept cryptocurrencies as payment must manage the risks associated with chargebacks and fraudulent transactions.

The broader economic impact of cryptocurrency fraud is significant. When individuals and businesses suffer losses, it diminishes consumer confidence and slows down the adoption of legitimate cryptocurrency solutions. This loss of trust also stifles innovation in the blockchain and cryptocurrency sectors, hindering technological progress that could benefit society (Balaban, 2023).

To address the rising threat of cryptocurrency fraud, regulators and industry stakeholders need to work together to create effective countermeasures. Regulatory efforts should aim to establish a unified framework that considers the global and decentralized characteristics of cryptocurrencies. For instance, international organizations like the Financial Action Task Force (FATF) have

suggested guidelines to combat money laundering and terrorist financing in cryptocurrency transactions. However, for these guidelines to be effective, they must be consistently implemented across different jurisdictions.

Technological solutions are also vital in reducing cryptocurrency fraud. Blockchain analytics tools that utilize artificial intelligence and machine learning can assist in identifying suspicious transactions and tracking illicit activities on the blockchain. Additionally, multi-signature wallets and hardware wallets offer enhanced security for users, lowering the risk of unauthorized access. Educational initiatives designed to raise awareness about cryptocurrency security can further empower users to protect their assets and identify potential scams (Chainalysis, 2024).

Despite ongoing efforts to tackle cryptocurrency fraud, several challenges persist. The fast-paced evolution of technology means that fraudsters are constantly coming up with new ways to exploit weaknesses. Regulators and industry stakeholders need to stay ahead of these trends by promoting innovation in security technologies and adapting to new threats. Moreover, the importance of enhanced international cooperation cannot be emphasized enough. Effective collaboration across borders is vital for investigating and prosecuting crimes related to cryptocurrency (Fruhlinger, 2020). Public-private partnerships can also play a significant role in advancing the fight against cryptocurrency fraud. By sharing intelligence and resources, governments and private organizations can improve their collective capacity to detect and prevent fraudulent activities. Additionally, a proactive regulatory approach-one that balances innovation with consumer protection is essential for creating a secure and trustworthy cryptocurrency environment.

The rise of cryptocurrency-related fraud highlights the complex nature of technological progress. While cryptocurrencies present tremendous opportunities for innovation and financial inclusion, their misuse brings considerable risks to individuals, businesses, and the global economy. Tackling these risks demands a comprehensive strategy that includes strong regulatory frameworks, technological advancements, and public awareness campaigns. By encouraging collaboration among all stakeholders and prioritizing security and transparency, the cryptocurrency ecosystem can achieve sustainable growth while reducing the threats of fraud and abuse.

C. Weaknesses in Banking Software and Insider Threats

The banking industry is a prime target for cyberattacks, largely due to the immense value of the assets and sensitive data it manages. Even with significant technological advancements, vulnerabilities in banking software and the constant threat of insider attacks continue to pose serious challenges. These weaknesses can lead to financial losses, damage to reputation, and potential regulatory fines. To effectively understand and address these risks, a thorough approach is necessary, incorporating strong software design, strict security measures, and diligent oversight.

A major issue with banking software is the dependence on outdated systems. Many banks still operate on legacy systems that were created many years ago. While these systems may have been dependable in their era, they often do not align with contemporary cybersecurity practices and are more vulnerable to attacks. For example, unaddressed vulnerabilities in legacy systems played a significant role in the Equifax breach of 2017, which compromised the personal information of 147 million people (Asseco South Eastern Europe, 2025). Additionally, the failure to implement regular software updates worsens the situation by leaving known security gaps unresolved. Keeping software up to date is essential, as it not only fixes security vulnerabilities but also helps maintain compliance with regulatory requirements.

Banking software often struggles with poorly designed user interfaces and inadequate authentication methods. A complex user interface can lead to mistakes, such as mishandling sensitive information or failing to identify phishing attempts. Furthermore, weak authentication systems, like the ongoing use of single-factor authentication, make it easier for attackers to gain unauthorized access. Research by Asseco South Eastern Europe (ASEE) shows that multifactor authentication (MFA) can decrease unauthorized access attempts, yet many institutions have been slow to implement it (Storchak, 2024). Adopting MFA and biometric solutions can greatly improve security by ensuring that only legitimate users are granted access.

Insider threats represent a major risk for banking institutions. These threats can arise from malicious insiders who deliberately misuse their access to sensitive systems, or from careless employees who unintentionally compromise security. A report by the Ponemon Institute indicates that insider threats are responsible for nearly 60% of data breaches in the financial sector (Khan, Kabanov, Hua & Madnick, 2023). A prominent example is the Capital One breach, a former employee took advantage of a misconfigured firewall to steal sensitive data (Anisa & Widianingsih, 2024). To effectively combat insider threats, institutions should conduct regular employee training, monitor user activity, and implement role-based access controls to limit exposure to sensitive information.

The integration of third-party applications into banking systems brings about additional vulnerabilities. Often, third-party vendors do not adhere to the same strict security standards as banks, which can create potential entry points for attackers. A notable example is the 2020 SolarWinds attack, where hackers took advantage of weaknesses in third-party software to breach numerous organizations, including financial institutions (Erizon, 2024). To reduce these risks, banks should perform comprehensive due diligence on their vendors, impose strict security requirements in contracts, and consistently monitor third-party activities.

Weak encryption protocols and poor data storage practices also jeopardize the security of banking software. Encryption is a crucial aspect of cybersecurity, but if implemented incorrectly, it can become ineffective. According to Data Breach Investigations Report that between 59% and 66% of financial institutions still rely on outdated encryption algorithms that are vulnerable to brute-force attacks (Nadeau, 2024). Moreover, inadequately secured databases can attract cybercriminals. For example, Security Data Intelligence exposed sensitive data 3 billion US citizen data due to a misconfigured database (Deloitte, 2023). It is vital to adopt advanced encryption standards and ensure secure storage practices to safeguard sensitive information.

Many banking institutions currently lack strong incident response plans, which are essential for reducing the effects of security breaches. A solid incident response plan should outline clear procedures for identifying, containing, and addressing threats. However, a survey conducted by Deloitte revealed that 40% of financial institutions do not have thorough incident response strategies in place (Satter & Vicens, 2024). This unpreparedness often leads to slow reactions to cyberattacks, worsening their consequences. Investing in incident response training, simulation exercises, and automated threat detection systems can greatly improve an institution's capability to respond to and recover from security incidents.

Additionally, weaknesses in banking software and the increasing risk of insider threats are pressing issues that need urgent attention. From outdated systems and inadequate authentication methods to the dangers posed by third-party applications, banks encounter numerous challenges. Tackling these vulnerabilities requires a comprehensive approach, including regular software updates, employee training, advanced encryption techniques, and thorough incident response planning. By emphasizing cybersecurity, banks can safeguard themselves against financial losses and uphold the trust of their customers.

IV. DISCUSSION

A. The increase in cyberattacks aimed at financial institutions

The financial sector's interconnectedness and its vital role in the global economy make it a prime target for cybercriminals. A notable instance is the cyberattack on the U.S. Treasury Department which was linked to Chinese hackers (European Union Agency for Cybersecurity (ENISA), 2024). As these institutions increasingly depend on third-party vendors for various services, the likelihood of cyberattacks exploiting these connections rises significantly. Attackers take advantage of these vulnerabilities to circumvent strong defenses, turning third-party relationships into potential risks. This incident reflects a broader trend where hackers focus on third-party vendors, a tactic often called "watering hole" attacks (Cyber Management Alliance, 2024). Consequently, financial institutions must prioritize vendor management and implement strict cybersecurity standards for all contractors involved. Neglecting this could lead to operational disruptions, damage to reputation, and substantial financial losses.

Ransomware attacks have emerged as a major threat to financial institutions. In 2024, 65% of financial organizations reported experiencing ransomware attacks, a significant rise from 34% in 2021 (European Union, 2022). These statistics highlight the industry's susceptibility to advanced ransomware tactics and data breaches. Ransomware attackers frequently take advantage of outdated security protocols, unpatched systems, and human mistakes to gain access to financial networks. The financial repercussions and operational disruptions resulting from these attacks can be severe. For example, ransomware demands can reach millions of dollars, and the downtime caused by such incidents can halt essential financial operations. Moreover, the compromise of sensitive client information damages customer trust and invites regulatory scrutiny, further increasing the burden on affected institutions. To address these threats, financial institutions need to implement robust security measures like endpoint detection and response (EDR) systems, continuous monitoring, and regular security assessments. Additionally, improving employee training programs is crucial to reduce human errors that could give attackers an opportunity to breach security.

Regulatory bodies have taken action against the increasing cybersecurity threats by introducing new frameworks designed to bolster digital resilience. A key regulation in this effort is the European Union's Digital Operational Resilience Act (DORA), which is lays out standardized requirements for managing technological risks within the financial sector, emphasizing incident reporting, monitoring of ICT providers, and testing for operational resilience (Zhang & Tenney, 2024). The importance of DORA lies in its comprehensive approach to cybersecurity. By requiring financial institutions to implement rigorous risk management strategies and establish thorough incident reporting systems, DORA aims to create a consistent standard throughout Europe. Institutions have been granted a two-year period to adapt to these requirements, facilitating a steady yet decisive shift towards improved cybersecurity practices. Nonetheless, the regulation poses challenges, especially for smaller financial entities that may find it difficult to allocate the necessary resources for compliance. These institutions face the risk of penalties for non-compliance, which could further complicate their operations.

The incorporation of artificial intelligence (AI) into cyberattacks has introduced a new layer of complexity to the cybersecurity landscape. AI was extensively utilized to enhance sophisticated phishing attacks, allowing attackers to create highly convincing scams. The emergence of "Phishing-as-a-Service" (PaaS) platforms has also made cybercrime more accessible, enabling attackers to rent or buy phishing kits with little technical know-how (Reuters, 2025).

This trend has resulted in a rise in banking trojans and cryptocurrency scams that take advantage of weaknesses in financial systems to steal funds and compromise sensitive information. To effectively combat these threats, financial institutions need to implement advanced AI-driven cybersecurity tools. For instance, machine learning-powered behavioral analytics can identify

unusual activities that may signal cyberattacks in real-time, allowing institutions to act quickly. Additionally, it is crucial for financial institutions to collaborate with cybersecurity firms to share threat intelligence and create innovative solutions to counter AI-enhanced cyber threats.

Additionally, financial institutions must emphasize employee training and awareness programs to reduce human errors, which continue to be a major vulnerability. Governments should maintain a proactive stance in establishing cybersecurity standards and offering resources to help smaller entities meet these requirements. Public-private partnerships are crucial for driving innovation in cybersecurity and tackling the ever-evolving threat landscape. The growing wave of cyber threats calls for a united effort from all players in the financial sector. By implementing advanced security measures, adhering to stringent regulatory frameworks, and promoting international collaboration, financial institutions can protect their operations and contribute to global financial stability. Recent incidents, like the U.S. Treasury breach (Wang et al., 2025), should serve as a crucial reminder to prioritize cybersecurity across all levels of the financial ecosystem.

B. Cryptocurrency-related fraud and the growing acceptance of digital currencies

The rise of cryptocurrency has transformed the global financial landscape, offering significant advantages such as decentralized control, anonymity, and the ability to conduct transactions across borders. However, these same features have also made cryptocurrencies appealing for fraudulent activities, leading to an increase in crimes related to digital currencies. The rapid expansion of these currencies, combined with a lack of comprehensive regulatory measures, has created an environment ripe for scams, phishing, and other malicious actions. Cryptocurrency fraud includes a variety of schemes, such as Ponzi schemes, phishing attacks, ransomware, and the misuse of non-fungible tokens (NFTs). For example, Ponzi schemes attract investors with promises of high returns, only to collapse when new investments dry up, resulting in substantial financial losses (Hornuf, Kück & Schwienbacher, 2022). Similarly, initial coin offering (ICO) scams deceive investors by presenting fake cryptocurrency projects, taking their money under the pretense of innovation (Upadhyay & Upadhyay, 2025a). Additionally, phishing attacks aim to steal users' private keys or wallet information through misleading tactics, while ransomware demands cryptocurrency payments to restore access to critical systems. In the rapidly growing NFT market, fraudulent activities include fake digital assets and manipulative tactics like wash trading, which undermine trust and negatively impact legitimate participants (Uzougbo, Ikegwu & Adewusi, 2024). These types of fraud reveal the weaknesses within the cryptocurrency ecosystem and highlight the pressing need for strong measures to protect users and investors.

Several key factors have led to the rise of cryptocurrency fraud, many of which stem from the very nature of cryptocurrencies. The decentralized and pseudonymous structure of blockchain technology removes intermediaries like banks and regulatory agencies, allowing fraudsters to operate with a degree of freedom. Unlike traditional financial transactions, which can be reversed and traced, cryptocurrency transactions are permanent, leaving victims with few options once a fraudulent transfer takes place. The global nature of cryptocurrencies adds another layer of complexity to enforcement efforts, as criminals often take advantage of differences in laws across jurisdictions to avoid being caught (Narain & Moretti, 2022). Additionally, the relative novelty of digital currencies means that many users are not fully aware of how to protect their assets, making them vulnerable to scams and cyberattacks. Regulatory gaps further complicate the situation, with a fragmented international framework that allows fraudsters to exploit inconsistencies between different regions. While some countries have put strict measures in place to oversee cryptocurrency activities, others have not kept pace, creating safe havens for those with malicious intent (Möller, 2023). These systemic weaknesses highlight the need for a unified and comprehensive regulatory strategy to address the risks linked to cryptocurrency fraud.

The impact of cryptocurrency fraud goes well beyond just individual financial losses; it has repercussions for businesses, economies, and regulatory bodies worldwide. For those affected, the results can be devastating, with victims often losing their life savings to scams or suffering from the emotional toll of their losses. Companies, especially those hit by ransomware, experience major operational disruptions and damage to their reputation. The costs tied to these attacks include not just the ransom itself but also the expenses related to system recovery and improved cybersecurity measures (Maleh, Zhang & Hansali, 2024). The wider economic implications are equally alarming. Rampant fraud erodes public trust in digital currencies, which can stall their adoption and stifle innovation in the blockchain sector. This loss of confidence deters investment and slows the progress of technologies that could promote financial inclusion and transparency (Financial Action Task Force (FATF), 2024). On the regulatory front, the rise in fraud presents a challenge for governments trying to balance the need for innovation with the necessity of consumer protection. The lack of unified international standards worsens the situation, underscoring the importance of collaborative efforts to effectively tackle cross-border cryptocurrency crimes.

Addressing the increasing threat of cryptocurrency fraud requires a comprehensive strategy that includes regulatory oversight, technological advancements, and public awareness. International bodies like the Financial Action Task Force (FATF) have suggested guidelines to tackle money laundering and terrorist financing in cryptocurrency transactions, but their success hinges on consistent application across different jurisdictions (Esan, Ajayi & Olawa, 2024). Technological innovations, such as blockchain analytics and enhanced security tools, hold great promise for detecting and preventing fraud. For example, artificial

intelligence and machine learning can scrutinize transaction patterns to spot suspicious activities, while multi-signature and hardware wallets improve user security.

Public education efforts are also vital, equipping users to identify and steer clear of scams while adopting best practices for safeguarding their assets (Federal Trade Commission, 2024). Despite these initiatives, challenges remain. The fast-paced evolution of technology enables fraudsters to create new exploitation methods, requiring regulators and industry participants to continuously adapt. Moreover, effective international collaboration is a crucial yet underdeveloped element in the fight against cryptocurrency fraud. Public-private partnerships, intelligence sharing, and proactive regulation are key to building a secure and transparent cryptocurrency environment. By focusing on these strategies, stakeholders can reduce the risks associated with digital currencies and promote their sustainable growth within the global financial system.

C. Vulnerabilities in Banking Software and Risks Posed by Insider Threats

The banking industry has become a prime target for cyberattacks, largely due to the valuable assets and sensitive information it manages. As digital banking continues to expand, cybercriminals are increasingly exploiting weaknesses in banking software to gain access to financial resources and personal data. Despite significant technological advancements, the sector remains at risk because of issues like poor software design, outdated systems, insider threats, third-party vulnerabilities, and inadequate encryption practices. Tackling these problems requires a thorough strategy that encompasses strong software development, effective authentication methods, and diligent oversight.

One major vulnerability in banking software is the ongoing dependence on outdated legacy systems. While these systems may have been effective in the past, they are becoming less compatible with current cybersecurity measures. Many banks continue to use legacy software due to its perceived reliability and the high costs of upgrading or replacing it. However, these older systems often lack essential security updates and are more susceptible to attacks. A notable example is the Equifax data breach in 2017, which compromised the personal information of over 147 million individuals, primarily because of an unpatched flaw in a legacy system (Cyber Readiness Institute, 2024). Regular software updates are crucial not only for fixing vulnerabilities but also for adhering to regulatory requirements. Financial institutions that neglect to keep their software current face serious risks, including regulatory penalties, damage to their reputation, and financial losses. Therefore, banks must prioritize updating their IT infrastructure to align with modern cybersecurity demands.

In addition to outdated systems, banking software often struggles with poorly designed user interfaces and inadequate authentication methods. An unintuitive or overly complex user interface can lead to mistakes that jeopardize sensitive information. Furthermore, many banking systems still depend on single-factor authentication (SFA), which can be easily circumvented by attackers. A report from the Cyber Readiness Institute shows that 85% of organizations do not mandate the use of multi-factor authentication (MFA) for their customers or suppliers, yet many institutions have been slow to adopt it (Khan, Kabanov, Hua & Madnick, 2022). MFA and biometric verification are crucial elements of modern cybersecurity, providing an extra layer of defense against unauthorized access. By integrating stronger authentication systems, banks can prevent attackers from accessing their systems, even if they manage to acquire login credentials. With the increasing threat of credential theft through phishing and other tactics, MFA has become an essential tool in minimizing the risk of successful cyberattacks.

A major challenge in banking cybersecurity is the risk posed by insiders. Insider threats, whether they are deliberate or accidental, make up a significant portion of data breaches in the financial sector. Malicious insiders, like disgruntled employees or contractors, may intentionally misuse their access to sensitive information, while negligent insiders might unintentionally compromise security through errors such as improper data handling. A notable example of an insider threat is the 2019 Capital One data breach (Marelli, 2022), where a former employee took advantage of a misconfigured firewall to access millions of customer records. To address insider threats, banks need to invest in employee training, implement strict access controls, and monitor user activities for any signs of suspicious behavior. Role-based access controls (RBAC) are especially effective in restricting access to sensitive data according to an individual's job responsibilities, thereby reducing the risk of unauthorized exposure.

The integration of third-party applications and vendors into banking systems adds complexity to the cybersecurity landscape. Financial institutions often rely on these external partners for various services, such as software development, cloud storage, and data analytics. However, these vendors may not follow the same strict security protocols as the banks, which can lead to potential vulnerabilities. The 2020 SolarWinds cyberattack highlighted the risks associated with third-party relationships, as hackers took advantage of weaknesses in the company's software to breach multiple organizations, including several banks (International Bank for Reconstruction and Development, 2023). To mitigate these risks, banks need to perform comprehensive due diligence on third-party vendors before forming partnerships. This process should involve assessing the vendor's security measures, conducting regular security audits, and implementing strict security requirements in vendor contracts. Ongoing monitoring of third-party activities is crucial to detect potential threats before they develop into serious breaches.

Banks face additional vulnerabilities from weak encryption protocols and poor data storage practices, which can jeopardize customer information. Encryption plays a crucial role in protecting sensitive data both during transmission and while

stored. Yet, some banks continue to rely on outdated encryption algorithms that are susceptible to modern attack techniques, including brute-force attacks. World Bank Report found that 30% of financial institutions still use these outdated methods, putting their data at risk (Sobers, 2024). Moreover, databases that lack proper security measures can easily fall prey to cybercriminals. To protect data effectively, banks need to implement advanced encryption standards and secure storage practices. Essential steps include utilizing end-to-end encryption, regularly updating encryption protocols, and ensuring that databases are correctly configured to prevent data breaches.

The absence of strong incident response plans poses a major challenge for many banks. A well-crafted incident response plan allows organizations to effectively detect, contain, and lessen the impact of a cyberattack. However, a recent Varonis survey revealed that 40% of financial institutions lack a comprehensive incident response strategy. This unpreparedness often results in delayed reactions, which can worsen the damage inflicted by cyberattacks. Insufficient incident response plans can also complicate the recovery process, leading to extended service interruptions and a decline in customer trust. To enhance their response capabilities, banks should focus on providing incident response training for staff, conducting regular simulation drills, and implementing automated threat detection systems that can swiftly identify and address security incidents. The banking sector encounters a variety of cybersecurity challenges, including outdated software, weak authentication methods, insider threats, and vulnerabilities from third parties. Tackling these risks demands a comprehensive strategy that involves updating IT infrastructure, adopting more robust security measures, and establishing effective oversight mechanisms. By emphasizing cybersecurity and proactively addressing these weaknesses, banks can safeguard their assets, protect customer data, and uphold trust in an increasingly digital landscape. Without a dedicated effort to bolster cybersecurity, banks face the risk of substantial financial and reputational harm, along with regulatory penalties that could jeopardize their long-term sustainability.

CONCLUSIONS

Banking crimes in today's technological landscape pose complex challenges that demand innovative solutions to tackle the ever-evolving threats from cybercriminals, hackers, and other malicious entities. As the financial sector becomes more digitized, the risks of fraud, identity theft, and cyberattacks on banking systems increase, jeopardizing public trust and the stability of financial institutions. While technological advancements have enhanced banking services and accessibility, they have also created opportunities for sophisticated criminal activities that are hard to trace and combat. As financial institutions shift towards more automated and online platforms, the urgency for strong cybersecurity measures, stricter regulatory frameworks, and international collaboration has never been greater.

To effectively address banking crimes in the digital age, future initiatives should prioritize enhancing technological safeguards, such as adopting advanced encryption protocols and AI-driven security systems to identify and counter fraudulent activities in real time. Furthermore, regulators need to create a global framework for cybersecurity standards that can evolve with emerging threats. Financial institutions ought to invest in ongoing employee training programs, equipping their staff with the skills to recognize and respond to potential cyber risks. Public awareness campaigns on cybersecurity should also be emphasized to help individuals protect their personal financial information. Finally, fostering international cooperation among governments, financial institutions, and law enforcement agencies will be essential in tracking cross-border cybercriminal networks and prosecuting offenders.

CONFLICT OF INTEREST: The author declares no conflict of interest

FUNDING: The author receive no funding for this research

REFERENCES

1) FATF, Interpol, & Egmont Group. (2023). Illicit financial flows from cyber-enabled fraud. https://www.fatf-gafi.org/en/publications/Methodsandtrends/illicit-financial-flows-cyber-enabled-fraud.html
2) Petrosyan, A. (2024, July 10). Share of financial organizations worldwide hit by ransomware attacks from 2021 to 2024. Cyber attacks in the financial sector. Statista. https://www.statista.com/statistics/1460896/rate-ransomware-attacks-global/
3) United Nations Office on Drugs and Crime. (2024). Money laundering. UNODC Annual Report. https://www.unodc.org/unodc/en/about-unodc/annual-report.html
4) Interface. (2024, June 27). Navigating the EU cybersecurity policy ecosystem: A comprehensive overview of legislation, policies, and actors. https://www.interface-eu.org/publications/navigating-the-eu-cybersecurity-policy-ecosystem
5) The Economic Times. (2025, January 22). Banking frauds rise in H1FY25, amount involved jumps 8-time: RBI report. The Economic Times. https://economictimes.indiatimes.com/industry/banking/finance/banking/banking-frauds-rise-in-h1fy25-amount-involved-jumps-8-time-rbi-report/articleshow/116685504.cms
6) World Bank Group. (2024). World development report 2024: The middle-income trap. World Bank Group. https://www.worldbank.org/en/publication/wdr2024
7) Cyber Management Alliance. (2024, July 11). The impact of digital transformation on the evolution of banking systems.

https://www.cm-alliance.com/cybersecurity-blog/the-impact-of-digital-transformation-on-evolution-of-banking-systems

8) Asmar, M., & Tuqan, A. (2024, September 15). Integrating machine learning for sustaining cybersecurity in digital banks. Heliyon, 10(17), e37571. https://doi.org/10.1016/j.heliyon.2024.e37571
9) World Economic Forum. (2024, May 15). Global financial stability at risk due to cyber threats, IMF warns. Here's what to know. Cybersecurity. https://www.weforum.org/stories/2024/05/financial-sector-cyber-attack-threat-imf-cybersecurity/
10) Saha, S., Hasan, A. R., Mahmud, A., Ahmed, N., Parvin, N., & Karmakar, H. (2024). Cryptocurrency and financial crimes: A bibliometric analysis and future research agenda. Multidisciplinary Reviews, 7(8), 2024168. https://doi.org/10.31893/multirev.2024168
11) Yaseen, Q. (2024). Insider threat in banking systems. In S. A. Aljawarneh (Ed.), Online banking security measures and data protection (pp. 222–236). https://doi.org/10.4018/978-1-5225-0864-9.ch013
12) Whitelaw, F., Riley, J., & Elmrabit, N. (2024). A review of the insider threat, a practitioner perspective within the U.K. financial services. IEEE Access, 12, 34752–34768. https://doi.org/10.1109/ACCESS.2024.3373265
13) Bello, O. A., & Olufemi, K. (2024). Artificial intelligence in fraud prevention: Exploring techniques and applications, challenges, and opportunities. Computer Science & IT Research Journal, 5(6), 1505–1520. http://dx.doi.org/10.51594/csitrj.v5i6.1252
14) Akter, S., McCarthy, G., Sajib, S., Michael, K., Dwivedi, Y. K., D'Ambra, J., & Shen, K. N. (2021). Guest editorial: Algorithmic bias in data-driven innovation in the age of AI. International Journal of Information Management, 60, 102387. https://doi.org/10.1016/j.ijinfomgt.2021.102387.
15) Meda, K. (2024, May 3). Identity theft is being fueled by AI & cyber-attacks. Thomson Reuters.
16) Financial Action Task Force (FATF). (2024). Virtual assets: Targeted update on implementation of the FATF standards on VAs and VASPs. Paris, France: FATF. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html
17) Financial Crime Academy. (2024, December 2). Breaking the chains: Confronting cross-border money laundering risks. Anti-Money Laundering (AML). https://financialcrimeacademy.org/
18) Natalucci, F., Qureshi, M. S., & Suntheim, F. (2024, April 9). Rising cyber threats pose serious concerns for financial stability. https://www.bacalahmalaysia.my/imf-rising-cyber-threats-pose-serious-concerns-for-financial-stability/
19) Msweli, N. T., & Mawela, T. (2025). The benefits and challenges of using datathons as a method of learning data analytics. In K. Hinkelmann & H. Smuts (Eds.), Society 5.0. Society 5.0 2024 (Communications in Computer and Information Science, Vol. 2173. Springer. https://doi.org/10.1007/978-3-031-71412-2_20
20) Alashwali, E., Chandrashekar, R. M., Lanyon, M., & Cranor, L. F. (2024, August 15). Detection and impact of debit/credit card fraud: Victims' experiences. arXiv. https://doi.org/10.48550/arXiv.2408.08131
21) Bloomberg. (2025, January 17). Chinese hackers accessed Janet Yellen's computer in US Treasury breach. South China Morning Post. https://www.scmp.com/news/world/united-states-canada/article/3295105/chinese-hackers-accessed-janet-yellens-computer-us-treasury-breach
22) Medium. (2025, January 18). Digital heist: Chinese hackers breach U.S. Treasury, Yellen's computer compromised. Medium. https://medium.com/@FromLagosto/digital-heist-chinese-hackers-breach-u-s-treasury-yellens-computer-compromised-5e8ad9ac91ff
23) Help Net Security. (2024, December 20). 46% of financial institutions had a data breach in the past 24 months. https://www.helpnetsecurity.com/2024/12/20/financial-industry-data-breaches/
24) Heiding, F., Schneier, B., & Vishwanath, A. (2024, May 30). AI will increase the quantity—and quality—of phishing scams. Harvard Business Review. https://hbr.org/2024/05/ai-will-increase-the-quantity-and-quality-of-phishing-scams
25) Zhang, J., & Tenney, D. (2024). The evolution of integrated advance persistent threat and its defense solutions: A literature review. Open Journal of Business and Management, 12, 293–338. https://doi.org/10.4236/ojbm.2024.121021
26) Swayne, M. (2025, January 17). Biden expands cybersecurity mandate, targets AI and quantum risks. Quantum Insider. https://thequantuminsider.com/2025/01/17/biden-expands-cybersecurity-mandate-targets-ai-and-quantum-risks/
27) Selena, N. (2024, December 4). The dark side of crypto: Fraud and money laundering. Digital Watch. https://dig.watch/updates/the-dark-side-of-crypto-fraud-and-money-laundering
28) Hetler, A. (2024, December 17). Cryptocurrency scams: Common types and prevention. Informa TechTarget. https://www.techtarget.com/whatis/feature/Common-cryptocurrency-scams%3Famp=1
29) Desetty, A. G., Jangampet, V. D., & Pulyala, S. R. (2020, December). Phishing attacks: Evolving techniques, emerging trends, and countermeasure strategies. Cybersecurity Journal, 9(12), 985–991. https://www.researchgate.net/publication/376645699_Phishing_Attacks_Evolving_Techniques_Emerging_Trends_and_Countermeasure_Strategies
30) Upadhyay, N., & Upadhyay, S. (2025). The dark side of non-fungible tokens: Understanding risks in the NFT marketplace from a fraud triangle perspective. Financial Innovation, 11(62). https://doi.org/10.1186/s40854-024-00684-6

31) Tamébé, N., Owen, A., & Nizzero, M. (2024, December). Crypto-asset recovery challenges, observed practices, and strategies. Royal United Services Institute. https://www.rusi.org/explore-our-research/publications/special-resources/crypto-asset-recovery-challenges-observed-practices-and-strategies
32) Octavia, J. (2021). Addressing legal ambiguities and regulatory gaps: Defining online fraud and scams in Indonesia. Tech For Good Institute. https://saferinternetlab.org/addressing-legal-ambiguities-and-regulatory-gaps-defining-online-fraud-and-scams-in-indonesia/.
33) Millett, R., Budd, C., Knight, R., Shrimpton, H., Meghjee, W., & Slark, F. (2025, January 14). The experiences and impacts of ransomware attacks on individuals and organizations. GOV.UK. https://www.gov.uk/government/publications/the-experiences-and-impact-of-ransomware-attacks-on-victims/the-experiences-and-impacts-of-ransomware-attacks-on-individuals-and-organisations
34) Mulligan, C., Morsfield, S., & Cheikosman, E. (2024). Blockchain for sustainability: A systematic literature review for policy impact. Telecommunications Policy, 48(2), 102676. https://doi.org/10.1016/j.telpol.2023.102676
35) Balaban, D. (2023, August 7). Advancing cybersecurity education within the cryptocurrency sphere. Forbes. https://www.forbes.com/sites/davidbalaban/2023/08/07/advancing-cybersecurity-education-within-the-cryptocurrency-sphere/
36) Chainalysis. (2024, May 9). How to use blockchain intelligence to investigate crypto crime. https://www.chainalysis.com/blog/investigate-crypto-crime-blockchain-intelligence/
37) Fruhlinger, J. (2020, February 12). Equifax data breach FAQ: What happened, who was affected, what was the impact? CSO Online. https://www.csoonline.com/article/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html
38) Asseco South Eastern Europe. (2025). SxS – Strong multi-factor authentication. https://see.asseco.com/more-sectors/426/630/?L=-9654.
39) Storchak, Y. (2024, February 14). Insider threat statistics for 2024: Reports, facts, actors, and costs. Cybersecurity Insiders. https://www.syteca.com/en/blog/insider-threat-statistics-facts-and-figures
40) Khan, S., Kabanov, I., Hua, Y., & Madnick, S. (2023, February). A systematic analysis of the Capital One data breach: Critical lessons learned. ACM Transactions on Privacy and Security, 26(1), Article 3. https://doi.org/10.1145/3546068
41) Gia Anisa, & Widianingsih, F. (2024). SolarWinds attack: Stages, implications, and mitigation strategies in the cyber age. Electronic Integrated Computer Algorithm Journal, 2(1), 47–52. https://doi.org/10.62123/enigma.v2i1.31
42) Erizon. (2024). 2024 data breach investigations report. https://www.verizon.com/business/resources/Tfdb/reports/2024-dbir-data-breach-investigations-report.pdf?msockid=0e392546a01a6ab200a8305ca1406b00
43) Nadeau, J. (2024, December 19). 2024 roundup: Top data breach stories and industry trends. Security Intelligence. https://www.ibm.com/think/insights/2024-roundup-top-data-breach-stories-and-industry-trends
44) Deloitte. (2023). Riding the wave: 2023 hot topics for IT internal audit: An internal audit viewpoint. https://www.deloitte.com/uk/en/Industries/financial-services/perspectives/hot-topics-it-internal-audit.html
45) Satter, R., & Vicens, A. J. (2024, December 31). US Treasury says Chinese hackers stole documents in 'major incident'. Reuters.https://www.reuters.com/technology/cybersecurity/us-treasurys-workstations-hacked-cyberattack-by-china-afp-reports-2024-12-30/
46) European Union Agency for Cybersecurity (ENISA). (2024, September). ENISA threat landscape (C. Ardagna, S. Corbiaux, & K. Van Impe, Eds.). ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
47) Cyber Management Alliance. (2024, September 13). Top 5 cyber threats facing financial institutions today. https://www.cm-alliance.com/cybersecurity-blog/top-5-cyber-threats-facing-financial-institutions-today
48) European Union. (2022, December 27). The Digital Operational Resilience Act (DORA), Regulation (EU) 2022/2554, OJ L 333. http://data.europa.eu/eli/reg/2022/2554/oj
49) Zhang, J., & Tenney, D. (2024). The evolution of integrated advanced persistent threat and its defense solutions: A literature review. Open Journal of Business and Management, 12(1), 293–338. https://doi.org/10.4236/ojbm.2024.121021
50) Reuters. (2025, January 16). Chinese hackers accessed Yellen's computer in US Treasury breach. Reuters. https://www.reuters.com/technology/cybersecurity/chinese-hackers-accessed-yellens-computer-us-treasury-breach-bloomberg-news-2025-01-17/
51) Wang, L., Cheng, H., Sun, Z., Tian, A., & Yang, Z. (2025). PSPL: A Ponzi scheme smart contracts detection approach via compressed sensing oversampling-based peephole LSTM. Future Generation Computer Systems, 166, 107655. https://doi.org/10.1016/j.future.2024.107655
52) Hornuf, L., Kück, T., & Schwienbacher, A. (2022). Initial coin offerings, information disclosure, and fraud. Small Business Economics, 58, 1741–1759. https://doi.org/10.1007/s11187-021-00471-y
53) Upadhyay, N., & Upadhyay, S. (2025). The dark side of non-fungible tokens: Understanding risks in the NFT marketplace from a fraud triangle perspective. Financial Innovation, 11(62). https://doi.org/10.1186/s40854-024-00684-6

54) Uzougbo, N. S., Ikegwu, C. G., & Adewusi, A. O. (2024). International enforcement of cryptocurrency laws: Jurisdictional challenges and collaborative solutions. Magna Scientia Advanced Research and Reviews, 11(1), 68–83. https://doi.org/10.30574/msarr.2024.11.1.0075
55) Narain, A., & Moretti, M. (2022, September). Regulating crypto. International Monetary Fund (IMF). https://www.imf.org/en/Publications/fandd/issues/2022/09/Regulating-crypto-Narain-Moretti
56) Moller, D. P. F. (2023). Ransomware attacks and scenarios: Cost factors and loss of reputation. In Guide to cybersecurity in digital transformation (Advances in Information Security, Vol. 103, pp. [page numbers if available]). Springer, Cham. https://doi.org/10.1007/978-3-031-26845-8_6
57) Maleh, Y., Zhang, J., & Hansali, A. (Eds.). (2024). Advances in emerging financial technology and digital money (1st ed.). CRC Press.
58) Financial Action Task Force (FATF). (2024, June). Jurisdictions under increased monitoring. https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/increased-monitoring-june-2024.html
59) Esan, O., Ajayi, F. A., & Olawa, O. (2024). Supply chain integrating sustainability and ethics: Strategies for modern supply chain management. World Journal of Advanced Research and Reviews, 22(01), 1930–1953. https://doi.org/10.30574/wjarr.2024.22.1.1259
60) Federal Trade Commission. (2024, November). Equifax data breach settlement. https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3203-equifax-inc
61) Cyber Readiness Institute (CRI). (2024, November 12). New study underscores slow adoption of multifactor authentication by global SMBs. https://cyberreadinessinstitute.org/news-and-events/new-study-underscores-slow-adoption-of-multifactor-authenification/
62) Khan, S., Kabanov, I., Hua, Y., & Madnick, S. (2022, February). A systematic analysis of the Capital One data breach: Critical lessons learned. ACM Transactions on Privacy and Security, 26(1), Article 3. https://doi.org/10.1145/3546068
63) Marelli, M. (2022). The SolarWinds hack: Lessons for international humanitarian organizations. International Review of the Red Cross, 104(919), 1267–1284. https://doi.org/10.1017/S1816383122000194
64) International Bank for Reconstruction and Development / The World Bank. (2023). Lessons learned from the first generation of money laundering and terrorist financing risk assessments. https://documents1.worldbank.org/curated/en/099052110042330899/pdf/IDU0c1b39c8c0bfd604cf608ad40de3e4e0e24b8.pdf
65) Sobers, R. (2024, September 13). 157 cybersecurity statistics and trends. Varonis. https://www.varonis.com/blog/cybersecurity-statistics