Guarding the Financial System: Strengthening IT Governance to Combat Mule Accounts

Mule accounts, or bank accounts used for illegal financial transactions, pose a significant threat to the integrity of financial systems worldwide, including in Thailand, where the rapid expansion of mobile banking, high smartphone penetration, and relatively easy account opening procedures have made it an attractive target for fraudsters.[1] In particular, Thailand's financial system faces unique challenges due to the high volume of real-time fund transfers, widespread use of social media for recruitment, and limited digital literacy among certain population segments. Financial experts have noted that mule accounts frequently exploit vulnerabilities in digital banking infrastructure, particularly in areas such as cross-bank data verification and real-time monitoring systems. It is estimated that global money laundering activities, often facilitated through mule accounts, could reach up to US$1.6 trillion annually, underlining the magnitude of the issue.[2] In Thailand, authorities suspended more than 135,000 mule accounts in the first quarter of 2025 alone, highlighting the scale of the challenge at the national level.[3] This problem mirrors global trends, with fraudsters continually evolving tactics to exploit technological gaps and regulatory loopholes.

Data from Thailand's Ministry of Digital Economy and Society (DE) indicates a sharp increase in mule account activities since 2023, often linked to the expansion of digital fraud schemes.[4] Evidence shows that fraudsters have adapted quickly to weaknesses in mobile banking security, making real-time detection and intervention more crucial than ever.[5] This swift adaptation correlates with the rise of digital payment fraud cases. Fraudsters increasingly exploit gaps in mobile banking security frameworks, underscoring the increasing complexity of financial fraud. Effective IT governance plays a crucial role in proactively defending against emerging threats by identifying, monitoring, and managing the risk associated with mule accounts. The growing sophistication of these crimes demands a holistic approach that integrates advanced technologies with regulatory compliance frameworks.

UDOM NETRATTANAGUL | CISA, CPIAT, ISO/IEC 27001

Is an IT governance and compliance professional with extensive experience in Thailand's financial sector, including at banks. He specializes in IT governance, data privacy, and regulatory compliance. He has led various initiatives to enhance IT governance frameworks, focusing on risk mitigation and regulatory alignment.

Understanding Mule Accounts

There are generally two types of mule accounts: willing mules and unwitting mules.

The term "willing mule" describes individuals who knowingly allow their bank accounts to be used for criminal purposes, usually in exchange for financial compensation. While not a legal term, it reflects behaviors consistent with what law enforcement agencies, including the US Federal Bureau of Investigation (FBI), categorize as "complicit" or "witting" money mules. These individuals are often recruited through social media advertisements, online forums, or peer networks with promises of quick and easy money. Although they are fully aware that their involvement is illegal, they may ignore red flags and rationalize their actions as a seemingly harmless way to earn extra income.[6] Regardless of their understanding, their participation directly facilitates fraudulent transactions and money laundering. Under US federal law, such involvement, particularly when conducted knowingly, can result in serious legal consequences, including criminal prosecution.[7]

Unwitting mules are often victims themselves, manipulated into participating through deception. Fraudsters commonly use fake job postings, romantic scams, or fake investment opportunities to trick individuals into sharing their banking credentials or opening new accounts on their behalf. In many cases, unwitting mules believe they are engaging in legitimate business activities, such as processing customer payments or assisting with international fund transfers. Because they are unaware of the criminal intent behind the transactions, identifying and prosecuting these individuals poses unique

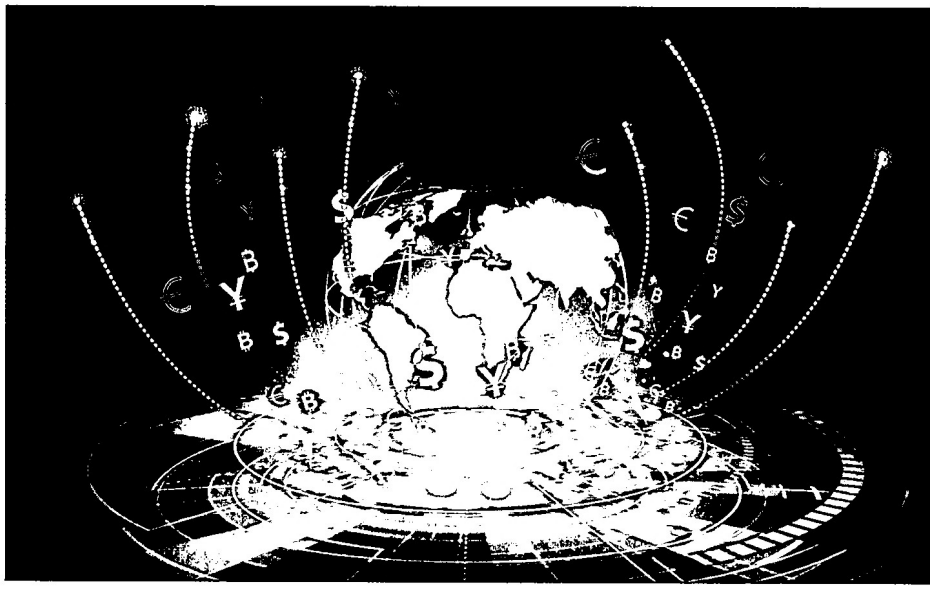
challenges for law enforcement and financial institutions.[8] Distinguishing between these two types of mule accounts is essential for crafting effective detection and prevention strategies tailored to each group's behavioral patterns.

In Thailand, the rapid growth of online financial transactions and digital banking has created more opportunities for mule accounts to emerge, adding layers of complexity to the regulatory and compliance landscape. Due to the country's high smartphone penetration rate and the widespread adoption of mobile banking, mule accounts have become a preferred tool for fraudsters.[9] The ease of opening new bank accounts online, often with minimal verification, has contributed to the proliferation of mule accounts. Fraudsters exploit this convenience by recruiting individuals through social media platforms and promising quick money in exchange for the use of their bank accounts.

The impact of mule accounts extends beyond individual banks, affecting the broader financial ecosystem. Fraudulent transactions facilitated through mule accounts result in annual financial losses amounting to billions of baht, impacting financial institutions, enterprises, and individuals alike.[10] These accounts are often tied to organized crime syndicates involved in activities such as money laundering, online scams, and cybercrimes. Additionally, the reputational damage to banks can erode public trust, leading to reduced confidence in digital financial services. Regulatory fines and legal consequences for inadequate anti-fraud controls can also impose long-term financial burdens on financial institutions.[11]

It is estimated that call center scams have accounted for more than 30% of all reported financial fraud cases in India since 2023, reflecting the scale of the issue.

One of the most alarming trends is the surge in call center scams run by organized criminal groups. These gangs manipulate victims using social engineering tactics, often impersonating



authorities or financial institutions to extract sensitive information and coerce victims into transferring money. Such scams lead to monetary losses and significantly undermine public trust in the banking sector. It is estimated that call center scams have accounted for more than 30% of all reported financial fraud cases in India since 2023, reflecting the scale of the issue.[12]

Human Factors in Mule Account Proliferation

The human factors in the proliferation of mule accounts are critical and multifaceted. In Thailand, individuals are drawn into mule activities through a complex interplay of psychological, economic, and social vulnerabilities. Psychological manipulation is a key tactic where fraudsters exploit cognitive biases and emotional triggers such as fear of authority, desire for quick financial gains, and social conformity pressures. Economic vulnerability exacerbates this risk, as individuals facing financial hardship are more susceptible to fraudulent promises of easy money. Furthermore, a widespread lack of financial literacy and awareness about the mechanisms of financial crimes leaves many unaware of the legal risk and ethical implications of their actions.[13] This combination of factors creates fertile ground for fraudsters to operate, emphasizing the need for targeted educational campaigns and robust financial literacy programs to mitigate this human-centric risk. To better understand how this risk materializes in practice, it is helpful to examine the specific human vulnerabilities that fraudsters commonly exploit.

Several key behavioral dimensions contribute to the proliferation of mule accounts:

1. **Psychological manipulation**—Social engineering tactics are at the core of recruitment strategies used by fraudsters to turn ordinary individuals into money mules. These tactics exploit fundamental psychological vulnerabilities, leveraging trust, fear, and urgency to bypass critical thinking. Scammers often impersonate credible figures, such as bank officials, law enforcement officers, or trusted acquaintances, establishing authority to manipulate their targets. They deploy tactics to create high-pressure scenarios, such as the threat of legal consequences or promises of lucrative, time-sensitive opportunities, to trigger impulsive decisions. Moreover, fraudsters use emotional appeals, instilling fear, guilt, or a false sense of duty to coerce individuals into compliance. Understanding these psychological levers is crucial for developing effective countermeasures, including public awareness initiatives that empower individuals to recognize and resist manipulation tactics.[14]
2. **Economic hardship**—Economic hardship is a significant driver behind involvement in mule activities, particularly in Thailand, where income inequality and financial instability affect large segments of the population.[15] Vulnerable groups such as students burdened with educational expenses, the unemployed facing limited job opportunities, and low-income workers struggling to meet daily living costs are often prime targets. Fraudsters craft deceptive narratives, presenting seemingly legitimate job offers through social media platforms and online job portals, promoting roles that promise high earnings for minimal effort. These scams are meticulously designed to exploit the financial desperation of individuals, making them susceptible to propositions that, under normal circumstances, would raise suspicion. The lack of stable financial support systems further exacerbates this vulnerability, highlighting the urgent need for comprehensive financial education and social safety nets to reduce the appeal of such fraudulent schemes.[16]
3. **Lack of awareness**—A significant number of unwitting mules remain unaware that they are participating in illegal activities due to gaps in financial literacy and critical thinking regarding digital transactions. Many individuals genuinely believe they are assisting with legitimate business operations, such as processing payments for an online store or helping someone manage finances, without understanding the underlying fraudulent schemes. This issue is especially prevalent among elderly individuals who may be less familiar with evolving digital threats and younger populations who lack comprehensive financial education. The rapid adoption of technology, without parallel growth in digital literacy, compounds this risk. Furthermore, language barriers and limited access to credible information sources can prevent individuals from recognizing red flags, making them more susceptible to manipulation. Enhancing public awareness through targeted educational programs and community outreach initiatives is crucial to bridging this knowledge gap and reducing the prevalence of mule account activities.[17]
4. **Cultural and social pressures**—Cultural norms and social dynamics play a significant role in influencing individuals to participate in mule activities, often without fully understanding the legal consequences. In tight-knit communities where interpersonal relationships and social cohesion are highly valued, fraud networks exploit these connections to establish trust and manipulate individuals. Peer pressure and familial obligations can create situations where refusing a request feels socially unacceptable, particularly in cultures that emphasize collectivism and respect for authority figures. For example, an individual may consent to letting a trusted family member use their bank account, believing it to be a harmless favor. This misplaced trust, combined with a lack of awareness about financial regulations, increases vulnerability to exploitation. Addressing these cultural factors requires not only legal deterrents but also community-based awareness programs that educate individuals on the risk of such seemingly innocuous actions.[18]
5. **Overreliance on digital platforms**—The growing dependence on digital banking and online platforms has inadvertently expanded the landscape for financial fraud. Fraudsters capitalize on the anonymity and vast reach of these platforms to recruit unsuspecting individuals as money mules without the need for face-to-face interactions.

LOOKING FOR MORE?

- Learn more about, discuss, and collaborate on risk in ISACA's Online Forums. *https://engage.isaca.org/onlineforum*

Victims are often enticed through seemingly legitimate job offers, investment opportunities, or social media connections, where the absence of traditional verification mechanisms makes it difficult to assess the authenticity of transactions. Moreover, the rapid pace of digital transactions reduces the window for critical reflection, increasing the likelihood of impulsive decisions driven by persuasive scams. This overreliance underscores the need for robust digital literacy programs and enhanced verification protocols within financial ecosystems to safeguard against such exploitation.[19]

By understanding the psychological and socioeconomic factors that contribute to mule account proliferation, stakeholders can develop more effective prevention strategies.

Addressing these vulnerabilities requires a multifaceted approach, including public education campaigns to raise awareness about financial scams, targeted interventions for vulnerable populations, and continuous training for bank employees to help them recognize signs of mule activity. By understanding the psychological and socioeconomic factors that contribute to mule account proliferation, stakeholders can develop more effective prevention strategies.

Case Study: Call Center Scam Crackdown

In 2025, Thai law enforcement successfully dismantled a large call center scam network operating across multiple provinces. This syndicate was responsible for defrauding more than 5,000 victims, causing financial losses exceeding THB฿1 billion.[20] The criminals used sophisticated social engineering tactics, posing as government officials and bank employees to convince victims to transfer funds into mule accounts.

Collaboration between financial institutions and regulatory bodies allowed the authorities to freeze more than 135,000 mule accounts and recover significant amounts of stolen money.[21] This case underscores the essential role of IT governance in enabling early detection, rapid response, and interagency cooperation to combat threats effectively. Financial professionals emphasize that the success of this operation was largely due to proactive data sharing protocols and the implementation of real-time fraud detection algorithms.[22]

A comparative example from Singapore showed similar success when law enforcement leveraged artificial intelligence (AI) to analyze transaction patterns, leading to the identification of more than 1,200 mule accounts within six months.[23] This cross-border perspective reinforces the importance of international cooperation in combating financial crimes.

Challenges in Managing Mule Accounts

Despite considerable technological advancements in fraud detection and regulatory compliance, several persistent challenges remain in managing mule accounts. One of the most pressing issues is the increasing sophistication of fraud techniques. Criminals continuously adapt by blending illicit transactions with legitimate financial activity, making it difficult for both automated systems and human analysts to distinguish between the two. These deceptive patterns often evade standard monitoring tools, requiring more advanced and adaptive technologies.

Cross-border activities further complicate enforcement efforts. As many mule transactions involve international accounts, they demand coordination among financial institutions and law enforcement agencies across multiple jurisdictions. These cross-border dynamics introduce inconsistencies in legal procedures, data-sharing protocols, and regulatory requirements—all of which can be exploited by organized crime networks.

In addition to technological and jurisdictional challenges, human factors persist. Many individuals unknowingly participate in mule activities, often manipulated by fraudsters through fake job offers or social engineering tactics. This lack of awareness makes it difficult to distinguish between intentional collusion and unintentional involvement. Ongoing public education and digital literacy campaigns are essential to reducing this risk.

Addressing these issues requires not only better alignment between regulatory bodies, but also ongoing dialogue and standard-setting at the global level.

Last, regulatory fragmentation across countries remains a major obstacle. The lack of harmonized legal definitions and enforcement mechanisms regarding mule accounts prevents seamless international cooperation. Addressing these issues requires not only better alignment between regulatory bodies, but also ongoing dialogue and standard-setting at the global level.

The Role of IT Governance

IT governance is not merely about policies and frameworks—it is about ensuring that technology actively supports an organization's security and risk management goals.[24] To that end, Thailand recently updated its regulatory measures. The Bank of Thailand (BOT) has announced an enhancement of measures to manage mule accounts and is promoting a shared responsibility approach among relevant parties.[25] Additionally, the BOT has introduced comprehensive anti-fraud measures aimed at strengthening the financial system's resilience against fraud risk, such as:[26]

1. **Intensifying the crackdown on mule accounts**—By tightening the criteria for identifying such accounts, considering additional factors such as transaction behaviors and amounts, the BOT can uncover evolving fraudulent activities. This allows banks to proactively suspend suspected mule accounts even without victim reports.
2. **Strengthening individual-level management**—Banks are required to extend the suspension of fund transfers and the denial of new account openings to include accounts deemed high-risk for being mule accounts, even if no damage has been reported. They must also prevent funds from entering any clearly high-risk mule accounts and alert senders that they might be transferring money to a mule account to prevent initial losses.
3. **Expanding collaborative management**—Banks must share lists of individuals exhibiting suspicious behaviors among themselves, even without victim reports, to enhance comprehensive and swift fraud prevention.

The BOT emphasizes that the sustainable resolution of financial fraud requires cooperation from all parties, including banks, telecommunications providers, relevant agencies, and the public, each fulfilling their responsibilities as clearly defined by regulators.

If any party neglects these duties, they may be held accountable and required to compensate for the resulting damages. The BOT will specify the responsibilities banks must uphold to assess accountability in cases of technological crime, in collaboration with other regulators.

To further strengthen the management of mule accounts, banks should consider:

- **Integrated monitoring systems**—Combining data from multiple sources offers a comprehensive view of account activities. Adopting emerging technologies (e.g., exploring the use of blockchain for transaction transparency, advanced biometrics) can ensure secure customer verification.
- **Continuous training**—Staff should be updated on the latest fraud techniques and IT security measures. Fraud tactics evolve rapidly, and training must evolve with them.
- **Cross-industry collaboration**—Working closely with regulators and international bodies to exchange insights will help improve detection capabilities. Public-private partnerships are becoming increasingly vital in the fight against financial crime.

Conclusion

Mule accounts remain a persistent threat to banks. However, robust IT governance frameworks focusing on risk management, data analytics, regulatory compliance, and incident response can significantly mitigate risk. As technology continues to evolve, so do the tactics of fraudsters, who find increasingly sophisticated ways to exploit digital platforms through methods such as social engineering and advanced phishing schemes.

Moreover, many individuals lack sufficient awareness of financial scams, which increases their exposure to deception. Real-life cases illustrate how easily people can be deceived by persuasive offers or urgent requests for money transfers. Industry experts highlight that such scams often succeed because they exploit psychological triggers such as fear and urgency, affecting even well-informed individuals.

Continuous improvements, public awareness campaigns, ongoing education, and strong collaboration with key stakeholders are critical to staying ahead of emerging threats. According to cybersecurity analysts, fostering a culture of security awareness within organizations and among the public is just as important as technological safeguards in mitigating fraud risk.

Continuous improvements, public awareness campaigns, ongoing education, and strong collaboration with key stakeholders are critical to staying ahead of emerging threats.

Two key questions remain: Are we evolving our defenses as rapidly as threats continue to evolve? And how can financial institutions strike a balance between customer convenience and anti-fraud measures? The answer lies not in choosing between speed and security, but in designing systems that support both. Proactive IT governance, supported by adaptive technologies and strong collaboration among stakeholders, can equip institutions to stay one step ahead. By embedding fraud awareness into everyday operations, both within organizations and in customer interactions, financial institutions can reduce risk without compromising user experience. The fight against mule accounts is ongoing, but with the right mindset and mechanisms, it is a challenge we are prepared to overcome.

Endnotes

1 The Economist, "How to Launder Ill-Gotten Gains," 10 September 2020, *https://www.economist.com/finance-and-economics/2020/09/10/how-to-launder-ill-gotten-gains*

2 United Nations Office on Drugs and Crime, "Estimating Illicit Financial Flows Resulting From Drug Trafficking and Other Transnational Organized Crimes," 2011, *https://www.unodc.org/documents/data-and-analysis/Studies/Illicit-financial-flows_31Aug11.pdf*

3 The Nation Thailand, "Over 135,000 Mule Accounts Suspended, 869 Suspects Arrested This Year," 15 April 2025, *https://www.nationthailand.com/news/general/40048808*

4 The Nation Thailand, "Over 135,000 Mule Accounts Suspended"

5 Money and Banking Online, "DE Has Suspended Mule Accounts," 3 February 2025, *https://moneyandbanking.co.th/en/2025/153688/*

6 US Federal Bureau of Investigation, "Money Mules," USA, *https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/money-mules*

7 US Department of Justice Civil Division, "Money Mule Initiative," USA, 21 October 2024, *https://www.justice.gov/civil/consumer-protection-branch/money-mule-initiative*

8 American Bankers Association, "Money Mule Scams," *https://www.aba.com/advocacy/community-programs/consumer-resources/protect-your-money/money-mules*

9 The Thai Bankers' Association, "Get to Know "Mule Accounts," the (Most) Dangerous Accounts With Extraordinary Punishment," 2023, *https://www.tba.or.th/en/%e0%b8%97%e0%b8%b3%e0%b8%84%e0%b8%a7%e0%b8%b2%e0%b8%a1%e0%b8%a3%e0%b8%b9%e0%b9%89%e0%b8%88%e0%b8%b1%e0%b8%81-%e0%b8%9a%e0%b8%b1%e0%b8%8d%e0%b8%8a%e0%b8%b5%e0%b8%a1%e0%b9%89%e0%b8%b2/*

10 Bank of Thailand, "Let's Build a 'Crypto Account' Shield," 15 April 2025, https://www.bot.or.th/th/research-and-publications/articles-and-publications/articles/article-20250415.html

11 Bank of Thailand, "Enhancing Financial Institutions' Policies and Operational Guidelines on Transactions With High-Risk Countries and Safeguarding Sanctions Risks," 30 December 2024, *https://www.bot.or.th/th/news-and-media/news/news-20241230.html*

12 Abhinash, "How India's Increasing Online Scams Are Threatening the Digital Landscape," GlobalVoices, 10 November 2023, *https://globalvoices.org/2023/11/10/how-indias-increasing-online-scams-are-threatening-the-digital-landscape/*

13 Siam Legal Thailand Law Library, "Mule Accounts and Financial Scams in Thailand," 2023, *https://library.siam-legal.com/mule-accounts-and-financial-scams-in-thailand/*

14 Li, C.; "Building Effective Defenses Against Social Engineering," *ISACA Now Blog*, 22 June 2023, *https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/building-effective-defenses-against-social-engineering*

15 World Bank Group, "Bridging the Gap: Inequality and Jobs in Thailand," 29 November 2023, *https://www.worldbank.org/en/country/thailand/publication/bridging-the-gap-inequality-and-jobs-in-thailand*

16 The Nation Thailand, "Job Seekers Beware: Platform Flags Thousands of Job Ads for Scams," 14 February 2025, *https://www.nationthailand.com/blogs/news/general/40046303*

17 *KPMG, Money Mules: FinCrime's Trojan Horse Unveiled*, 2024, *https://assets.kpmg.com/content/dam/kpmgsites/in/pdf/2024/07/money-mules-fincrimes-trojan-horse-unveiled.pdf*

18 TravelerTopia, "The Challenges of Thai Culture: Hidden Realities," 27 November 2024, https://travelertopia.com/culture/the-challenges-of-thai-culture-hidden-realities/

19 Krungthai, "Scammers Applying for Jobs Online May Fall Into an Mule Account," 13 September 2024, *https://krungthai.com/th/krungthai-update/announcement-detail/2952*

20 Khaosod English, "1,154 Fraud Victims Await Justice as Scammers Face Prosecution," 1 April 2025, *https://www.khaosodenglish.com/news/2025/04/01/1154-fraud-victims-await-justice-as-scammers-face-prosecution/* Reuters, "Thailand Arrests 100 People for Operating in Border Scam Centre," 5 March 2025, *https://www.reuters.com/world/asia-pacific/thailand-arrests-100-people-operating-border-scam-centre-2025-03-05/*

21 The Nation Thailand, "Over 135,000 Mule Accounts Suspended"

22 Bank of Thailand, "Media Briefing: BOT Raises Measures to Manage Mule Accounts and Pushes for Shared Responsibility Approach," 30 January 2025, *https://www.bot.or.th/content/dam/bot/documents/th/news-and-media/news/2025/news-th-20250130-attach1.pdf*

23 The Straits Times, "Police Investigate 312 Suspected Scammers, Money Mules Involved in Over 1,200 Cases," 26 June 2023, *https://www.straitstimes.com/singapore/police-investigate-312-suspected-scammers-money-mules-involve-in-over-1200-cases*

24 ISACA®, COBIT® Framework: Introduction and Methodology, USA, 2019, *https://www.isaca.org/resources/cobit*

25 Bank of Thailand, Guidelines on Information Technology Risk Management, 2023, *https://www.bot.or.th/content/dam/bot/fipcs/*documents/FOG/2566/ThaiPDF/25660202.pdf

26 Bank of Thailand, "The BOT has Further Enhanced Measures to Manage Mule Accounts and Pushed for Joint Responsibility," 2025, *https://www.bot.or.th/th/news-and-media/news/news-20250130.html*