



BANK OF THAILAND



PUEY UNGPHAKORN
INSTITUTE FOR
ECONOMIC RESEARCH

The Bangkok Blueprint in Action

Regional Experiences
and Policy Lessons
for Fraud-Resilient
Financial Services



The Bangkok Blueprint in Action: Regional Experiences and Policy Lessons for Fraud-Resilient Financial Services

Sommarat Chantararat, Thammarak Moenjak,
Nakarin Amarase, Kanyarat Suwannama, Thiti Tosborvorn

October 2026

This paper is a companion paper to the Bangkok Blueprint for Fraud-Resilient Financial Services, launched during the IMF–World Bank Group Annual Meetings 2026 in Bangkok. The findings, policy recommendations, and conclusions expressed in this paper do not necessarily reflect the views of the Bank of Thailand, the Puey Ungphakorn Institute for Economic Research, the International Monetary Fund (IMF) and the World Bank Group (WBG). The sole responsibility of this paper lies with the authors.

Contents

Executive Summary	1
I Introduction	2
II Stylized Facts of Cyber-Enabled Fraud	3
Stylized Facts of Cyber-Enabled Fraud in Thailand	6
From Key Characteristics to Core Policy Considerations	10
The Inevitable Policy Trade-offs	10
III The Bangkok Blueprint's Foundations of Fraud-Resilient Financial Services	11
IV From Principles to Practice: Regional Experiences and Policy Lessons	13
1. Establish Strategic and Legal Foundation	13
2. Strengthen the Fraud Mitigation Life Cycle	18
3. Leverage Existing Risk Mitigation and Enforcement Frameworks	26
4. Expand Domestic and Cross-Border Coordination and Cooperation	27
5. Promote Consumer Protection and Resilience	29
V Cross-Cutting Lessons Learned	33
VI Remaining Challenges and the Way Forward	34
VII Conclusions and Policy Takeaways	35
Notes	36
References	37

Boxes

BOX 1	Stylized Facts of Cyber-Enabled Fraud in Thailand	6
BOX 2	Thailand's Emergency Decree: From Enabling Law to Ecosystem-Wide Accountability	15
BOX 3	Shared Responsibility Frameworks: Scope, Trigger, and Allocation	17
BOX 4	Use of Central Intelligence Data in Thailand and Malaysia	20
BOX 5	Strengthening Mule-Account Management in Thailand	23
BOX 6	Managing the Trade-off between Early Response and Misdetection	24
BOX 7	The Reporting Bottleneck: Why Victims Stay Silent, and What Lowers the Cost of Speaking Up	25
BOX 8	FRONTIER+: Cross-Border Enforcement at the Speed of the Payment	29
BOX 9	Singapore's Multi-Layered, Behavioral Consumer Resilience Interventions	30
BOX 10	Hong Kong SAR's Comprehensive and Behavioral Consumer Education Program	32

Annexes

ANNEX I	Evolution of Anti-Fraud Strategies	40
ANNEX II	Governance Structure of National Fraud Strategy	45
ANNEX III	Mapping of Fraud Mitigation Taskforces	47
ANNEX IV	Multi-layered Interventions across the Fraud Life Cycle	49
ANNEX V	Broadening the Scope, Strengthening the Response: Thailand's Framework for Safeguarding the Financial Sector from Illicit Activities	54

Acknowledgements

The authors gratefully acknowledge the contributions of colleagues from the International Monetary Fund (IMF) and the World Bank Group (WBG), including Anca Paduraru, Ben Aldersey, Carine Chartouni, Dirk Jan Grolleman, Dorothee Delort, Erik Feyen, Gabriela Conde, Guillermo Alfonso Galicia Rabadan, Indulekha Thomas, Marianne Bechara, Michelle Morales, Nadine Schwarz, Puja Singh, and Tanai Khiaonarong, for their collaboration in the development of the Bangkok Blueprint for Fraud-Resilient Financial Services, which helped us frame the discussions in this paper.

We also thank colleagues from the Hong Kong Monetary Authority (HKMA) – Charlie Wong, Kyle Tong, Leo Hui, Nancy Chau, Sophia Lam, and Wyatt Tang; Bank Negara Malaysia (BNM) – Amalina Nabilah binti Rozlan, Julian Lim Wei Sheng, Muhammad bin Puwira Jaya, Muhammad Fikri bin Abdullah, Nor Halimaton Sa’adiah binti Abdul Halim, and Qaiser Iskandar bin Anwarudin; and the Monetary Authority of Singapore (MAS) – Huili Han, Rennie Soh, and Wenhua Chew – for generously sharing their jurisdictions’ policy and operational experiences, which enriched our comparative analysis.

We extend our appreciation to external reviewers Nualnoi Treerat (Chulalongkorn University), Krislert Samphantharak (University of California San Diego), Supot Tiarawut (Chairman of the Technology Committee, Siam Commercial Bank Public Company Limited), Supreecha Limpikanjanaowit (Integrated Channels Business Division Head, Kasikornbank

Public Company Limited) and Phitha Tanpairoj (Head of Products Division, Bank of Ayudhya Public Company Limited) for their expert insights and valuable comments.

At the Bank of Thailand (BOT), we are deeply grateful to Governor Vitai Ratanakorn; former Governor Sethaput Suthiwartnarueput; Deputy Governors Roong Mallikamas, Piti Disyatat, Suwannee Jatsadasak, and Daranee Saeju; and Assistant Governors Chayawadee Chai-anant and Sakkapop Panyanukul for their leadership and support.

We also thank BOT colleagues from the anti-fraud and fintech teams – Oramone Chantapant, Buncha Manoonkunchai, Pucktada Treeratpituk, Prim Bud-saratragoon, Yuwadee Jeamwattanasirikij, Songchai Ngermuen, and Thunyachad Roongsrisawad – for their guidance and operational insights, as well as Surasak Choedpasuporn and Amila Tochuendee from the Puey Ungphakorn Institute for Economic Research for their analytical support.

Finally, we extend our sincere gratitude to the experts and practitioners across the public and private sectors whom the team engaged throughout this research journey, sharing their time and insights across numerous occasions. From technical data analytics exchanges and expert consultation roundtables to engagements at the Bank of Thailand Symposium 2025, their collective perspectives and constructive feedback on earlier drafts greatly enriched this work.

Any remaining errors or omissions are the sole responsibility of the authors.

Abbreviations

ADA	Anti-Deception Alliance	FS-ISAC	Financial Services Information Sharing and Analysis Center
ADCC	Anti-Deception Coordination Centre	GASA	Global Anti-Scam Alliance
AMLO	Anti-Money Laundering Office	HKMA	Hong Kong Monetary Authority
AOC	Anti-Online Scam Operation Center	HKPF	Hong Kong Police Force
APP	Authorized Push Payment	IMCS	Inter-Ministry Committee on Scams
ASEAN	Association of Southeast Asian Nations	IMDA	Infocomm Media Development Authority
BNM	Bank Negara Malaysia	MAS	Monetary Authority of Singapore
BOT	Bank of Thailand	MCMC	Malaysian Communications and Multimedia Commission
CAD	Commercial Affairs Department	MDES	Ministry of Digital Economy and Society
CCB	Commercial Crime Bureau	MLAT	Mutual Legal Assistance Treaty
CCIB	Cyber Crime Investigation Bureau	NBTC	National Broadcasting and Telecommunications Commission
CCID	Commercial Crime Investigation Department	NFCC	National Anti-Financial Crime Centre
CFR	Central Fraud Registry	NFP	National Fraud Portal
COSMIC	Collaborative Sharing of Money Laundering/Terrorism Financing Information and Cases	NSRC	National Scam Response Centre
CSA	Cyber Security Agency of Singapore	OFCA	Office of the Communications Authority
CSTCB	Cyber Security and Technology Crime Bureau	OCHA	Online Criminal Harms Act
DSI	Department of Special Investigation	OTP	One-Time Password
EMEAP	Executives' Meeting of East Asia-Pacific Central Banks	PDPA	Personal Data Protection Act
ETDA	Electronic Transactions Development Agency	PDRM	Polis Diraja Malaysia (Royal Malaysia Police)
FAST	Fast and Secure Transfers	RTP	Royal Thai Police
FATF	Financial Action Task Force	SEC	Securities and Exchange Commission
FIU	Financial Intelligence Unit	SFC	Securities and Futures Commission
FINEST	Financial Intelligence Evaluation Sharing Tool	SPF	Singapore Police Force
FMLIT	Fraud and Money Laundering Intelligence Taskforce	SPOC	Single Point of Contact
		SRF	Shared Responsibility Framework
		TBA	Thai Bankers' Association
		TCSC	Technology Crime Prevention and Suppression Center

Executive Summary

Digital finance has not only expanded access, efficiency, and financial inclusion, but it has also enabled cyber-enabled fraud to operate at unprecedented scale, speed, and sophistication. As stronger controls have reduced unauthorized fraud, many jurisdictions are increasingly confronting authorized fraud, where victims are manipulated through deception and social engineering into initiating transactions themselves.

The Bangkok Blueprint for Fraud-Resilient Financial Services, launched during the IMF-World Bank Group Annual Meetings 2026 in Bangkok, establishes a common strategic framework organized around twelve Key Considerations under five pillars. This paper complements the Blueprint by drawing practical lessons from how Hong Kong SAR, Malaysia, Singapore, and Thailand implement some of the operational measures that came to be embodied in the Bangkok Blueprint's principles. While institutional models vary, their experiences reveal common operational mechanisms and priorities.

Several cross-cutting lessons emerge. Building fraud resilience requires strong leadership and comprehensive legal foundations. Decisive leadership is essential to synchronize an ecosystem-wide defense across financial and non-financial sectors. Crucially, statutory and supervisory frameworks must allocate responsibility and liability across actors to align prevention incentives, mandate secure information sharing, and grant authorities adequate intervention powers, while remaining agile as criminal tactics shift.

Given the extreme speed and scalability of fraud, prevention and early intervention are vastly more cost-effective than downstream response and recovery. Yet because no single tool suffices, defenses require

multi-layered safeguards across the fraud life cycle – pairing advanced technology against cyber threats with behavioral design to intercept authorized fraud. Crucially, operational speed remains decisive: real-time interventions must halt illicit flows before instant payment rails disperse them.

Centralized intelligence and shared expertise build vital data-driven capacity against systemic fraud.

System-wide data sharing overcomes reporting blind spots, elevating institution-level monitoring into collective defense. Beyond centralized infrastructure, stakeholders must collaboratively strengthen analytical capabilities to detect illicit networks and emerging threats in real time.

Collaboration and collective action will be key.

Integrating counter-fraud measures with anti-money laundering and combating the financing of terrorism (AML/CFT) and anti-illicit regimes enhances effectiveness, dismantling criminal networks and financial incentives. Concurrently, domestic public-private partnerships and structured international cooperation enable coordinated intelligence sharing to dismantle global syndicates and strengthen cross-border defenses.

Policymakers must navigate critical trade-offs to ensure balanced policy objectives.

Strict controls must not create inconvenience, disrupt commerce, or exclude less digitally literate users, nor can data sharing compromise privacy boundaries. Crucially, prioritizing cost-effective, high-value recovery must not sacrifice distributional fairness, leaving small-scale victims without redress.

This paper also highlights ongoing challenges, emphasizing continuous collective learning toward safe, inclusive financial services.

Introduction

Cyber-enabled fraud poses a growing risk to digital finance. Regional experiences, read alongside the Bangkok Blueprint, chart a course toward fraud-resilient financial services.

Digital finance has transformed access to financial services, improving efficiency, convenience, and financial inclusion through fast payments, digital identity, and mobile platforms. Yet these same technologies have created new opportunities for cyber-enabled fraud. Fast payments and interconnected ecosystems allow fraud to be conducted at greater scale and speed, challenging traditional prevention, detection, and recovery mechanisms. Ensuring digital finance remains both innovative and safe has become a central policy priority.

One of the most significant risks arising from this transformation is cyber-enabled fraud. As stronger authentication controls have reduced unauthorized fraud, jurisdictions face a rapid surge in authorized fraud, where victims are socially engineered into initiating transactions themselves. Beyond direct financial loss, this inflicts emotional harm and erodes trust in digital finance. Asian economies are disproportionately exposed, accounting for 67% of estimated global scam losses in 2024 (Global Anti-Scam Alliance & Feedzai, 2024) – reflecting universal digital adoption paired with increasingly sophisticated criminal networks.

Recognizing these challenges, the Bangkok Blueprint for Fraud-Resilient Financial Services was launched during the 2026 IMF – World Bank Group Annual Meetings in Thailand. The Blueprint provides a common framework for strengthening resilience through twelve Key Considerations organized under five pillars: (i) strategic and legal foundations, (ii) strengthening the fraud-mitigation life cycle, (iii) leveraging existing risk and enforcement frameworks, (iv) expanding domestic and cross-border coopera-

tion, and (v) promoting consumer protection and resilience.

This paper complements the Blueprint by illustrating how these principles can be implemented in practice. Drawing on experiences from Hong Kong SAR, Malaysia, Singapore, and Thailand, it examines cyber-enabled fraud characteristics, identifies practical lessons, policy trade-offs, cross-cutting implications, and remaining challenges for authorities.

The four jurisdictions provide valuable perspectives. While all face severe fraud exposure, their institutional responses diverge: Hong Kong SAR demonstrates how an international financial hub manages fraud prevention and detection through a multi-strata fraud prevention and response ecosystem; Malaysia demonstrates centralized rapid response integrating police, banks, and telcos; Singapore offers lessons from a mature digital ecosystem where combating scams and fraud is a top-tier national priority, with concerted efforts across detection, prevention, recovery, and education; and Thailand reflects statutory safe harbors enabling rapid cross-sector intervention amid universal fast-payment adoption. This implies that while resilience goals are universal, implementation pathways must reflect national circumstances.

Together, the Bangkok Blueprint and this paper are designed to support continued learning, adaptation, and international collaboration. By pairing a shared policy framework with practical implementation experience, they support policymakers in building digital financial ecosystems that are innovative, inclusive, resilient, and trusted.

Stylized Facts of Cyber-Enabled Fraud

The dynamics of cyber-enabled fraud are shifting, and with them the fundamental policy trade-offs. Navigating those trade-offs is what operationalizing a fraud-mitigation framework demands.

Cyber-enabled fraud¹ refers to the use of digital technologies and psychological manipulation to obtain illicit gains across transactions involving actors within or outside the financial sector. Over the past decade, rapid digital transformation has fueled cyber-enabled fraud across financial services, nearly tripling the number of cases (Khiaonarong & Zheng, 2026). These figures likely underestimate the true scale of the threat, as reporting mechanisms remain rudimentary and underreporting is pervasive (Global Anti-Scam Alliance & Feedzai, 2025). Despite these data constraints, global and national estimates consistently point to substantial and rapidly mounting losses.²

The nature of cyber-enabled fraud has shifted from unauthorized breaches to authorized fraud. While unauthorized fraud involves transactions executed without customer consent, authorized fraud – predominantly APP fraud – manipulates legitimate account holders into initiating and approving transfers themselves. In recent years, as baseline cybersecurity hardened technical perimeters, criminal syndicates pivoted toward authorized schemes, weaponizing telecommunications, SMS phishing (smishing), e-commerce, and social media platforms to induce irreversible payments.

Global data confirms this structural divergence: while unauthorized fraud has steadily declined, APP fraud has surged to unprecedented levels. Annual global losses to fraud have surpassed USD 442 billion, with APP fraud accounting for the vast majority (Global Anti-Scam Alliance & Feedzai, 2025).

Asia has emerged as the global epicenter of cyber-enabled fraud, bearing over 67% of worldwide fraud losses in 2024. Driven by rapid mobile banking adoption and real-time payment infrastructure, exposure is exceptionally high across Asia's leading digital economies. Survey-based estimates put annual economic losses at 0.2% of GDP in Hong Kong SAR, 2.1% in Malaysia, 0.5% in Singapore and 0.6% in Thailand (Global Anti-Scam Alliance & Feedzai, 2025; World Bank, 2024). However, most survey-based ratios exceed those derived from official reported losses,³ pointing to potential underreporting in the other three jurisdictions.

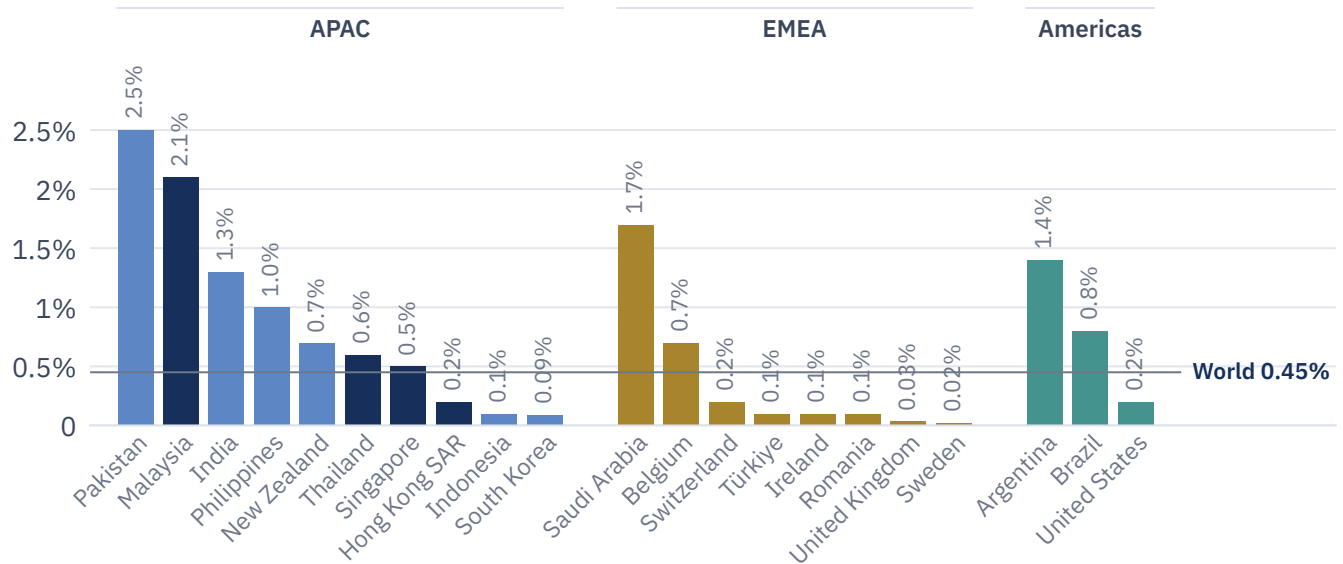
The landscape of cyber-enabled fraud risk varies across the four jurisdictions. (See Annex I for a summary of the fraud journey and the evolution of anti-fraud strategies in the four jurisdictions.)

Hong Kong SAR's fraud landscape spans cross-border channels and multiple financial institutions. Phishing scams account for only 6% of reported cases, while purchase fraud constitutes the largest fraud category. Fraudsters commonly use social media platforms, instant messaging applications, fraudulent websites, and impersonation techniques to establish credibility before requesting payment. High cross-border connectivity makes pre-transaction counterparty identification the critical operational control point before funds move across jurisdictions.

Malaysia's fraud profile is distinguished by the prominence of impersonation frauds, which account for 32% of reported cases, slightly exceeding purchase

FIGURE 1 Asia suffers the highest fraud losses globally

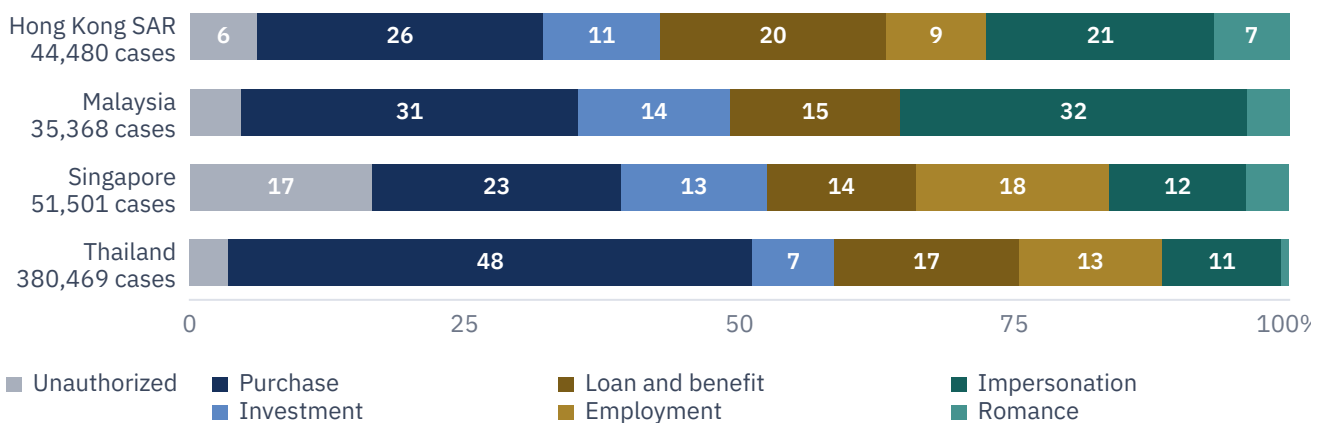
Economic losses of fraud worldwide (% of GDP)



Note: Authors' calculations based on the GASA Global State of Scams 2025 survey (approximately 46,000 adults across 42 markets, nationally weighted), measuring self-reported gross scam losses over the preceding 12 months for countries with available data.

FIGURE 2 Varying fraud profiles across jurisdictions

Share of fraud cases by type in 2024 (%)



Note: Hong Kong Police Force, Royal Malaysia Police, Singapore Police Force, Thai Police Online. Hong Kong SAR's "Loan and benefit" encompasses credit card scams, fraud involving Comprehensive Social Security Assistance, insurance scams, street deception, etc. Also, "Purchase", "Impersonation" and "Unauthorized" correspond to Hong Kong SAR's "online shopping", "telephone deceptions", and "phishing", respectively. Malaysia's report does not single out employment fraud cases.

frauds at 31%. Fraud commonly originates through phone calls, messaging applications, and social media platforms before funds are routed through domestic financial institutions and mule-account networks. The increasing use of real-time payments compresses response windows and elevates the importance of rapid intervention.

Singapore has experienced a pronounced shift toward APP fraud, though unauthorized cases remain comparatively elevated at 17% of reports. Losses span diverse typologies – chiefly government impersonation, investment, and employment scams – exploiting messaging apps, social media, and phone calls. Given robust institutional defenses, the primary vulnerability is no longer technical, but the manipulation of consumer decision-making.

Thailand's fraud landscape is characterized by the near-complete dominance of APP fraud, with unauthorized transactions representing only 3% of reported cases. Driven by pervasive e-commerce, purchase frauds comprise nearly half of all incidents. Fraudsters exploit social media, messaging apps, and phone calls, rapidly funneling proceeds through PromptPay mule networks into digital assets or offshore accounts within minutes – severely compressing recovery windows.

Cyber-enabled fraud has evolved into a systemic policy challenge for three main reasons:

1. **When social engineering and advanced technology combine, they enable highly tailored**

fraud to operate at unprecedented scale, speed, and agility, making attacks easier to execute and far harder to combat. While psychological manipulation allows fraudsters to tailor schemes across demographic profiles so that “there is fraud for everyone,” data-driven targeting, generative AI, deepfakes, and automated “fraud-as-a-service” platforms drastically lower the barriers to mass deception (Financial Action Task Force et al., 2023). When coupled with instant payment rails, illicit funds disperse across automated mule networks within seconds, easily outpacing manual intervention and legacy controls.

2. **Its cross-sector and cross-border nature exposes the fragmentation of policy and regulatory frameworks.** Fraud spans several sectors – from banking, payments and investments to telecommunications, social media, and e-commerce – and crosses national borders, yet oversight remains largely siloed, reactive, and insufficient. Because fraud proceeds can move across accounts and borders within minutes, swift and coordinated cross-industry action is essential to trace and recover funds and freeze fraud-related accounts.
3. **The rise of cyber-enabled fraud erodes public trust in digital finance, payment systems, and public institutions.** This growing trust deficit in turn undermines the effectiveness of fraud mitigation and further threatens safe and inclusive digital finance.

Stylized Facts of Cyber-Enabled Fraud in Thailand

Understanding what distinguishes cyber-enabled fraud from traditional fraud is essential for designing targeted mitigation policy. Ranking among the most fraud-prone jurisdictions globally due to deep fast-

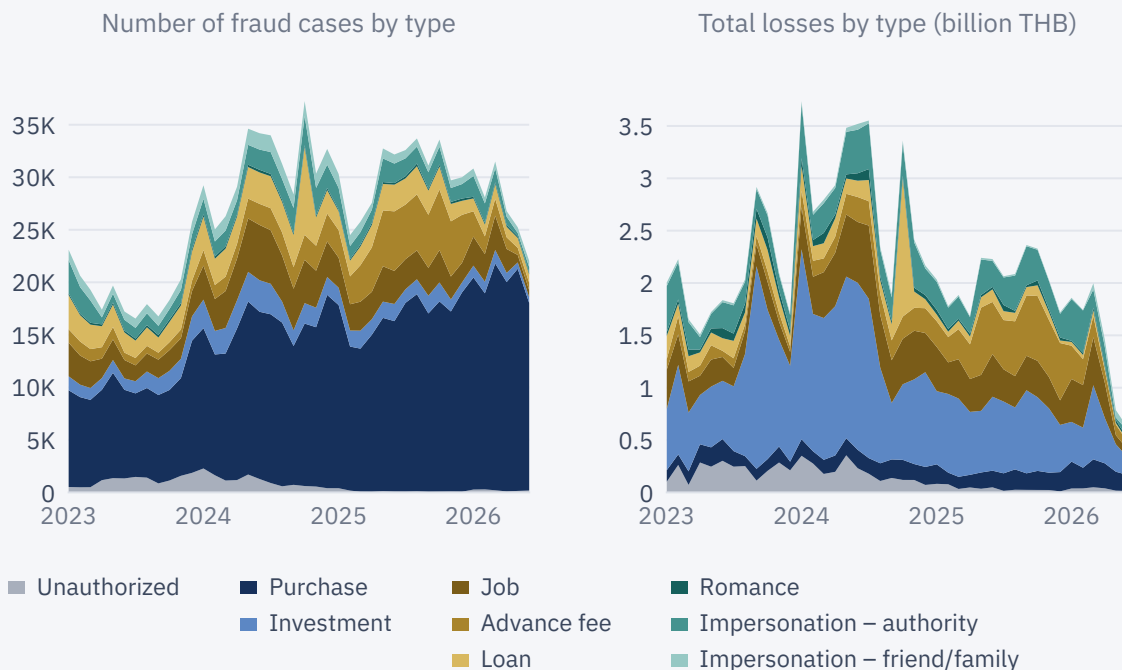
payment penetration, Thailand mirrors broader global trends. Box 1 draws on national survey data, police reports, and Central Fraud Registry (CFR) transaction data to outline these key stylized facts.

BOX 1 Stylized Facts of Cyber-Enabled Fraud in Thailand

Thailand's rapid adoption of fast payments (PromptPay), e-commerce, and social media has been accompanied by a sharp rise in cyber-enabled fraud. This box draws on Thai Police Online records (January–August 2025), transaction-level data from the Central Fraud Registry (CFR) (Tosborvorn et al., 2026), and a nationally representative survey of 6,973 individuals (Hapipat, 2024) to highlight key features of Thailand's fraud landscape.

- 1. APP fraud dominates the fraud landscape.** Social engineering has made legitimate payment rails the primary vehicle for fraud. Within APP fraud, frequency and severity differ markedly: purchase scams account for more than half of reported cases but only 7.3% of losses, while investment scams represent just 5.1% of cases yet generate roughly one-third of total losses.

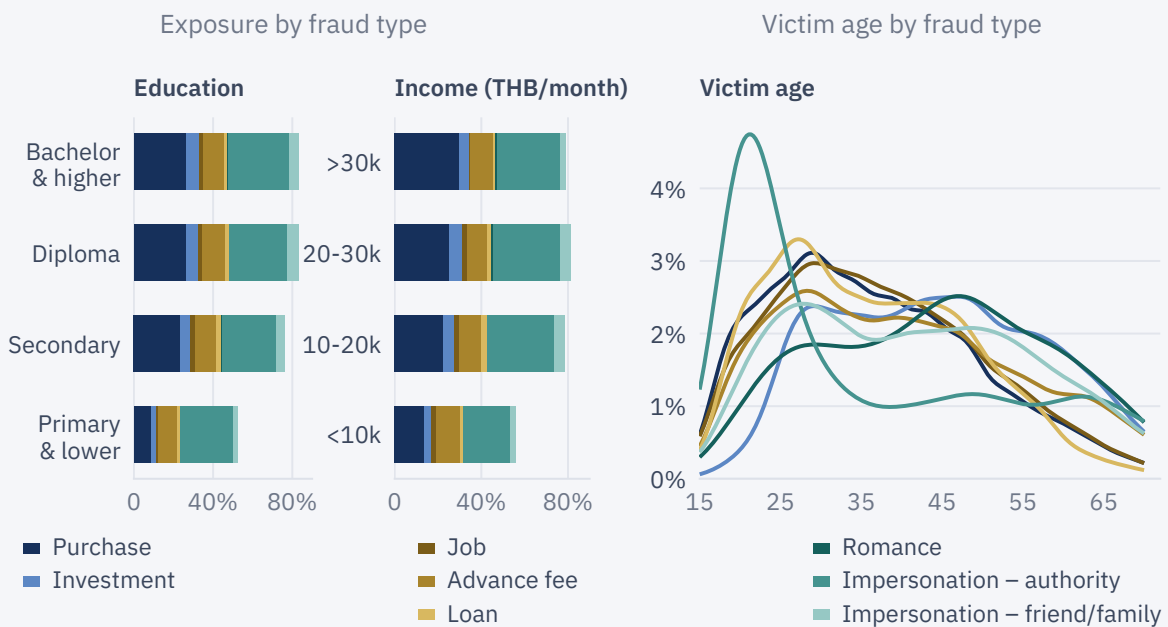
The rise of APP and decline of unauthorized frauds



Note: Data from Thai Police Online between January 2023 and June 2026 (excluding non-cybercrime cases).

- 2. There is fraud for everyone.** Fraud exposure is near-universal, but vulnerability is highly segmented. Survey data shows that 73.4% of respondents encountered fraud and 34.5% suffered financial losses, yet only 11.4% reported them. Contrary to common perceptions, exposure is highest among more digitally engaged users, particularly those with higher education and middle-to-upper incomes. Different fraud types also target different vulnerabilities: impersonation scams are concentrated among younger adults, purchase and credit scams among individuals in their twenties, and investment scams among middle-aged groups. **The implication is clear: effective fraud prevention requires targeted interventions rather than a one-size-fits-all approach.**

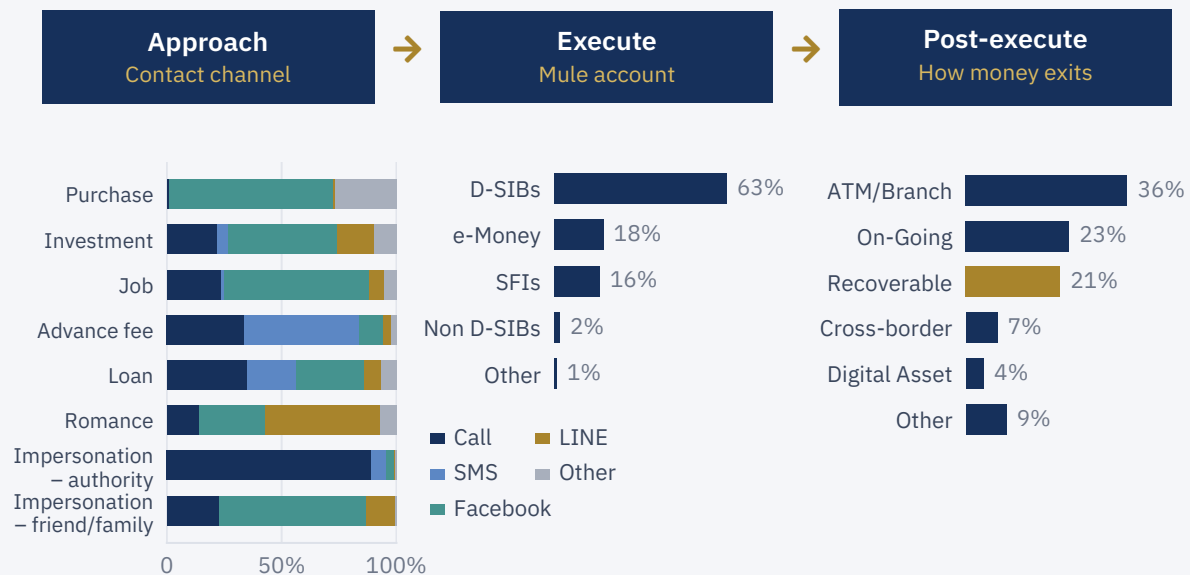
Fraud exposure is near-universal, but vulnerability is highly segmented



Note: (a) Data from the survey in Hapipat (2024). Exposure is the portion of respondents in that group who answer “Yes” to the question: “Have you ever experienced being approached or scammed by fraudsters through online channels or call center (regardless of whether you suffered any actual loss or not)?” (b) Data from Thai Police Online for APP fraud cases reported between January–August 2025.

- 3. Fraud is cross-sector, cross-border, and multi-channel.** Criminals exploit seams across banks, telecoms, e-commerce, and social media platforms. Contact channels mirror fraud types – phone calls drive impersonation (89%), while social media fuels purchase and romance scams. Proceeds disperse rapidly through bank mules (62.9%) and e-wallets (17.9%), with 36% cashed out at ATMs alongside crypto and offshore leakage, asset recovery reaches only 21%.

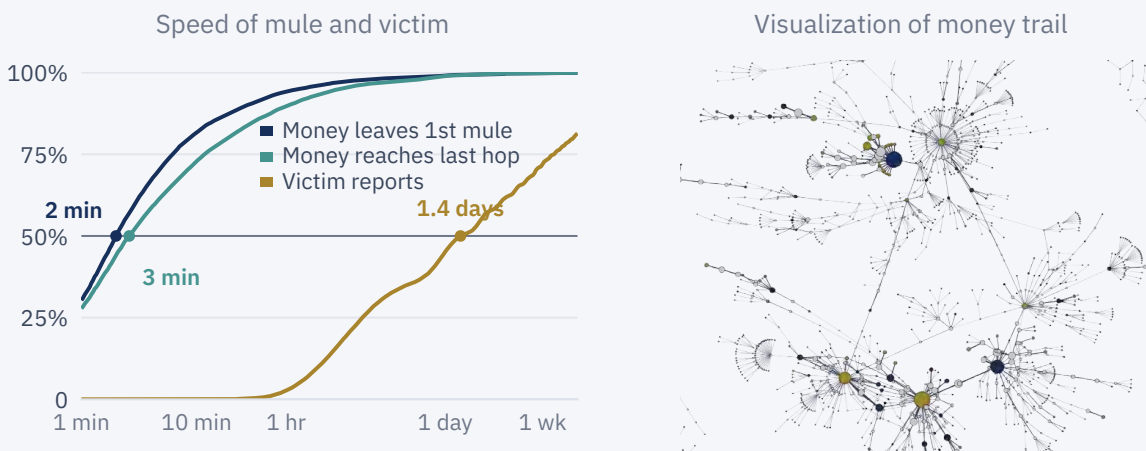
Multi-channel and cross-sector nature of fraud throughout the life cycle



Note: (a) Hapipat (2024), victim-reported channels. (b–c) CFR (February 2026). “Other” accounts include digital-asset exchanges, bill payments and payment facilitators. Cross-border share omits ATM and digital-asset. “Recoverable” is frozen before exit. D-SIBs: Domestic Systemically Important Banks; SFIs: Specialized Financial Institutions.

4. Fraudsters operate with extreme speed and scalable network operations. Instant payment systems create a stark mismatch between the speed of laundering and the speed of detection. Stolen funds leave first-layer mule accounts within a median of two minutes, and half exit the banking system within three minutes, while victims typically take 30 hours to report. Transaction data reveal highly organized mule-account networks that rapidly aggregate and disperse proceeds across multiple layers, creating a severe timing disadvantage for recovery efforts.

Half of the illicit funds leave the system in less than three minutes through a sophisticated and scalable network, while it takes more than a day for victims to report half of the losses to the police

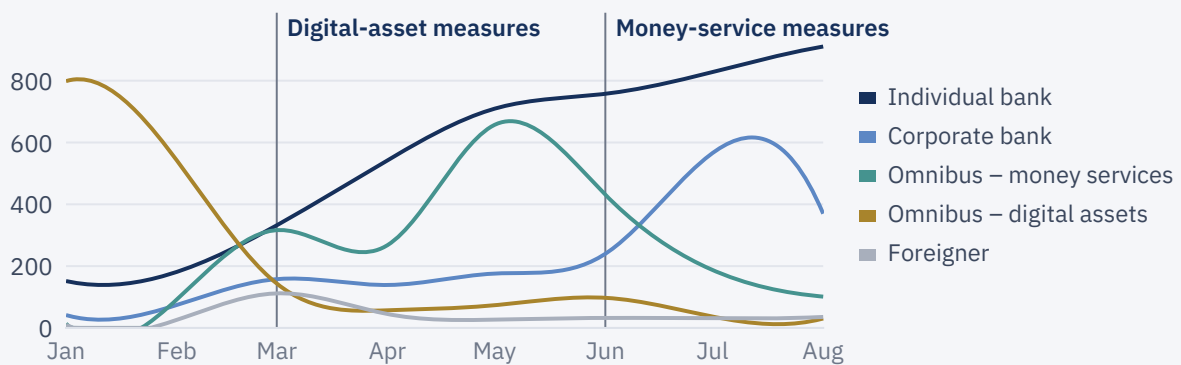


Note: CFR, APP cases (January–August 2025). (a) Cumulative share of stolen funds, by value. (b) Illustrative; nodes are accounts (navy = victim, grey = mule, gold = exit), sized by transaction volume.

- 5. Fraudsters are highly adaptive and agile.** Concealment channels shift rapidly to circumvent regulatory friction. In Thailand throughout 2025, terminal accounts evolved in lockstep with policy interventions. When digital-asset omnibus accounts were curbed in March, illicit flows shifted to money service providers; when non-bank channels were restricted in June, they moved again to corporate bank accounts. Meanwhile, flows to individual accounts for ATM cash-outs rose steadily.

Concealment of fraud money changes in response to new policies

Total losses by type of terminal account (million THB)

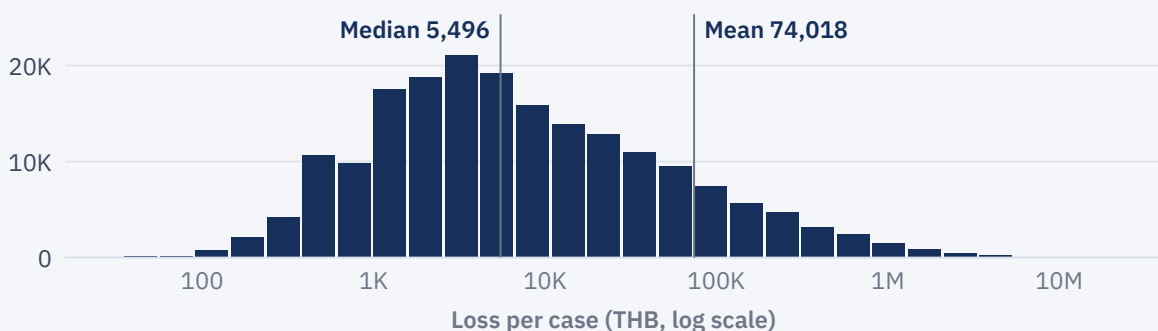


Note: Thai Police Online data (January–August 2025; includes unauthorized cases). A “terminal account” denotes the final traceable account where interbank money trails terminate. In March 2025, digital-asset measures imposed 24-hour settlement holds for new users, withdrawal caps, and transfer delays. In June 2025, money service providers were integrated into the CFR to extend intra-service fund tracing.

- 6. Fraud losses are highly concentrated.** Fraud exhibits an extreme bimodal distribution. The top 5% of cases drive over 70% of total losses, even when severe reporting bias masks a long tail of micro-losses. Policy frameworks must pair high-value asset interdiction with accessible, low-friction redress for micro-losses, which disproportionately harm lower-income and vulnerable cohorts.

Fraud losses are highly skewed

Distribution of fraud losses



Note: Data from the CFR for cases reported between January–August 2025, excluding unauthorized cases.

From Key Characteristics to Core Policy Considerations

Drawing on the stylized facts from Thailand, five core characteristics emerge that reflect common vulnerabilities and dynamics shared across jurisdictions.

1. **The shift toward authorized fraud.** Policy must move beyond standard cybersecurity perimeters and generic awareness campaigns to mandate risk-based behavioral safeguards that strengthen customer resilience at the point of authorization.
2. **Universal exposure, segmented vulnerability.** Policy must establish baseline safeguards for all users while deploying escalated, risk-based protections for segments identified as highly susceptible.
3. **Multi-channel, cross-sector, and cross-border.** Effective policy demands a whole-of-society approach anchored in cross-sector and interna-

tional cooperation to eliminate gaps and secure the weakest links across the entire ecosystem and fraud life cycle.

4. **Speed, scalability, and adaptability driven by technology.** This implies that prevention and early intervention are far more cost-effective than downstream recovery. Policy frameworks must operate at real-time speed – balancing agile disruption of evolving threats with safeguards against false positives and operational errors.
5. **Skewed and concentrated fraud incidence.** To ensure fairness, response and recovery frameworks must address both ends of this spectrum – pairing specialized asset tracing for severe harms with streamlined, low-friction redress for widespread micro-losses.

The Inevitable Policy Trade-offs

These core characteristics highlight three fundamental trade-offs that policymakers must navigate in implementing fraud mitigation measures.

1. **Security vs. convenience, efficiency, and inclusion.** Countering machine-speed, instant payment rail fraud requires aggressive friction and automated intervention, which inevitably slows legitimate commerce, triggers false positives, and risks excluding less digitally literate users.
2. **Data sharing vs. privacy.** Closing the cross-sector and cross-border seams exploited by fraudsters demands real-time intelligence sharing across

financial and non-financial institutions, which could undermine data protection standards and user privacy.

3. **Cost-effectiveness vs. distributional fairness.** Given an extreme loss skew, optimizing enforcement resources for high-value recovery yields the greatest financial return but leaves vulnerable, small-scale victims without redress.

Navigating these inevitable trade-offs is a central consideration as policymakers translate fraud-mitigation principles into operational practice.

The Bangkok Blueprint's Foundations of Fraud-Resilient Financial Services

Five foundational pillars carry the Bangkok Blueprint's approach to fraud resilience, built on an end-to-end mitigation life cycle spanning prevention, detection, and response and recovery.

The fraud mitigation life cycle serves as the foundational framework for systemic resilience, orchestrating core interventions – prevention, detection, and response and recovery – across the three stages of cyber-enabled fraud. During approach and preparation, interventions focus on disrupting enabling vectors across telecommunications and digital (e-commerce and social media) platforms before funds move. During execution, defenses aim to detect and intercept illicit transfers across payment rails in real

time. During post-execution, response and recovery mechanisms enforce rapid account freezes, trace diverted assets, and deliver fair consumer redress.

Building on international standards and frameworks, the Bangkok Blueprint establishes a five-pillar framework for fraud-resilient digital finance, integrating the mitigation life cycle – prevention, detection, and response and recovery – into a whole-of-ecosystem approach across five pillars:



1. Establishing strategic and legal foundations.

Because cyber-enabled fraud creates systemic vulnerabilities, an effective response requires a unified national strategy with clear stakeholder responsibilities and strong coordination. This should be supported by a comprehensive legal, regulatory, and supervisory framework that enables effective oversight, consumer protection, liability allocation across financial and non-financial actors, secure information sharing, and timely asset freezing and recovery.

2. Strengthening the fraud mitigation life cycle.

Ecosystem resilience depends on an end-to-end approach spanning prevention, detection, response, and recovery. Prevention should be built into fraud-resilient system design and reinforced through intelligence-led controls, real-time information sharing, and advanced technologies. Detection requires institution-level monitoring supported by shared intelligence and coordinated analytics. These capabilities should be complemented by rapid response, investigation, and recovery arrangements to contain fraud, remediate harm, and recover assets.

3. Leveraging existing risk mitigation and enforcement frameworks. The national fraud strategies can build on existing frameworks, such as cyber-security and AML/CFT regimes, which already

help protect the financial system from exploitation by criminals. For example, the AML/CFT frameworks provide preventive measures, such as customer identification requirements, alongside enforcement tools that help deter fraud, disrupt criminal networks, and remove the financial incentives that sustain fraudulent activity.

4. Expanding domestic and cross-border cooperation and coordination. Existing financial sector collaboration should extend beyond traditional boundaries to enable shared intelligence, aligned responsibilities, and coordinated action across public and private stakeholders, including through public-private partnerships. Given the transnational nature of cyber-enabled fraud, structured cross-border cooperation and information sharing are also essential to support coordinated prevention, detection, response, recovery, and enforcement across jurisdictions.**5. Promoting consumer protection and resilience.** Authorities can build upon existing consumer protection frameworks, supervisory tools, complaints mechanisms, and redress arrangements, while updating them where necessary to address cyber-enabled fraud. Consumer awareness and empowerment are equally important to help users understand fraud risks, available safeguards, and applicable liability and redress mechanisms, and to respond effectively when fraud occurs.

From Principles to Practice: Regional Experiences and Policy Lessons

Operationalizing the Bangkok Blueprint demands tailoring its principles to local contexts. Implementation across four jurisdictions yields practical policy lessons.

Operationalizing the Bangkok Blueprint requires tailoring its high-level principles to domestic contexts, reflecting differences in legal frameworks, digital payment behavior and development, and fraud threat profiles. In practice, policymakers must navigate complex trade-offs among security, efficiency, convenience, financial inclusion, and data privacy – meaning no single institutional or operational model fits every jurisdiction.

This section draws on how four jurisdictions implemented some of the operational measures that came to be embodied in the Bangkok Blueprint’s principles. The four jurisdictions provide valuable comparative perspectives. While all have experienced rapid digitalization and significant exposure to cyber-enabled fraud, jurisdictions have prioritized different policy tools and implementations given varying fraud contexts. Hong Kong SAR highlights how an international financial hub combats fraud through a multi-layered ecosystem of intelligence sharing, coordinated alerts, customer protection measures, and public education; Malaysia demonstrates the

power of integrating police, banks, and telcos into a centralized rapid-response center for fund recovery; Singapore offers lessons from a mature digital ecosystem where combating scams and fraud is a top-tier national priority, with concerted efforts across detection, prevention, recovery, and education; and Thailand reflects the use of statutory safe harbors to enable rapid, cross-sector interventions amid universal adoption of fast payments and social platforms.

Drawing on the diverse experiences of the four jurisdictions, this section presents key implementation lessons to assist policymakers in operationalizing the Bangkok Blueprint’s five pillars within their specific legal, institutional, and technological contexts. It highlights variations in governance and regulatory designs, good practical examples, persistent operational gaps, and policy trade-offs, providing actionable takeaways to assist authorities in establishing adaptive, ecosystem-wide anti-fraud frameworks.

1 Establish Strategic and Legal Foundation

A sound legal and strategic foundation is essential for an effective anti-fraud regime. While governance structures inevitably vary according to current institu-

tions and domestic legal traditions, implementation reveals common strategic priorities.

1.1 Effective whole-of-ecosystem governance frameworks share four common characteristics.

These are (1) high-level leadership, (2) clearly defined responsibilities and liabilities across public and private stakeholders, (3) cross-sector data and intelligence sharing, and (4) legal mechanisms enabling coordinated, expedited intervention (see Annex II for details of national anti-fraud governance structures across the four jurisdictions along these four dimensions).

- **Hong Kong SAR** coordinates joint leadership between the Hong Kong Police Force (HKPF) and Hong Kong Monetary Authority (HKMA) across government agencies, regulators, and law enforcement. Public-private operations are institutionalized via the Anti-Deception Alliance (ADA) and HKMA's multi-strata framework across banks, sectoral coordination, and customer touchpoints. Intelligence is pooled through Scameter,⁴ FMLIT, and FINEST, while the Banking (Amendment) Ordinance 2025 establishes statutory safe harbors for rapid interbank sharing and fund interdiction.
- **Malaysia** implements multi-agency coordination through the National Scam Response Centre (NSRC), a joint arrangement involving the National Anti-Financial Crime Centre (NFCC), Bank Negara Malaysia (BNM), the Malaysian Communications and Multimedia Commission (MCMC), the Royal Malaysia Police (RMP), financial institutions, and the telecommunications industry. This coordination is supported by the National Fraud Portal (NFP), an end-to-end automated platform from handling of scam reports to tracing of stolen funds across the financial system.
- **Singapore** drives whole-of-government leadership via the Inter-Ministry Committee on Scams (IMCS), which coordinates operational roles across the Singapore Police Force (SPF), Monetary Authority of Singapore (MAS), Infocomm Media Development Authority (IMDA), and industry. Intelligence is

pooled through ScamShield and Anti-Scam Command bank co-location, backed by statutory tools (OCHA, Protection from Scams Act 2025, and the Shared Responsibility Framework). Interestingly, Singapore structures this governance oversight directly around the four stages of the fraud life cycle – Prevent & Block, Detect & Report, Enforce & Recover, and Public Education – eliminating silos and enforcing end-to-end accountability.

- **Thailand** anchors high-level leadership in the statutory committee established under the Emergency Decree on Technology Crime Prevention and Suppression. This framework enforces cross-sector duties across banks, payment service providers, digital-asset operators, telcos, and social media platforms – integrating real-time fund tracking via the CFR while empowering rapid account freezes, direct Anti-Money Laundering Office (AMLO)-led asset restitution, and shared responsibility regimes under the amended Decree.

1.2 Legal and regulatory frameworks must establish clear responsibility and liability allocation across all actors in the ecosystem.

The framework should also extend necessary statutory powers to eliminate regulatory arbitrage and align incentives across financial and non-financial institutions.

- **Jurisdictions anchor anti-fraud authority either by layering targeted statutes onto existing frameworks or by enacting dedicated omnibus legislation.** Hong Kong SAR, Malaysia, and Singapore augment established regimes with targeted statutes – such as Hong Kong SAR's amended Banking Ordinance for interbank data sharing, Malaysia's Penal Code and Online Safety Act 2025, and Singapore's OCHA and Protection from Scams Act. In contrast, Thailand relies on an omnibus statutory framework via its Emergency Decree to enforce ecosystem-wide duties under a single unified regime.⁵

BOX 2 Thailand's Emergency Decree: From Enabling Law to Ecosystem-Wide Accountability

Why a Decree? Pre-2023 legal barriers prevented pre-complaint account freezes and cross-sector intelligence sharing. Constitutional emergency powers bypassed 12–18 months of legislative lag, establishing immediate statutory mandates for proactive intervention.

The decree introduced in 2023 designated MDES as national lead, criminalized mule accounts and SIMs, and authorized 72-hour pre-complaint bank holds. It also launched the CFR and the 24/7 AOC 1441 operations center. In 2025, Amendment No. 2 extended statutory duties to telcos, digital-asset operators, and social media platforms. It introduced shared liability for negligence, compliance safe harbors, and fast-track administrative asset returns via AMLO.

How does the Decree enforce ecosystem-wide duties? Replacing voluntary cooperation with binding accountability, the decree unifies the entire fraud life cycle into an integrated operational defense.

1. COORDINATED LEADERSHIP & GOVERNANCE

Designate MDES as executive coordinator: Statutory lead aligning policy and cross-sector anti-fraud operations.

UNIFIED REGULATORY ALIGNMENT ACROSS AUTHORITIES

BOT Banking and payments	NBTC Telcos and SIM controls	SEC Crypto and digital assets	AMLO Asset recovery and return	RTP/DSI Police and law enforcement
------------------------------------	--	---	--	--

CENTRALIZED OPERATIONAL TASKFORCE: AOC 1441

24/7 multi-agency co-location 24/7 war room co-locating police, banks, and AMLO analysts.	Unified intake and instant case ID Single 1441 hotline: instant case IDs and immediate downstream holds.	Real-time freezing protocols Minutes-level interbank freezes, bypassing manual court delays.
---	--	--

2. ECOSYSTEM-WIDE RESPONSIBILITY, MANDATES, AND ALIGNED INCENTIVES

Shared responsibility: Civil liability for baseline security failures. **Statutory safe harbors:** Legal immunity for good-faith freezes and sharing.

ECOSYSTEM MANDATES STRUCTURED ACROSS THE FRAUD LIFE CYCLE

APPROACH	EXECUTION	POST-EXECUTION
Telcos - Real-time SMS and phishing filter 3-SIM cap; shut rogue SIM boxes	Banking and payments 72-hour pre-complaint holds on alert - Section 7 recursive mule freezes	Law enforcement (CCIB) - Expedited warrants and prosecution - Transnational syndicate raids
Social media platforms - Mandatory advertiser KYB checks - Fast takedown of fake ads and pages	Digital-asset operators - Screen wallets against blacklists - Restrict P2P off-ramps and freeze	AMLO (asset restitution) - Asset seizure without court delay - Fast summary restitution to victims

3. UNIFIED DATA AND INTELLIGENCE SHARING

1 Safe harbor to share

- Overrides secrecy and PDPA
- Full immunity for data sharing

2 Central Fraud Registry (CFR)

- National ITMX graph analytics
- Predictive in-flight mule scoring

3 Cross-sector AOC data lake

- Links accounts to MSISDN and crypto
- Synchronized sector deactivations

The Decree thus drives an adaptive regulatory perimeter, allowing authorities to issue immediately enforceable rules without legislative delays. This progressive perimeter targeted bank mule accounts (2023), telecom vectors (2024–2025), and digital assets with online ad platforms (2025–2026) to combat fraud in time.

- **Shared responsibility frameworks are increasingly adopted to incentivize ecosystem-wide security investments.** Malaysia, Singapore, and Thailand have each developed distinct approaches to allocating liability and strengthening incentives for fraud prevention. Malaysia emphasizes shared accountability, with losses allocated according to the degree of fault. As an additional safeguard, banks' controls must be assessed first and reinforced by independent review if customers are to bear the losses. Singapore's Shared Responsibility Framework (SRF) establishes a defined "waterfall" approach assigning discrete duties to financial institutions and telecommunications operators for phishing scams. Thailand's amended Emergency Decree imposes proportional statutory responsibility across a broad ecosystem of financial and non-financial entities. Thus, all three regimes condition liability on compliance, but diverge in scope, triggers, and loss sharing – trading off victim protection against moral hazard, operational feasibility, and legal certainty. In addition to the existing safeguards for unauthorized transactions, Hong Kong SAR is also considering a responsibility framework for APP frauds.

1.3 Clear statutory gateways and safe harbors are essential to enable cross-sector data sharing.

While data protection laws such as the Personal Data Protection Act (PDPA) safeguard personal privacy,

legal uncertainty and confidentiality concerns often deter institutions from proactively exchanging actionable fraud intelligence without explicit statutory protection.

- **Statutory safe harbors remove legal barriers to information sharing by shielding institutions from liability when exchanging risk-relevant data in good faith.** Regional precedents reflect this mechanism across diverse architectures: Hong Kong SAR's Banking (Amendment) Ordinance 2025 provides legal protection for banks sharing intelligence, facilitating interbank data sharing via FINEST (Box 4); Malaysia's Financial Services Act 2013 allows sharing of information between banks enabling automated money trail and mule tracking via the National Fraud Portal; and Thailand's Emergency Decree exempts banks, payment service providers, digital-asset operators, and telcos from privacy and confidentiality liabilities when contributing to the CFR.

1.4 National strategies must remain adaptive to enable rapid policy pivots.

- **National strategies must operate as living frameworks anchored by agile governance structures, continuous learning, dynamic intelligence sharing, and public-private operational coordination.** Hong Kong SAR's FMLIT provides one example through a three-tier architecture:

BOX 3 Shared Responsibility Frameworks: Scope, Trigger, and Allocation

Why share liability? Shared-responsibility frameworks seek to provide predictable redress while allocating losses to the parties best placed to prevent them.

Three design choices, four approaches. Frameworks differ in their scope, trigger, and allocation of liability. Hong Kong SAR holds banks liable for unauthorized losses unless the customer acted fraudulently or with gross negligence; Malaysia applies a joint liability approach between banks and customers; Singapore follows a waterfall approach, placing full liability on the party that failed to meet its obligations; and Thailand uses proportional loss-sharing.

JURISDICTION	SCOPE	TRIGGER	ALLOCATION
Framework in force	Who is covered, and which fraud	What moves liability off the customer	Who bears how much
Hong Kong SAR HKMA Supervisory Policy Manual, Oct 2024 STATUTORY GUIDELINE	Only unauthorized transactions Banks and personal customers; business customers by contract	No customer fraud or gross negligence E.g. failing to safeguard devices or passwords	Customer bears no direct loss Otherwise liable in full if customer fraud, or assessed case-by-case if gross negligence
Malaysia BNM policy document, Oct 2024 SUPERVISORY POLICY	Only unauthorized transactions Banks and their customers	Gaps in the bank's own controls Checked before customer conduct; 14-day outcome	Shared liability for joint culpability cases Otherwise shared fairly; no cap; disputes to ombudsman
Singapore Shared Responsibility Framework, Dec 2024 REGULATORY FRAMEWORK	Phishing scams only Banks, e-wallets, telcos; other scams excluded	Breach of a prescribed duty Waived if all duties are met	Full liability on the breaching party Bank or e-wallet first, then telco; disputes to FIDReC
Thailand Emergency Decree 2023, amended Apr 2025 STATUTE	All technological crimes All payments; banks, PSPs, digital assets, telcos, platforms	Breach of regulator-set standards May be waived based on proof of compliance	Proportional to involvement Courts decide disputes; no cap

Designing a Shared Responsibility Framework: Key Trade-offs

- 1. No single best model.** Different fraud risks and legal systems require different combinations of scope, triggers, and loss allocation.
- 2. Too much liability creates friction.** Strong reimbursement obligations can lead to more controls, delays, and customer inconvenience.
- 3. Too little liability creates inertia.** Weak accountability reduces incentives to invest in prevention.
- 4. Good frameworks align incentives.** The goal is to make prevention more attractive than reimbursement.

a Strategic Group setting macro priorities, an Operations Group generating case-based tactical intelligence, and an Alert Function Group disseminating emerging fraud types and red flags across

financial institutions. This institutionalizes a continuous feedback loop between policy, frontline operations, and industry-wide controls as threats evolve.

2 Strengthen the Fraud Mitigation Life Cycle

Strengthening fraud resilience requires an integrated multi-layered approach across the entire mitigation life cycle, spanning prevention, detection, response, and recovery. Regional experience highlights policy lessons for operationalizing this end-to-end life cycle (see Annexes III–IV for an outline of fraud mitigation taskforces and interventions across the fraud life cycle in the four jurisdictions).

2.1 Prevention and early intervention are far more cost-effective than downstream recovery, especially in fast-payment environments.

Evidence from Thailand shows illicit funds disperse across mule networks within minutes (Tosborvorn et al., 2026). Countries thus need to combine effective detection and prevention, coordinated mechanisms, and lawful restriction powers to ensure pre-emptive, system-wide interventions throughout the fraud life cycle.

- **Ecosystem-wide investment in upstream prevention delivers the highest returns by intercepting fraud at first contact, yet critical gaps persist across communication networks, social media platforms, and consumer touchpoints.** Closing these vulnerabilities requires mandating proactive safeguards across four core lines of defense:

- **Telecommunication (telco) gateway controls:** Mandate operators to eliminate inbound attack vectors before contact occurs – including blocking spoofed SMS sender IDs, filtering malicious URLs, and deregistering unauthorized

SIMs and VoIP channels (e.g., Singapore’s SMS Sender ID Registry, Hong Kong SAR’s SMS Sender Registration Scheme, and Thailand’s NBTC SIM verification rules).

- **Social media platform gatekeeper obligations:** Impose statutory obligations on search engines and social media platforms to verify commercial advertisers, pre-screen financial promotions, and execute rapid takedowns of fraudulent accounts (e.g., Singapore’s Online Criminal Harms Act, Malaysia’s Online Safety Act 2025, and Thailand’s Emergency Decree provisions).
- **Financial institution dual-track safeguards:** Pair technical perimeter integrity to stop unauthorized fraud (embedding anti-malware shields and hardware-bound biometrics over SMS OTPs) with behavioral friction to intercept authorized fraud through targeted contextual prompts that break psychological urgency, structural cooling-off delays on high-value transfers or credential changes, and self-defense ring-fencing via a user-activated Money Lock feature that isolates core deposits from digital rails even if credentials are compromised (more in 2.2 and see Annex IV for detailed interventions across jurisdictions).
- **Consumer behavioral resilience:** Reinforce technical barriers with ongoing user empowerment and targeted behavioral friction to mitigate social engineering vulnerabilities before transaction initiation (more in Pillar 5).

Despite these initiatives, bridging the incentive divide between banking and non-financial gatekeepers remains an ongoing challenge. While financial institutions face direct financial risk, telcos and platforms lack commercial incentives to curb scam traffic without legal compulsion. While jurisdictions are actively attempting to close this enforcement gap through targeted statutory interventions, these frameworks remain works in progress and have yet to fully stem upstream vulnerabilities.

- **Effective fraud response requires a coordinated, round-the-clock architecture that deploys escalating interventions to match varying levels of victim susceptibility.** To intercept fast-payment flows before dispersal, Hong Kong SAR's Anti-Deception Coordination Centre (ADCC) co-locates police with participating banks of ADA to expedite identification and interception of crime proceeds and identify potential victims, who are contacted and provided with anti-deception advice through the Upstream Scam Intervention (Annex III).

2.2 Fraud mitigation frameworks must counter the behavioral dynamics of APP fraud.

- **Mitigating APP fraud requires layered safeguards and deliberate friction across product design, prevention, and response,** spanning the following operational tiers:
 - **Pre-commitment controls:** Empower users to ring-fence savings against digital transfer (e.g., Singapore's Money Lock, Hong Kong SAR's branch-unlocked Money Safe, and Malaysia's emergency kill switch).
 - **Decision-moment frictions:** Disrupt psychological urgency through real-time threat prompts (Hong Kong SAR's Suspicious Account Alert, Malaysia's SemakMule), mandatory cooling-off periods for new devices (Singapore, Malaysia), holds on large-value transfers resulting in draining of accounts (Singapore), biometric step-

ups (Singapore, Thailand's biometric thresholds for transfers exceeding THB 50,000), and face-to-face verification before release of protected funds (Hong Kong SAR's Money Safe).

- **Statutory interventions:** Enforce protective restrictions and expedited freezing when fraudulent transactions are underway, such as police-issued Restriction Orders halting victim banking under Singapore's Protection from Scams Act, immediate 72-hour administrative freezes under Thailand's Emergency Decree, expedited police account-freezing powers under Malaysia's Criminal Procedure Code (Section 116D), and safe harbors for institutions acting on shared intelligence under Hong Kong SAR's Banking (Amendment) Ordinance 2025.
- **A comprehensive APP fraud framework requires a dynamic APP fraud monitoring system to address evolving fraud typologies.** For example, in Hong Kong SAR, the HKMA mandates banks to maintain effective APP monitoring systems, adapting to the latest fraud trends and typologies and external intelligence on suspicious accounts. In May 2026, for instance, the HKMA, jointly with the HKPF and the Securities and Futures Commission (SFC), introduced a series of measures to combat online investment scams, including issuance of investment scam risk indicators and recommended customer enquiry methods to banks, as well as expanded use of the SFC's "alert list" by banks.

2.3 Collaborative data sharing and collective analytics form the operational core of effective fraud detection.

- **Jurisdictions must combine shared infrastructure with multi-sector intelligence to eliminate information silos.** In Thailand, the CFR consolidates fraud reports and money trails across commercial banks, payment service providers, and digital-asset exchanges. Financial institutions then integrate this intelligence directly into

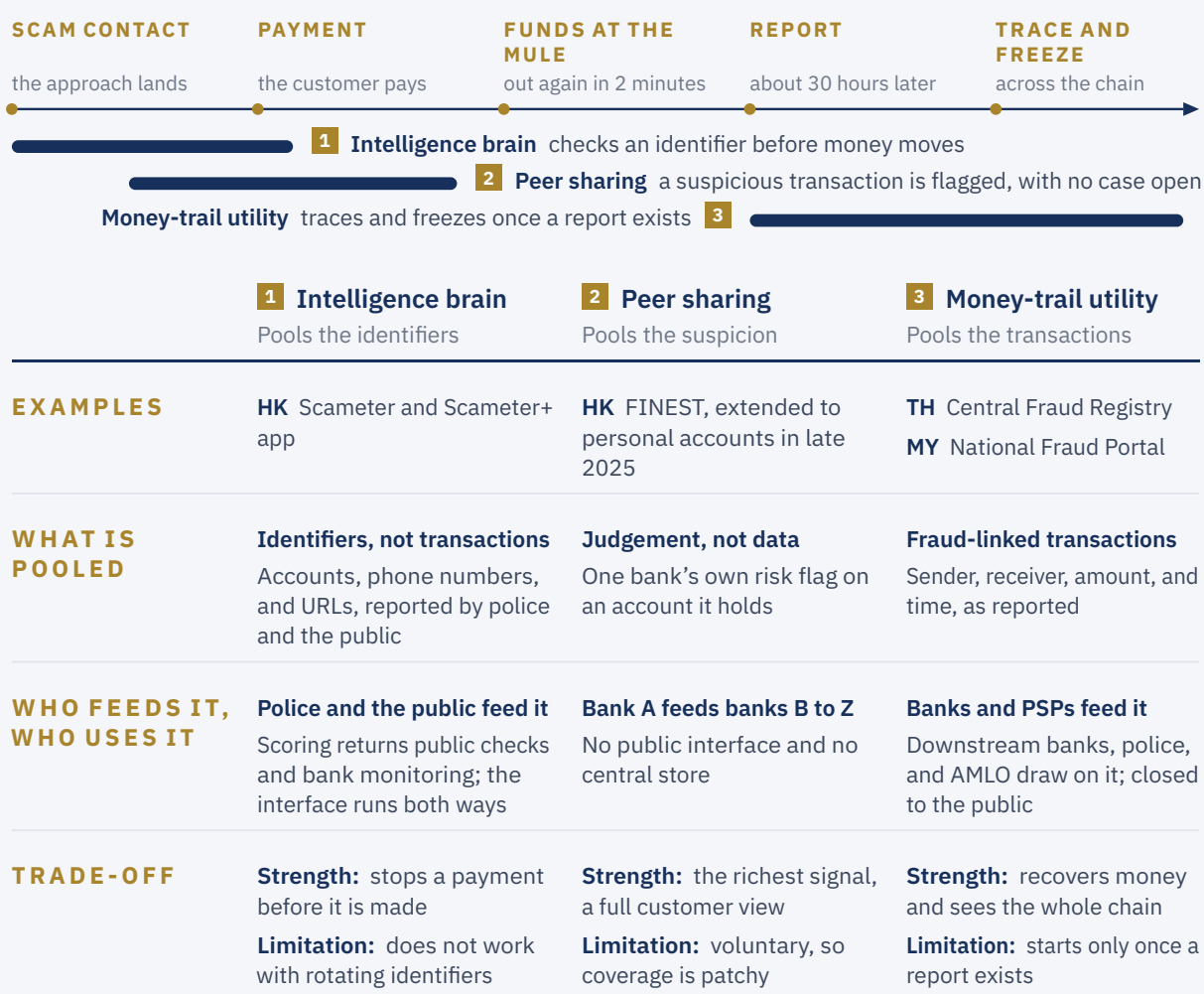
their real-time transaction monitoring, ensuring fraud patterns detected anywhere immediately strengthen defensive controls everywhere. The CFR is also being uplifted through application programming interface (API) based integration, enabling faster, more automated data exchange between participating institutions.

- **Challenges remain in closing data-sharing gaps, particularly beyond the financial sector.** Informa-

tion sharing with telecommunications operators, e-commerce platforms, and social media companies is often constrained by missing legal gateways, weak incentives, inconsistent data standards, and uneven technical capabilities. Cross-border exchange remains even more difficult, hampered by divergent regulatory frameworks and reliance on slow formal legal requests rather than pre-established operational arrangements.

BOX 4 Use of Central Intelligence Data in Thailand and Malaysia

Why pool intelligence? In Thailand's CFR, 84% of victim-to-mule transfers cross institutional boundaries, meaning no institution sees the full transaction chain. Intelligence sharing is therefore essential. The key design choices are what data to share, who can access it, and how to use it to inform intervention. The four jurisdictions illustrate three different approaches.



Key trade-off: Transaction-level sharing offers the strongest tracing and recovery capabilities, while indicator-sharing and peer-sharing are easier to implement and support prevention.

Example of Proactive Fraud Mitigation in Thailand: the BOT, Thai Bankers' Association, National ITMX, and Technology Crime Prevention and Suppression Center (TCSC) are developing an AI-driven Fraud Score using CFR and payment data to identify potential victims, mule accounts, risky transactions, and suspicious devices. Because most fraud flows cross institutional boundaries, the shared score enables participating institutions to verify, delay, or block high-risk transactions earlier.

In Malaysia: Once a victim's report is lodged with the National Scam Response Centre (NSRC 997), the National Fraud Portal (NFP), operated by the national payment network PayNet, automatically generates the trail of stolen funds across institutions, flags suspicious accounts for validation, and records the action each institution takes. The NFP is now being embedded with predictive analytics and AI models to pre-empt suspicious flow patterns and potential mules before funds move.

EXISTING MEASURES: RULE-BASED

1 Inside one bank



Victim to mule, and mule to mule

A bank identifies **potential victims** and **potential mules** among its own customers, starting from accounts already reported as mules and applying rule-based criteria.

- A potential victim is warned before the next transfer leaves
- A potential mule is restricted under the Box 5 measures

2 Across institutions



Expanded scope of action

National ITMX, which operates the Central Fraud Registry, traces the accounts at *other* institutions that a reported mule account has paid or been paid by, and notifies those institutions to act.

- Reach no longer stops at the bank that holds the mule account
- One report can trigger warnings and restrictions system-wide

FRAUD SCORING MODEL

A dynamic, model-based score replaces fixed rules, reading transactions or account usage for abnormal behavior rather than for a match.

- Scores an account or a transaction, not a completed case
- Adapts as patterns change

WHAT THE SCORE IS BUILT ON

Data held inside an institution

- Basic transaction data
- Historical transfer behavior and customer profile
- ATM and mobile-banking app usage

Data shared between institutions

- PromptPay payment transactions
- Central Fraud Registry fraud cases

Data from outside the payment record

- Device and location signals
- Further sources as the model is extended

Note: National ITMX is Thailand's national payment infrastructure provider and the operator of the Central Fraud Registry. Source: Bank of Thailand, Thai Bankers' Association, National ITMX, and TCSC.

- **Authorities must harness shared data and advanced analytics to drive proactive, scalable anti-fraud interventions.** In Thailand, once a mule account is flagged in the CFR, the national switch (National ITMX) traces connected nodes across banks, allowing them to issue real-time warnings to potential victims and freeze potential mules before funds disperse. Scaling these interventions relies on the CFR identifying critical network hubs across the system. Furthermore, transitioning to a dynamic, interbank fraud scoring model – combining PromptPay flows, CFR intelligence, and behavioral telemetry – enables authorities to detect abnormal activity, pinpoint high-risk hubs early, and scale proactive warnings before transfers clear (Box 4). Box 5 further illustrates how payment rails are used to detect and dismantle mule-account networks, preemptively applying tiered restrictions to disable fraudsters and intercepting illicit funds before they leave the banking system in Thailand.

2.4 At the core of early intervention is managing the critical trade-off between rapid fund containment and misdetection risk, safeguarding long-term public trust in digital payments.

Acting on early suspicion inevitably increases false positives, which can trigger cash flight if recourse is absent. Restrictions must therefore be swiftly reversible. Box 6 illustrates this using the case in Thailand, where automated mule suspensions initially impacted innocent merchants.

2.5 Fraud mitigation must balance inclusion, risk-tailored design, and equitable recovery.

- **Security safeguards must be inclusively designed to prevent excluding vulnerable populations.** Complex controls often disadvantage elderly and less digitally literate users. Baseline protections should remain intuitive and free of charge. Singapore

illustrates this by pairing no-cost features like Money Lock and kill switches with in-branch support and public education on anti-scam features, safeguarding users without compromising access.

- **Tailoring safeguards through customer risk profiling enhances protection while minimizing friction for legitimate commerce.** Uniform limits often disrupt normal users without stopping fraud. In Hong Kong SAR, banks allow customers such as the elderly to adjust ATM withdrawal and e-banking debit limits, and to disable high-risk e-banking functions such as online increases to fund transfer limits and online registration of third-party payees. In Thailand, consumer profiling measures allow banks to implement dynamic transfer caps based on transaction patterns and demographic risk. This delivers dual benefits: shielding vulnerable groups (such as the elderly) from executing large fraud transfers and restricting rapid outbound velocity on accounts prone to mule recruitment, including youth and students.
- **Response and recovery mechanisms must operate equitably across all loss levels.** Because investigative and enforcement resources are finite, recovery efforts often skew toward high-value cases, leaving retail victims of smaller frauds with little to no redress. To optimize resource allocation and maintain broad public confidence, jurisdictions must implement automated, threshold-based fast-track procedures that streamline fund freezing and restitution for high-volume, low-value incidents.

2.6 Overcoming reporting bottlenecks is critical to unlock network-wide fraud intelligence.

Fraud reporting creates positive network externalities by exposing mule accounts and strengthening collective intelligence. Yet reporting remains low globally because private friction and stigma far outweigh the perceived private benefit of fund recovery.

BOX 5 Strengthening Mule-Account Management in Thailand

Mule accounts are the plumbing of cyber-enabled fraud: they are where a victim's money lands and, within minutes, where it leaves (Box 1). Since 2023 Thailand has tightened mule-account management on three axes at once: who may flag an account, what is restricted, and what is shared, with each step closing a route the previous one had left open.

Thailand's mule-account measures, 2023–2025

	DETECTION CRITERIA	ACTIONS	DATA SHARING
	Who may flag an account, and on what	What the flag restricts	What is shared, and how far it travels
2023	AMLO reports, and nothing else One account at a time, named in the report 	Block Electronic channels closed on AMLO's instruction	Account level The flagged account travels, and nothing attached to it
2024	Risk-based color codes Three AMLO tiers graded by risk, and a light brown code the bank raises itself    	Withdrawal and onboarding Block withdrawals, and refuse the holder a new account	Individual level The holder, not only the account the report named
2025 First quarter	Additional brown codes Two further tiers, raised on the bank's own detection  	Inflow and warning Block incoming deposits, and alert those who have sent to the account  Report to police	Across the banking industry Holder level, for the cases a bank reports to police 
2025 Second to fourth quarter	Juristic entities An AMLO report may now name the company or its directors, not only an individual Beyond the banks Coverage extends to digital-asset and e-money accounts	One standard across operators The same mule-account measures for banks, e-money issuers, and digital-asset operators	Across operators Digital assets and e-payment join the exchange

Note: the horse marks the color code by which a suspected mule account is graded. Black and the two greys are AMLO's tiers; the browns are raised by a bank's own detection, the light brown from 2024 and the dark brown from 2025. Unit of restriction, trigger, and perimeter each widened in turn. Source: Bank of Thailand.

What the three movements share is direction: each widened the perimeter a unit at a time, from an account to its holder to the entity behind it, from an AMLO referral to a bank's own suspicion, and from the banks to the operators the money had moved to.

Making risk measurable. The color codes are also a common scale, so supervisors can compare mule-account risk across institutions and over time. As the perimeter widens and the trigger moves earlier, rapid resolution for accounts flagged in error matters correspondingly more (Box 6).

BOX 6 Managing the Trade-off between Early Response and Misdetection

The stress test. In September 2025, expanding fund-tracing downstream swept in legitimate users at scale: merchants whose high-frequency QR receipts matched flagging profiles, and unwitting minors tricked into forwarding illicit deposits. As false positives mounted, merchants posted “cash only” signs and suspended QR acceptance, prompting a visible retreat toward cash.

The correction: engineering the release side. An inter-agency “war room” (MDES, BOT, AMLO, TBA, CCIB, and CIB) rapidly retooled operational protocols. Suspensions were restricted to the disputed amount rather than entire accounts, reserving full seizures for court orders. Authorities committed to unblocking verified innocent holders within four hours, instituted proactive clearance without requiring formal complaints, narrowed flagging strictly to directly connected accounts, and centralized appeals through AOC 1441.

The recurrence – and the preventive turn. Despite operational fixes, youth mule cases surged 70% by early 2026, causing over THB 185 million in losses. Rather than relying on ex-post freezes, the BOT and TBA introduced ex-ante safeguards: daily transfer caps tiered by age band (THB 3,000 / THB 5,000 / THB 10,000), effective from 1 October 2026 for banks and 1 November 2026 for e-money providers. Calibrated to leave over 97% of young users unaffected while permitting parental overrides, this substituted proportionate guardrails for disruptive freezes.

Lessons learned. The converged lesson across jurisdictions: broad-based, pre-emptive freezes maintain public trust and financial system integrity only when release is engineered as deliberately as interdiction—through amount-specific holds, defined time bounds, essential-needs carveouts, a single appeal channel, and strict metrics for the release clock.

- **Policies must lower reporting barriers, enhance private returns, and highlight the positive externalities of public disclosure.** Jurisdictions minimize friction by expanding intake beyond traditional police desks. Malaysia exemplifies this by embedding the Royal Malaysia Police within its NSRC 997 hotline, enabling intake reports to serve directly as formal police reports to eliminate duplicative filings. Crucially, linking multi-channel intake directly to real-time inter-bank fund interception boosts recovery prospects, transforming reporting into a high-value action for victims. Highlighting how individual reports fuel network-level syndicate disruption further reinforces reporting incentives.

2.7 Using technology to fight technology: Harnessing shared infrastructure and adaptive defenses to level the playing field.

- **Leveraging shared verification utilities eliminates information asymmetries and prevents illicit entry.** Shared infrastructure provides an authoritative trust anchor over fragmented proprietary checks. In Singapore, banks are allowed to rely on national registries via Singpass Face Verification to authenticate high-risk transactions, such as the setup of new digital tokens, establishing a high-assurance onboarding barrier that curtails synthetic identity fraud and impersonation.

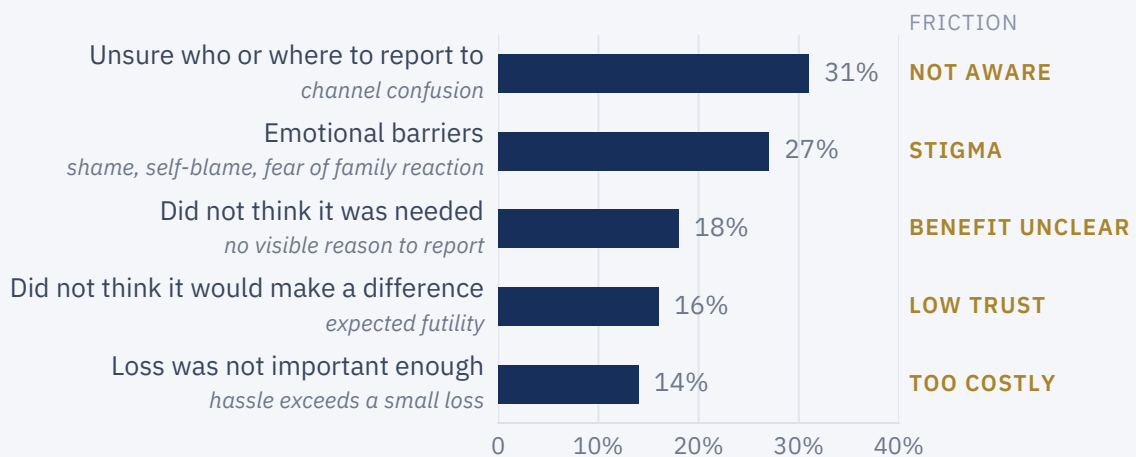
BOX 7 The Reporting Bottleneck: Why Victims Stay Silent, and What Lowers the Cost of Speaking Up

Reporting is a public good, and victims tend to under-supply it. Funds often leave mule accounts within minutes, while victims may take hours to report (Box 1). For most victims, reporting does little to recover their own losses, but it helps protect future victims by enriching shared intelligence systems such as Thailand’s CFR, Hong Kong SAR’s Scameter and ADCC, and Malaysia’s National Fraud Portal (Box 4). Because the benefits largely accrue to others, underreporting is a predictable outcome.

Underreporting is widespread. In Thailand, only 11.4% of victims who suffered financial losses reported them to authorities. Many victims report to their financial institution instead, helping explain why the CFR receives roughly twice as many cases through banks as through police channels.

Four barriers recur. Victims often do not know where to report, doubt that reporting will help, consider losses too small to justify the effort, or feel embarrassment and stigma. Larger losses are far more likely to be reported, while small-value scams frequently go unreported. Improving reporting therefore requires more than awareness campaigns; it requires simpler reporting channels, lower reporting costs, greater confidence in outcomes, and reduced stigma.

Why victims do not report: the frictions behind the silence



Source: Treerat et al. (2025), citing GASA/ScamAdviser/Whoscall, *State of Scams in Thailand 2025* (n = 1,000).

Good practice improves reporting by either reducing its cost or increasing its benefit. Costs can be reduced through simple, trusted reporting channels such as Thailand’s AOC 1441, Singapore’s ScamShield and 1799 hotline, Hong Kong SAR’s Anti-Scam Helpline 18222 and Malaysia’s NSRC 997 hotline, as well as digital tools that lower search costs and stigma. Benefits can be increased by improving recovery prospects, streamlining restitution, and turning individual reports into shared intelligence that helps identify mule networks and protect future victims. The broader lesson is that reporting should complement, not substitute for, shared intelligence, automated detection, and victimization surveys that uncover fraud otherwise missed by administrative data.

- **Dynamically upgrading technical defenses counters emerging threats like AI-enabled scams and deepfakes.** In 2025, the HKMA introduced the “E-Banking Security ABCD” enhancements: promoting greater use of in-app authentication in place of SMS OTPs (Authenticate in App), enabling voluntary deactivation of risky internet banking functions (Bye to unused functions), encouraging

more effective use of the Suspicious Account Alert mechanism (Cancel suspicious payments), and enhancing banks’ deepfake detection capabilities (deepfake detection). Good practices introduced under Measure D are associated with a close to 100% improvement in banks’ capability to detect sophisticated, real-time deepfake attacks.

3 Leverage Existing Risk Mitigation and Enforcement Frameworks

Rather than creating standalone mechanisms from scratch, effective anti-fraud regimes repurpose and integrate mature cybersecurity, AML/CFT, and law enforcement architectures. Practical implementation across the region reveals several core lessons.

3.1 Integrating cybersecurity and fraud risk management frameworks is essential to dismantle operational silos against cyber-enabled threats.

- **Converging cyber resilience and anti-fraud operations enables holistic threat sharing and defense.** Since vectors like malware and deepfakes start as technical breaches, governance must synchronize IT security and fraud teams. In Thailand, cybersecurity regulations explicitly incorporate fraud risk, allowing the Thailand Banking CERT (TB-CERT) to evolve into a sector-wide anti-fraud coordination hub, paralleling FS-ISAC and Hong Kong SAR’s FINEST in adapting and upgrading existing platforms for scam prevention.

3.2 AML/CFT frameworks should be leveraged to trace and intercept illicit fraud proceeds.

- **Leveraging AML/CFT machinery enhances fraud detection and asset interdiction.** Because fraud proceeds require laundering, foundational AML/CFT controls — due diligence, transaction

monitoring, and beneficial ownership checks — form critical defenses. Hong Kong SAR operationalizes this through the Fraud and Money Laundering Intelligence Taskforce (FMLIT), a public-private partnership (PPP), and FINEST, a bank-to-bank information-sharing platform, connecting regulators, police, and banks to rapidly exchange suspect accounts and fund-tracing intelligence.

Thailand has expanded its anti-fraud response into a broader systemic defense through the joint Framework for Safeguarding the Financial Sector from Illicit Activities, launched by the Bank of Thailand alongside 11 financial sector associations. The initiative escalates proactive measures across the ecosystem — tightening Know Your Customer (KYC), customer due diligence (CDD), and enhanced due diligence (EDD) standards, subjecting high-risk cash flows to greater scrutiny, deploying advanced surveillance technologies, and linking a high-risk individual database directly to the CFR to close inter-agency loopholes (Annex V).

3.3 Law enforcement operations and asset recovery must be accelerated to eliminate systemic bottlenecks.

The sheer volume of fraud cases severely undermines manual enforcement and timely victim redress.

Compounding this, most cases involve multiple defrauded victims claiming pooled funds, making the recovery process far more complicated. Authorities must eliminate procedural friction, automate core workflows, and redirect resources toward dismantling organized syndicates.

- **Modernizing enforcement requires automating fund tracing, streamlining victim restitution, and dismantling syndicates via pooled intelligence.** For example, Malaysia's National Fraud Portal (NFP) automates the end-to-end handling of fraud reports and fund tracing, and supports data-driven mule-account assessments, reducing tracing times

by 75% and increasing mule-account detections by 149% in 2025. To expedite recovery, Thailand's AMLO executes direct victim restitution without court proceedings, paralleling administrative tools in Singapore and Hong Kong SAR. Crucially, the Cross-Border Anti-Scam Collaboration Platform FRONTIER+, which is formed by the police forces across a number of jurisdictions including Singapore, Hong Kong SAR, Malaysia, and Thailand, and information sharing PPPs like Hong Kong SAR's FMLIT pivot resources from chasing individual transactions to taking down criminal networks at scale (see Box 8).

4 Expand Domestic and Cross-Border Coordination and Cooperation

Cyber-enabled fraud syndicates exploit institutional gaps and regulatory silos across sectors and borders – originating attacks outside the financial perimeter via telecommunications and social media while moving proceeds across borders in seconds. Defeating this borderless threat requires jurisdictions to replace fragmented domestic defenses with standing cross-sector and cross-border operational coordination.

4.1 Institutionalizing standing cross-sector coordination and clear liability frameworks is a critical first step to align ecosystem-wide defenses.

- **Pairing operational duties with enforceable liability backstops ensures cross-sector accountability.** Jurisdictions navigate a governance spectrum: a combination of regulatory codes and industry collaboration frameworks (Hong Kong SAR); and shared responsibility frameworks (Malaysia, Singapore, and Thailand).

- **Upstream statutory mandates create essential baselines but operate in silos due to an unresolved incentive divide.** As detailed in 2.1, while authorities have imposed targeted duties across telecommunications and social media platforms, these frameworks remain works in progress and are constrained by persistent incentive asymmetries.

4.2 Expanding cooperation beyond the financial sector remains challenging, with real-time cross-sector data sharing as the primary gap.

- While interbank data platforms (such as FINEST, CFR, and NFP) mature within the banking perimeter, real-time data integration between banks, telcos, and e-commerce or social media platforms lags behind. Upstream threat intelligence – such as Voice over Internet Protocol (VoIP) spoofing patterns, SIM rotation velocity, and fraudulent ad metadata – is rarely linked to banking surveillance engines in real time, leaving a

dangerous blind spot between initial digital contact and payment execution.

4.3 Cross-border enforcement must transition from slow formal treaties to pre-positioned operational networks matching payment speed.

The structural latency of Mutual Legal Assistance Treaties (MLATs) – which take months to execute – creates an enforcement gap against syndicates moving funds across borders into digital assets within seconds, rendering diplomatic channels obsolete.

- **Pre-positioned operational networks enable near-real-time tracing and asset freezing.** To match the velocity of illicit flows, authorities must establish operational frameworks anchored on three potential pillars: (1) designated 24/7 Single Points of Contact (SPOCs) across regional FIUs and specialized anti-scam units; (2) standardized, expedited data channels to trace cross-border transaction trails without formal diplomatic delays; and (3) interoperable emergency freezing protocols empowering receiving jurisdictions to immobilize recipient accounts upon verified alerts.

Pre-aligned operational coordination delivers immediate, scalable disruption, as demonstrated by Operation FRONTIER+. Established in 2024 among regional Anti-Scam Centers – including Thailand and Malaysia – with the Singapore Police Force’s Anti-Scam Command and Hong Kong SAR’s Anti-Deception Coordination Centre serving as the joint Secretariat, these pre-positioned networks enable agencies to exchange live transaction telemetry, execute cross-border account freezes within hours, and dismantle syndicate infrastructure at a speed and scale unattainable through traditional treaty channels alone (Box 8).

4.4 Regional supervisory and policy channels must harmonize fragmented control frameworks to eliminate regulatory arbitrage.

Cross-border regulatory asymmetries create exploitable operational seams: divergent fraud definitions, inconsistent mule taxonomies, and uneven security baselines enable syndicates to route illicit flows through jurisdictions with the weakest oversight.

- **Regional central bank fora can advance practical supervisory convergence.** Multilateral bodies such as EMEAP and the Association of Southeast Asian Nations (ASEAN) Working Committees could explore cooperative initiatives, such as standardizing mule definitions and risk indicators for cross-border flagging, aligning baseline controls (e.g., kill switches, cooling-off periods, biometric step-ups), and conducting joint crisis simulations to stress-test regional response protocols.

4.5 As cross-border fast-payment linkages could open up new vulnerabilities to cyber-enabled fraud, real-time fraud controls should be embedded directly into payment rail design architecture.

Bilateral links (e.g., PromptPay-PayNow) and multi-lateral networks (e.g., Project Nexus) reduce payment frictions and enhance connectivity, but their speed also compresses traditional intervention windows. Participating jurisdictions have already implemented safeguards such as real-time fraud screening, transaction holds, and customer alerts.

- **As cross-border networks become increasingly interconnected, authorities and payment system operators should continue strengthening rail-level controls to address evolving risks and prevent the rapid movement of illicit funds.** Also, they should embed core safeguards directly into rail design including (1) pre-transaction risk scoring to inject mule flags and velocity indicators into authorizations; (2) synchronized friction, applying automated holds and step-ups across switches for high-value anomalies; and (3) inter-clearinghouse stop-payment protocols to intercept transfers before final settlement.

BOX 8 FRONTIER+: Cross-Border Enforcement at the Speed of the Payment

The gap it fills. Traditional mutual legal assistance takes months, whereas illicit funds move in seconds. By the time formal requests are processed, funds and accounts have vanished. Standing operational networks bridge this latency gap by pre-establishing legal gateways and communication protocols, enabling cross-border intervention before stolen assets disperse.

What FRONTIER+ is. Convened by participating police forces, FRONTIER+ is a public-private partnership linking anti-scam units across 14 jurisdictions – now including the United States – for continuous intelligence sharing and joint enforcement. Demonstrating its operational velocity, Operation FRONTIER+ III in early 2026 resulted in over 7,500 subjects investigated, 3,000 arrests, roughly SGD 207 million seized, and more than 101,000 bank accounts frozen across member jurisdictions.



How it works. Enforcement is paired directly with technology platforms via initiatives like the Global Signal Exchange. Real-time sharing of scam indicators enables the rapid removal of fraudulent accounts, advertisements, and domains before additional victims are targeted, extending deterrence beyond conventional police powers.

The broader lesson. Cross-border networks succeed not through periodic operations, but through continuous intelligence flows that compound mutual defense. Joint operations serve as operational stress tests of the network itself. Cross-border cooperation cannot be improvised during a crisis; it must be built, exercised, and maintained as a standing institutional capability.

5 Promote Consumer Protection and Resilience

A persistent knowledge-action gap remains a core challenge in mitigating APP fraud. Empirical evidence from Thailand shows that protective efficacy hinges on the type of knowledge: generic digital hygiene is far less effective than understanding

specific manipulation mechanics, leaving even highly educated cohorts vulnerable. Ultimately, cognitive awareness fails once social engineering exploits acute psychological triggers – such as manufactured urgency, fear, or misplaced trust.

BOX 9 Singapore's Multi-Layered, Behavioral Consumer Resilience Interventions

Why multi-layered and behavioral design? Authorized social engineering accounted for 81.8% of Singapore's scam cases in 2025, exploiting cognitive biases rather than technical vulnerabilities. Because static advisories fail during active manipulation, Singapore embeds behavioral friction, pre-commitment devices, and on-demand verification directly into payment flows.

Consumer empowerment and public utilities. The Scam Public Education Office drives the national "ACT" framework (Add security features, Check official sources, Tell authorities). The ScamShield Suite serves as the primary verification gateway: its 24/7 helpline (1799) handles 500–700 daily calls (85% pre-transaction inquiries that stop transfers in advance), while its AI app (>1.53 million downloads by February 2026) actively blocks blacklisted numbers, malicious links, and fraudulent SMSes.

Operator-side safeguards

- **Pre-commitments and kill switches:** Money Lock allows customers to set aside funds in their bank accounts that cannot be transferred through digital channels (e.g., FAST, PayNow), with unlocking requiring strict in-person verification at a branch or an ATM; by mid-2026, about 589,000 customers had locked close to SGD 49 billion. Self-service kill switches instantly freeze compromised accounts and digital banking access.
- **Cooling periods and transfer holds:** Banks enforce a 12-hour cooling delay on high-risk administrative actions (registering a new device, limit increases, contact detail updates) and a mandatory 24-hour hold or rejection on transfers draining over 50% of balances in accounts holding ≥SGD 50,000. Clickable links in bank communications are prohibited.
- **Statutory intervention:** The Protection from Scams Act 2025 empowers police to issue time-bound Restriction Orders that temporarily halt banking access when victims remain under psychological manipulation, buying critical time to break deception (Annex IV).



Public education under the national ACT framework

5.1 Closing the knowledge-action gap requires actionable education complemented by operator-side safeguards and modernized consumer protection.

- **Fraud education must combine broad awareness, interactive learning, and point-of-decision guidance to close the knowledge-action gap and**

overcome “education fatigue.” Because repetitive advisories induce public desensitization, effective regimes pivot toward emotionally resonant storytelling, gamification, and demographic-tailored outreach. In Hong Kong SAR, the HKPF, HKMA, SFC, and the Investor and Financial Education Council (IFEC) have jointly provided anti-scam

resources to help the public identify investment scams. At the IFEC FinEd Hub, a digital experiential learning center, the “IFEC Investment Game” simulates investment scams inspired by real-life cases, helping the public recognize red flags and respond with confidence. In Singapore, the Scam Public Education Office (SPEO) drives this multi-channel approach through the national “ACT” campaign (Add security features, Check for signs, Tell authorities) alongside MoneySense. This outreach is reinforced by Cyber Security Agency (CSA) interactive simulations, IMDA digital literacy workshops for seniors, and real-time behavioral friction embedded directly in mobile banking workflows.

- **A centralized anti-fraud utility bridges the knowledge-action gap by establishing an authoritative single front door for verification and response.** By enabling pre-transaction counterparty checks and feeding real-time data to banks and police, these hubs convert passive awareness into active defense. Singapore’s ScamShield Suite integrates automated call/SMS blocking with the 24/7 Helpline (1799) – where approximately 85% of inquiries intercept fraud before funds move – while Hong Kong SAR’s Suspicious Account Alert embeds live risk alerts directly into payment rails. These unified platforms institutionalize verification habits and eliminate reporting friction.
- **Building consumer resilience requires reinforcing education with operator-side safeguards and modernized protection frameworks.** Because awareness cannot withstand acute psychological manipulation, technical controls must be embedded directly into payment rails. As detailed in Pillar 2, key defenses include pre-commitment tools (e.g., Money Lock and Money Safe), risk-based transaction friction, and statutory powers to halt transfers when victims remain deceived – all backed by enforceable conduct standards, clear liability allocation, and accessible redress.

5.2 Protecting vulnerable populations requires tailoring inclusive education, safeguards, and protections to address the distinct cognitive and operational barriers they face.

- **Policy frameworks must integrate segmented outreach, assisted touchpoints, and passive technical defaults.** Since vulnerable groups cannot rely on self-directed settings, defenses must combine targeted literacy with automated ecosystem controls. For example, Singapore exemplifies this by pairing public education, including targeted publicity efforts around Money Lock for elderly customers, with other banking safeguards such as enhanced surveillance and proactive interventions for elderly customers. Similar measures have also been implemented in other jurisdictions.

Hong Kong SAR deploys a 360-degree education framework to embed anti-fraud vigilance across key life stages. For youth, the HKMA fosters cyber hygiene through school games, competitions, and campus campaigns deterring mule recruitment (“Don’t Lend/Sell Your Account”). For seniors, it partners with banks on eldercare seminars and “train-the-trainers” programs. Across the broader community, gamified AR mascot installations (Lachachu) pair with AI-driven multimedia on international and Mainland platforms to protect residents and cross-border commuters.

5.3 Authorities and financial institutions must institutionalize dynamic behavioral testing to continuously assess consumer resilience and adapt fraud defenses.

Relying solely on static compliance metrics – like campaign reach or formal complaint logs – obscures vulnerabilities under psychological deception.

- **Robust oversight requires continuous stress-testing of consumer responses in simulated environments,** analyzing fraud post-mortems, and utilizing live operational data to dynamically calibrate behavioral friction, step-up authentication thresholds, and surveillance parameters.

BOX 10 Hong Kong SAR's Comprehensive and Behavioral Consumer Education Program

Why behavioral design, delivered everywhere? Warnings wear out: when every channel carries scam alerts, repeated advisories produce “education fatigue”. Hong Kong SAR’s answer is a holistic approach rather than a campaign: communications built on behavioral science to drive a public cognitive shift against scams, and a 360-degree inter-agency model that reaches every group online and offline. Such customer education fortifies the final line of defense, thereby boosting the effectiveness of the other three pillars of the multi-strata anti-scam ecosystem: bank-level detection and prevention systems, cross-sectoral collaboration, and bank-to-customer safeguards.

Beating education fatigue. The HKMA moved from static warnings to behavioral-science-driven interventions anchored by characters the public remembers. The Hong Kong Police Force’s “Little Grape” (2020), named for the Cantonese contraction of “Beware of Liars”, carries a three-step ask: “Stay Alert to Scams”, “Ending Deception Starts with You” (tell family and friends) and call the ADCC Hotline 18222. Following the viral anti-fraud song co-performed by HKMA senior leadership and a cult artist in 2024, the HKMA introduced “Lachachu”, the Despicable Banana, in 2025, which reveals the scammer’s greed once the victim is hooked. In 2026, generative AI was adopted to produce a new anti-fraud music video inspired by a kung-fu game concept. The HKMA also turns awareness into practice: deepfake-awareness shorts let viewers vote on the ending, and mini-drama series held viewers across every episode with double the engagement of standard content. These efforts were recognized with the Communications Initiative award at the Central Banking Awards 2026.



A deepfake-awareness short from the HKMA's series

360-degree, tailored, online and offline. The HKMA aligns one message with the HKPF, regulators, the banking and stored-value-facility industries, and community stakeholders. Each group gets its own channel: gamified literacy for primary and secondary school students, campus networks for tertiary students (“Don’t Lend/Sell Your Account”), a train-the-trainers model with banks in elderly centers, and localized drama videos for cross-boundary commuters on Mainland platforms (five times the reactions of standard posts). Online, the characters live on social media; offline they appear at roadshows, light shows, school visits, interactive game booths at the Book Fair, 3D sculptures atop postal boxes with augmented reality installations, and Halloween flash mobs.

Cross-Cutting Lessons Learned

Drawing from cross-jurisdiction practices and operational insights, eleven salient lessons guide policymakers in strengthening national fraud-mitigation frameworks.

- 1. Build a whole-of-ecosystem defense.** Fraud exploits gaps between sectors and borders. Strong protection requires statutory responsibilities and standing public-private coordination to close weak links.
- 2. Strong leadership and governance that align responsibility and liability will be key.** Decisive leadership synchronizes cross-sector defense and intervention powers. Distributing accountability compels private gatekeepers to invest in robust fraud mitigation.
- 3. Prevention and early intervention are far more cost-effective than downstream recovery.** Fast payments disperse illicit funds instantly, so authorities must prioritize upstream prevention by blocking scam vectors and embedding banking friction, saving far more resources than fund recovery.
- 4. There is no silver bullet.** No single tool defeats cyber-enabled fraud. True resilience requires mutually reinforcing measures – prevention, detection, rapid freezing, and consumer protection – throughout the entire fraud life cycle.
- 5. Collective intelligence sharing and expertise are at the heart of effective intervention.** System-wide data pooling transforms isolated detections into collective defense. Overcoming victim under-reporting and data-sharing barriers remains critical to disrupt criminal networks.
- 6. Combine technology with behavioral design.** Because authorized fraud exploits human psychology, technological safeguards must incorporate risk-based friction to prompt users and interrupt deception before transactions are executed.
- 7. Fraud resilience demands continuous adaptation.** Criminal tactics rapidly shift as defenses harden, so mitigation frameworks must remain agile, intelligence-led, and dynamically updated through responsive administrative rule-making.
- 8. Behaviorally designed interventions to counter education fatigue.** Standard warnings induce education fatigue, widening the knowledge-to-action gap. Piercing this habituation requires shifting from dry facts to emotionally resonant, unconventional narratives that trigger immediate protective action.
- 9. Navigate policy trade-offs to balance security with usability, inclusion, and trust.** Overly strict controls harm user convenience and adoption. Mitigation must be risk-based and flexible to secure payments without undermining financial inclusion.
- 10. Protect vulnerable users with inclusive safeguards and redress.** Disadvantaged groups suffer disproportionately yet face steep mitigation barriers. Policies must provide universal baseline protection and fair, accessible dispute resolution.
- 11. Strengthen cross-border defenses.** Since syndicates operate globally, purely domestic measures are incomplete. Effective defense requires international cooperation, cross-border intelligence sharing, and fraud controls embedded within payment infrastructures.

Remaining Challenges and the Way Forward

The four jurisdictions have made remarkable progress in strengthening fraud resilience. Significant challenges nonetheless remain – upstream, across borders, and in returning money to victims.

Despite remarkable progress, seven significant challenges remain, highlighting priorities for the next phase of fraud-resilient efforts.

- 1. Challenges persist in shifting to more cost-effective upstream defenses among telcos and online platforms.** Intensive downstream safeguards cannot stop fraud if origination interdiction remains weak. Authorities must enforce gatekeeper compliance: mandating verified SIM registration, tighter ownership caps, rigorous advertiser vetting, and location intelligence.
- 2. Data-sharing across sectors and borders remains a critical gap.** Information exchange has matured within banking, but legal barriers, divergent standards, and weak incentives restrict sharing across telcos, digital platforms, and foreign counterparts. Authorities must mandate participation with statutory safe harbors and multilateral gateways.
- 3. A persistent awareness-action gap and low reporting leave consumers vulnerable.** Heavy investment notwithstanding, consumers remain susceptible to authorized push payment (APP) scams, compounded by low reporting. Authorities must pivot toward point-of-transaction behavioral nudges and frictionless reporting channels for consumer resilience.
- 4. Victim redress remains the weakest link despite growing asset recovery.** Authorities increasingly freeze illicit proceeds, but returning funds

to victims remains slow. Frameworks must pivot toward end-to-end restitution, establishing streamlined claims, transparent rules, and priority protections for vulnerable victims.

- 5. Cross-border cooperation remains uneven.** Domestic coordination has matured, but international mechanisms remain geared toward major investigations rather than fast-moving scams. National centers must establish standing pacts: standardized referrals, mutual freeze protocols, and streamlined cross-border recovery procedures.
- 6. The seam between fiat and crypto remains porous.** Exchanges face tighter oversight, but criminals move funds via cash and person-to-person transfers before freezes trigger. Authorities must strengthen monitoring across fiat and digital channels, linking blockchain analytics to national registries and flagging rapid cash-outs.
- 7. Policies are rarely evaluated for results.** Authorities should embed evaluation into policy design from inception, ensuring that interventions are systematically tested, measured, and refined based on evidence rather than assumption.

These challenges underscore that fraud resilience is not a destination, but a process of continuous adaptation. As fraud patterns evolve, effective mitigation will depend on iterative learning, rigorous evaluation, and timely policy adjustment.

Conclusions and Policy Takeaways for the Global Community

Policymakers must foster continued learning, adaptation, and international collaboration. Only then will digital finance remain innovative, inclusive, resilient, and secure.

Cyber-enabled fraud has emerged as one of the most critical risks of digital transformation in financial services. While digital finance expands access, efficiency, and financial inclusion, it also enables fraudsters to operate at unprecedented scale, speed, and sophistication by exploiting human psychology, institutional gaps, and system vulnerabilities. Consequently, cyber-enabled fraud has evolved from an institutional operational risk into a systemic policy challenge that threatens public trust in payment systems and the broader benefits of digital finance.

This paper serves as a practical companion to the Bangkok Blueprint, illustrating how its high-level principles and Key Considerations translate into operational practice. Drawing on implementation experiences and trade-offs across Hong Kong SAR, Malaysia, Singapore, and Thailand, eleven salient lessons emerge to guide policymakers in designing and strengthening their national fraud-mitigation frameworks.

As digital financial systems become increasingly interconnected across borders, the challenge of cyber-enabled fraud will continue to evolve. Organized fraud networks are likely to become more adaptive, technologically sophisticated, and international in scope. While significant progress has been made within the financial sector of the four jurisdictions, many of the remaining vulnerabilities lie beyond it, particularly in telecommunications networks, e-commerce and social media platforms, digital assets, cross-border payment channels, and the gaps between institutions and jurisdictions.

The common direction of travel is increasingly clear: stronger fraud resilience will depend on coordinated action across the fraud life cycle, supported by trusted partnerships, effective information sharing, aligned incentives, and a shared commitment to safeguarding the benefits of digital finance. Through continued learning, adaptation, and international collaboration, policymakers can help ensure that digital finance remains not only innovative and inclusive, but also trustworthy, resilient, and secure.

Notes

- 1 As in the Bangkok Blueprint, this aligns with standard international classifications established by the Financial Action Task Force (FATF), the Egmont Group, INTERPOL, and the United Nations Office on Drugs and Crime (UNODC).
- 2 For example, the Federal Trade Commission (2025) report estimates overall consumer fraud losses over 2024 at USD 195.9 billion compared with only USD 12.8 billion in reported fraud losses for the US alone. Global Anti-Scam Alliance and Feedzai (2025) estimated global fraud-related losses at almost half a trillion dollars in 2024.
- 3 Hong Kong SAR 0.29%, Malaysia 0.08%, Singapore 0.15% and Thailand 0.14%.
- 4 Launched by the HKPF in September 2022, the one-stop scam and pitfall search engine, Scameter, helps the public identify frauds and online pitfalls. When the public encounters suspicious calls, online sellers, friend requests, job ads, investment websites, etc., they can enter the platform account name or number, payment account, phone number, email address, URL, etc. to assess the risk of fraud. The search results of Scameter will be indicated in different colors based on the level of fraud risk involved.
- 5 Hong Kong SAR is exploring enhancing the legal framework to bolster the detection and removal of fraudulent content, including content generated through the misuse of artificial intelligence (AI) by sectors such as technology and telecommunications.

References

- Asia/Pacific Group on Money Laundering. (2026, May). *Cyber scam hubs and human trafficking*. <https://www.apgml.org/news/new-report-exposes-links-between-cyber-scam-hubs-and-human-trafficking>
- Bank Negara Malaysia. (2024a, June 28). *Ensuring fair treatment for victims of unauthorised e-banking transactions* (Policy Document). <https://www.bnm.gov.my/-/pd-fair-treatment24>
- Bank Negara Malaysia. (2024b, March 27). *Fair treatment of financial consumers* (Policy Document). <https://www.bnm.gov.my/-/pd-ftfc>
- Bank Negara Malaysia. (2024c, August 20). *National Fraud Portal to solidify coordinated efforts in curbing financial scams* [Press release]. <https://www.bnm.gov.my/-/nfp-launch>
- Boeddu, G. L., Chien, J., Grady, R. C., & Istuk, I. (2021, April). *Consumer risks in fintech: New manifestations of consumer risks and emerging regulatory approaches* (Policy Research Paper No. 159278). World Bank. <https://doi.org/10.1596/35699>
- Chang, S., Duflos, E., & Chalwe-Mulenga, M. (2026, May). *Solutions to protect consumers from fraud in digital finance* (Working Paper). CGAP. <https://www.cgap.org/research/solutions-to-protect-consumers-fraud-in-digital-finance>
- Federal Trade Commission. (2025, December 1). *Protecting older consumers 2024–2025: A report of the Federal Trade Commission*. https://www.ftc.gov/system/files/ftc_gov/pdf/P144400-OlderAdultsReportDec2025.pdf
- Financial Action Task Force. (2026a, February). *Cyber-enabled fraud: Digitalisation and money laundering, terrorist financing and proliferation financing risks*. <https://www.fatf-gafi.org/en/publications/Methodsandtrends/cyber-enabled-fraud-digitalisation-ml-tf-pf-risks.html>
- Financial Action Task Force. (2026b, July). *Information sharing to combat illicit finance: Global overview of public and private sector partnerships and data protection arrangements*. <https://www.fatf-gafi.org/en/publications/Methodsandtrends/information-sharing-ppp-data-protection-arrangements.html>
- Financial Action Task Force, INTERPOL, & Egmont Group of Financial Intelligence Units. (2023, November). *Illicit financial flows from cyber-enabled fraud*. <https://www.fatf-gafi.org/en/publications/Methodsandtrends/illicit-financial-flows-cyber-enabled-fraud.html>
- Financial Services Information Sharing and Analysis Center. (2025, April). *Leveling up: A cyber fraud prevention framework for financial services*. <https://www.fsisac.com/knowledge/cyber-fraud-prevention-framework>
- Financial Stability Board. (2024, December 12). *Recommendations to promote alignment and interoperability across data frameworks related to cross-border payments: Final report*. <https://www.fsb.org/2024/12/recommendations-to-promote-alignment-and-interoperability-across-data-frameworks-related-to-cross-border-payments-final-report/>

- Gaidosch, T., Islam, E., Khiaonarong, T., Ravikumar, R., & Wilson, C. (2026, January). *Good practices in cyber risk regulation and supervision* (Departmental Paper No. 2026/001). International Monetary Fund. <https://doi.org/10.5089/9798229026185.087>
- Global Anti-Scam Alliance & Feedzai. (2024). *Global state of scams report 2024*. <https://www.feedzai.com/resource/global-state-of-scams-report-2024/>
- Global Anti-Scam Alliance & Feedzai. (2025). *Global state of scams report 2025*. <https://www.feedzai.com/resource/global-state-of-scams-report-2025/>
- Government Technology Agency of Singapore. (2026). *ScamShield*. <https://www.tech.gov.sg/products-and-services/for-citizens/scam-prevention/scamshield/>
- Hapipat, T. (2024, September). *National survey on fraud victimisation and digital financial risks in Thailand*. Social and Business Development Research Center, Faculty of Economics, Chulalongkorn University.
- Hong Kong Monetary Authority. (2023, November 24). *The HKMA and banking sector support the launch of the Anti-Deception Alliance to fight against fraud* [Press release]. <https://www.hkma.gov.hk/eng/news-and-media/press-releases/2023/11/20231124-4/>
- Hong Kong Police Force. (2026). *Scameter*. <https://cyberdefender.hk/en-us/scameter/>
- Hong Kong Special Administrative Region. (2025). Banking (Amendment) Ordinance 2025 [Ord. No. 23 of 2025, gazetted 13 June 2025]. <https://www.elegislation.gov.hk/hk/2025/23!en>
- Infocomm Media Development Authority & Monetary Authority of Singapore. (2024). *Guidelines on Shared Responsibility Framework*. <https://www.imda.gov.sg/-/media/imda/files/regulations-and-licensing/regulations/consultations/2024/shared-responsibility-framework-for-phishing-scams/guidelines-on-shared-responsibility-framework.pdf>
- International Monetary Fund & World Bank. (2018, October). *The Bali fintech agenda* (IMF Policy Paper No. 2018/050). International Monetary Fund. <https://doi.org/10.5089/9781498309950.007>
- INTERPOL. (2026, March). *INTERPOL global financial fraud threat assessment*. <https://www.interpol.int/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat>
- Khiaonarong, T., & Zheng, S. (2026, March). *The rise of cyber events and digital fraud in the financial sector* (IMF Working Paper No. 2026/062). International Monetary Fund. <https://doi.org/10.5089/9798229043557.001>
- National Anti-Financial Crime Centre. (n.d.). *National Scam Response Centre (NSRC)*. Prime Minister's Department, Malaysia. <https://nfcc.jpm.gov.my/index.php/en/about-nsrc>
- OECD. (2026, March). *Consumer finance risk monitor 2026*. <https://doi.org/10.1787/61f7dbe0-en>
- O'Neill, G. (2017, October 24). *Fraud and money laundering intelligence taskforce (FMLIT)* [Presentation, Commercial Crime Bureau, Hong Kong Police Force; published by the Hong Kong Monetary Authority]. <https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/aml-cft/20171024e1a6.pdf>
- Payments Network Malaysia. (2026). *National Fraud Portal*. PayNet. <https://paynet.my/digital-initiatives/national-fraud-portal.html>
- ScamShield. (2026). *ScamShield*. Government of Singapore. <https://www.scamshield.gov.sg/>

- Singapore. (2025). Protection from Scams Act 2025 [No. 1 of 2025. Singapore Statutes Online]. <https://sso.agc.gov.sg/Act/PSA2025>
- Singapore Police Force. (2025, August). *Operation FRONTIER+: A unified front against transnational scams*. Police Life. <https://www.police.gov.sg/Media-Hub/Police-Life/2025/08/Operation-FRONTIER-A-United-Front-Against-Transnational-Scams>
- Thailand. (2023). Emergency Decree on Measures for the Prevention and Suppression of Technological Crimes, B.E. 2566 [Royal Thai Government Gazette, 140(18A), 1–7]. <https://ratchakitcha.soc.go.th/documents/140A018N00000000000100.pdf>
- Thailand. (2025). Emergency Decree on Measures for the Prevention and Suppression of Technological Crimes (No. 2), B.E. 2568 [Royal Thai Government Gazette, 142(27A), 5–13]. <https://ratchakitcha.soc.go.th/documents/67320.pdf>
- Tosborvorn, T. (2025). *Thailand's financial fraud landscape* [Conference presentation, BOT Symposium 2025, Bangkok]. https://www.pier.or.th/files/conferences/2025/symposium2025_slides_Thiti.pdf
- Tosborvorn, T., Choedpasuporn, S., Amarase, N., Maneesilp, S., & Chantararat, S. (2026). *The landscape of online scams in Thailand* (Discussion Paper No. 264). Puey Ungphakorn Institute for Economic Research.
- Treerat, N., Amarase, N., Kapilakanchana, M., & Kiatruangkrai, C. (2025). *Thailand's financial fraud landscape: From vulnerability to safety* [Conference presentation, BOT Symposium 2025, Bangkok]. https://www.pier.or.th/files/conferences/2025/symposium2025_slides_Nualnoi.pdf
- United Nations Development Programme. (2026, February). *Countering digital scams: Stemming the tide on an urgent development challenge* (Issue Brief). <https://www.undp.org/sites/g/files/zskgke326/files/2026-02/undp-countering-digital-scams.pdf>
- United Nations Office on Drugs and Crime. (2025, September). *Emerging threats: The intersection of criminal and technological innovation in the use of automation and artificial intelligence in the cybercrime landscape of Southeast Asia*. https://www.unodc.org/roseap/uploads/documents/Publications/2025/UNODC_Report_Emerging_threats_-_The_intersection_of_criminal_and_technological_innovation_in_the_use_of_automation_and_AI.pdf
- World Bank. (2021). *Universal Financial Access 2020: Lessons for the future*. <https://doi.org/10.1596/39736>
- World Bank. (2024). *World Development Indicators* [Data set]. <https://data.worldbank.org>

Evolution of Anti-Fraud Strategies

Although the four jurisdictions followed different paths, their strategies have converged around a common set of tools: legal accountability, intelligence sharing, stronger payment-security controls, and interventions against authorized fraud. Hong Kong SAR and Singapore each built domestic coordination among banks and intelligence-sharing mechanisms first, adding legal protection later to support information sharing and intervention. By contrast, Malaysia and Thailand relied on more concentrated legislative and regulatory reforms in 2022–2023 to establish accountability, centralized response mechanisms,

and fraud controls before progressively expanding their scope. Across all four jurisdictions, the policy focus has shifted from combating unauthorized fraud, such as account takeover and malware, toward authorized fraud driven by social engineering and APP scams. Recent reforms have also converged on three frontiers: strengthening cross-institution and cross-border intelligence sharing, extending responsibilities beyond banks to telecommunications operators and digital platforms, and deploying AI- and data-driven tools to identify fraud risks earlier and intervene before losses occur.

Annex I. Evolution of anti-fraud strategy – Hong Kong SAR

TIME	LEGAL & ACCOUNTABILITY FRAMEWORK	DATA-SHARING & COORDINATION INFRASTRUCTURE	ADDRESSING UNAUTHORIZED FRAUD	ADDRESSING AUTHORIZED FRAUD
● Pre-2022		FMLIT public-private intelligence taskforce		24/7 stop-payment mechanism (ADCC–banks)
● 2022		Scameter search engine (Police)		
● 2023	Anti-Scam Consumer Protection Charter – no embedded hyperlinks	- FINEST bank-to-bank sharing (corporates) - Anti-Deception Alliance – 10 banks in ADCC	- Real-time suspicious-account monitoring – 28 retail banks - Extra confirmation for binding cards to mobile wallets 10 measures to enhance e-banking security 33 measures to protect card customers - SMS Sender Registration Scheme	- Upstream scam intervention – SMS, calls, visits - FPS ‘High Risk’ alert (Scameter)
● 2024	Charter 2.0 – 230+ FIs & merchants	Established FRONTIER+	Enhanced security measures to safeguard customers against malware scams	- APS circular – dynamic monitoring, customer enquiry - Suspicious Account Alert extended to internet banking, branches, ATMs
● 2025	- Banking (Amendment) Ordinance – legal cover for bank-to-bank sharing - Charter 3.0 – tech & telecom firms	Enhanced FINEST – individual accounts	E-Banking Security ABCD – in-app authentication, deepfake detection, etc.	- Upstream intervention for hard-to-reach victims - Money Safe – segregated deposits - Wider use of Scameter data 24/7 stop-payment extended to securities firms (ADCC)
● 2026		Account Opening Pilot Project		Lower third-party transfer limits

Annex I. Evolution of anti-fraud strategy – Malaysia

TIME	LEGAL & ACCOUNTABILITY FRAMEWORK	DATA-SHARING & COORDINATION INFRASTRUCTURE	ADDRESSING UNAUTHORIZED FRAUD	ADDRESSING AUTHORIZED FRAUD
● Pre-2022				
● 2022		National Scam Response Centre – 997 hotline (NFCC, RMP, BNM, MCMC, FIS, telcos)	Five measures – SMS-OTP migration, cooling-off, single device, detection rules, hotlines + kill switch, no SMS links	National Scam Awareness Campaign (banking associations)
● 2023				
● 2024	- Penal Code & CPC amendments – mule-account offences; seizure powers - Cyber Security Act	National Fraud Portal (PayNet) – automated tracing, sharing, mule assessment	Fair Treatment for Victims of Unauthorised e-Banking Transactions	Industry-wide mule-account handling procedures
● 2025		RMP formally leads NSRC operations	Extended the five measures to major non-bank e-money issuers; advanced malware defense	FRONTIER+ joint regional operation
● 2026	- Online Safety Act 2025 in force – platform duties - Cybercrimes Bill 2026 passed (pending royal assent)			

Annex I. Evolution of anti-fraud strategy – Singapore

TIME	LEGAL & ACCOUNTABILITY FRAMEWORK	DATA-SHARING & COORDINATION INFRASTRUCTURE	ADDRESSING UNAUTHORIZED FRAUD	ADDRESSING AUTHORIZED FRAUD
● Pre-2022		- Anti-Scam Centre; Inter-Ministry Committee on Scams (Apr-20) - ScamShield app		
● 2022		Anti-Scam Command – 7 banks co-located	Kill switch; lower default limits; no clickable links	
● 2023	- Online Criminal Harms Act passed (in force Feb-24) - CDSA & Computer Misuse Act amendments		- SMS Sender ID Registry mandatory - Anti-malware controls on banking apps - Money Lock	
● 2024	- Misc. Offences Act – SIM-card abuse - Shared Responsibility Framework (MAS–IMDA)	- ScamShield Suite – 1799 helpline, app, web, alerts - FRONTIER+ regional operation (SPF-led)	- Google Play Enhanced Fraud Protection pilot - SMS OTP phased out for account logins by digital token users	Enhance fraud surveillance and tighten interventions for vulnerable segments
● 2025	- Protection from Scams Act passed (commenced Jul-25) - Facility restriction framework for mules	- Crypto Tracing Team - Participation in Global Signal Exchange	- SMS OTP phased out for card transactions by digital token users - Additional verification for provision of cards to mobile wallets	- Restriction Orders operational (PSA) - OCHA directives to Meta, Apple, Google (impersonation) - Cooling periods for higher risk activities: adding payees, raising limits, and large transfers that drain accounts
● 2026	Amendments to Protection from Scams Act passed	Proof-of-value for industry-level AI scam detection	Postpaid SIM cap – 10 per person	- Discontinue PayNow nickname feature - New/enhanced Codes of Practice for online service providers

Annex I. Evolution of anti-fraud strategy – Thailand

TIME	LEGAL & ACCOUNTABILITY FRAMEWORK	DATA-SHARING & COORDINATION INFRASTRUCTURE	ADDRESSING UNAUTHORIZED FRAUD	ADDRESSING AUTHORIZED FRAUD
● Pre-2022		• KYC rules for digital account opening • Mobile Banking Security Guiding Principles		
● 2022				
● 2023	• Emergency Decree on Technology Crime Prevention and Suppression	• Mobile Banking Security measures introduced (SMS-link ban, one user account per device, facial verification for high-risk transactions) • Central Fraud Registry launched		
● 2024			• Risk-tiered mule-account measures and person-level restrictions (black / grey / brown mules)	
● 2025	• Amended Emergency Decree No. 2 expands responsibilities across the ecosystem	• Security standards elevated to regulatory requirements • Non-bank and digital-asset operators integrated • CFR API pilot	• Identify mule accounts using transfer patterns and transaction values • Suspend suspicious accounts even without victims • Share lists of individuals with suspicious behavior • Measures extended to legal entities	• Risk-based customer profiling and daily transaction limits • Shared Responsibility Framework
● 2026			• Customer profiling safeguards for youth accounts (risk-based daily limits for youth deposit and e-money accounts)	• Minimum Expectation Guideline issued

Governance Structure of National Fraud Strategy

While institutional arrangements differ, anti-fraud frameworks across Hong Kong SAR, Malaysia, Singapore, and Thailand share four core governance elements:

(i) High-level leadership. Central governance structures reflect distinct national models: Hong Kong SAR's multi-agency ecosystem approach, Malaysia's multi-agency model led by NFCC/BNM, Singapore's whole-of-government model led by MHA, and Thailand's ecosystem-wide model led by MDES. Each aligns five core functional authorities – banking, telecommunications, digital assets, asset recovery, and cyber police – while directing collective operational coordination through standing command centers (ADCC, NSRC, ASCom, and AOC 1441).

(ii) Responsibilities and liabilities across stakeholders. Across all four jurisdictions, authorities assign baseline prevention and monitoring duties to their designated supervising institutions. Liability regimes (shared responsibility) diverge: Hong Kong SAR resolves losses case-by-case under established banking codes, paving the way for an institutionalized shared framework; Malaysia mandates a 14-day bank-first investigation with proportionate sharing; Singapore applies a strict waterfall approach for phishing scams under the SRF; and Thailand enforces

statutory, court-adjudicated proportionate liability without a cap.

(iii) Cross-sector data and intelligence sharing. Jurisdictions rely on dedicated operational platforms: Malaysia's NFP and Thailand's CFR centralize transaction-level data to automate fund tracing and multi-tier mule interdiction. In contrast, Hong Kong SAR's FINEST, Scameter, and Scameter+ app emphasize interbank customer risk profiling, intelligence exchange, and pre-transaction alerts.

(iv) Legal mechanisms enabling expedited intervention. Statutory frameworks provide immediate intervention powers and safe harbors: Hong Kong SAR leverages the Banking Ordinance alongside statutory PDPO guidance to safeguard interbank data sharing; Malaysia pairs supervisory policies with Penal Code amendments criminalizing mule accounts; Singapore leverages targeted legislation (OCHA, Protection from Scams Act, FSMA) to mandate bank directives and carve out secrecy exceptions; and Thailand's Emergency Decree authorizes warrantless account freezes and shields cross-sector sharing.

The accompanying table compares elements (i), (iii), and (iv) by jurisdiction; element (ii) is covered in the text only, as baseline duties are common to all four and liability regimes are described above.

Annex II. Comparative anti-fraud governance

	HONG KONG SAR	MALAYSIA	SINGAPORE	THAILAND
HIGH-LEVEL LEADERSHIP	Multi-agency ecosystem: law enforcement leadership with financial-sector oversight	Multi-agency coordination with a centralized operational response	Whole-of-government committee	Legally mandated, ecosystem-wide coordination
Executive coordinator	HKPF and HKMA , joint: criminal enforcement aligned with banking supervision	NFCC , co-led with BNM : national anti-financial-crime strategy and multi-agency operational response	MHA via IMCS : cross-ministerial anti-scam policy and strategic interventions	MDES : statutory lead on policy and cross-sector anti-fraud operations
Coordination center	Anti-Deception Coordination Centre (ADCC)	National Scam Response Centre (NSRC 997)	Anti-Scam Command (ASCom)	Anti-Online Scam Operation Center (AOC 1441)
Regulatory alignment across authorities	HKMA (banking, payments, and SVFs), OFCA (telcos and SMS controls), SFC (crypto, virtual assets, and capital markets), CCB & CSTCB (commercial and cyber crime police), HKPF (criminal investigation and asset recovery).	BNM (banking and payments), MCMC (telcos and SIM/network controls), SC (crypto and digital assets), NFCC (financial crime coordination and asset recovery), PDRM / CCID (commercial crime police and law enforcement).	MAS (banking, payments, and digital tokens), IMDA / MDDI (telcos and SMS registry controls), SPF / ASCom (Anti-Scam Command and law enforcement), CAD (commercial crime police and asset recovery), GovTech / CSA (cybersecurity and digital platform safeguards).	BOT (banking and payments), NBTC (telcos and SIM controls), SEC (crypto and digital assets), AMLO (asset recovery and return), RTP / DSI (police and law enforcement), ETDA (social media and digital platform safeguards).
CROSS-SECTOR DATA & INTELLIGENCE SHARING	FINEST (interbank), Scameter and Scameter+ app (threat indicators), with the Anti-Deception Alliance and FMLIT . Pools suspect accounts, numbers, and URLs → real-time pre-transaction alerts on FPS , internet banking, physical branches, and ATMs; banks also exchange risk assessments and mule indicators bilaterally, with no central database.	National Fraud Portal (NFP) , by BNM with PayNet and member institutions. Pools transaction-level data network-wide → end-to-end fund tracing, multi-tier mule-chain mapping, rapid interbank freeze notices via NSRC 997.	ScamShield ecosystem for public reporting of suspected scam calls and messages and blocking of scam calls and SMS messages; co-located bank staff at ASCom conduct live fund tracing and freezing.	Central Fraud Registry (CFR) , via National ITMX , linked to AOC 1441. Pools interbank records (amounts, timestamps, accounts) → money trails, mule-to-victim and mule-to-mule mapping (flagging potential victims and mules), dynamic fraud scoring on PromptPay before settlement.
LEGAL MECHANISMS ENABLING EXPEDITED INTERVENTION	Banking Ordinance and Banking (Amendment) Ordinance 2025 , with supervisory circulars; PDPO guidance permits bilateral interbank sharing of risk indicators within customer confidentiality.	Financial-sector and anti-financial-crime frameworks with enforceable BNM policy documents; Penal Code (Act 574) and Criminal Procedure Code amendments criminalize mule accounts and grant expedited freezing powers.	OCHA, Protection from Scams Act 2025 and the SRF .	Emergency Decree on Technological Crimes B.E. 2566 (2023, amended 2025) : safe harbor from PDPA and banking secrecy for cross-sector sharing; banks may freeze suspicious accounts without a court warrant.

Mapping of Fraud Mitigation Taskforces

Hong Kong SAR: Hong Kong SAR adopts an **intelligence-first, pre-loss engagement model**. The HKPF-run Scameter and Scameter+ app let the public check details such as accounts, phone numbers, and links for scam risks, with color-coded ratings. Suspicious Account Alerts and broader use of Scameter data enable FIs to identify risky transactions, warn customers, and take preventive action. If losses occur, a 24/7 stop-payment mechanism covering all 28 retail banks supports rapid fund recovery. This is reinforced by the Anti-Deception Alliance, where bank staff, ADCC officers, and law enforcement coordinate intelligence sharing, enabling swift fund interception and victim intervention. The HKMA co-manages the stop-payment mechanism and, under the Banking (Amendment) Ordinance 2025, provides legal protection for bank-to-bank information sharing.

Malaysia: Malaysia's model is built around a **shared fraud-response infrastructure**. The National Fraud Portal (NFP), operated by PayNet, underpins the NSRC and connects financial institutions, law enforcement, telecommunications providers, and regulators. It automates case handling, fund tracing, information sharing, and mule-account assessments, while enabling coordinated responses through the NSRC 997 hotline and participating financial institutions.

Singapore: Singapore fronts its taskforce with a **single consumer-facing brand backed by co-located enforcement**. The ScamShield Suite – the four-digit 1799 helpline, app, website, and alert channels – consolidates checking and reporting into one recognizable entry point, with most calls being pre-scam checks that avert losses before money moves. The app directs scam victims to lodge police reports, following which the Anti-Scam Command and Anti-Scam Centre, with co-located staff from seven banks, will conduct swift freezing and fund tracing. MAS continues to work with banks and other financial institutions to strengthen preventive safeguards and facilitate timely intervention.

Thailand: Thailand operates a **registry-centered, one-call architecture**. The Central Fraud Registry (CFR), operated by the Thai Bankers' Association, serves as the system backbone, while the AOC 1441 hotline and TCSC provide operational coordination. A single report can suspend accounts across the transfer chain, with reporting, account suspension, and police case filing integrated into a one-stop process. The BOT requires institutions to incorporate CFR data into real-time monitoring, while tracing and asset recovery are coordinated through TCSC and AMLO.

Annex III. Fraud mitigation taskforces compared

VICTIM / PUBLIC	CORE PLATFORM		WHO ACTS
Hong Kong SAR Scameter / Scameter+ app · ADCC / ADA			
Helpline 18222 Police Anti-Deception Coordination Centre	Scameter / Scameter+ app HKPF-run risk labels; “High Risk” alerts across FPS, internet banking, physical branches, and ATMs under Suspicious Account Alert mechanism.	Banks / SVFs / FIs 24/7 stop-payment, upstream alerts across all 28 retail banks	
Self-check Scameter / Scameter+ app Check payee before paying	ADCC / ADA 10 retail banks co-located in the ADCC as the Anti-Deception Alliance	Police · ADCC 24/7 case triage, intelligence exchange, and interception at the beneficiary bank	
		Regulator · HKMA Co-runs stop-payment, monitoring expectations. Banking (Amendment) Ordinance 2025	
OUTCOMES	USD 268 M intercepted 2025 (+41%) 4,060 upstream interventions (+69.4%); USD 52 M intercepted, USD 61.5 M prevented (2025) 10 / 28 banks in ADA / upstream scheme		
Malaysia NFP · NSRC 997			
Own bank 24/7 hotline Bank lodges the case directly into the NFP; no separate call needed.	NFP National Fraud Portal – operated by PayNet under NSRC (NFCC · RMP · BNM · MCMC); automates incident intake, fund tracing, information sharing, and mule-account assessment; receiving institutions earmark funds inside the banking system.	Banks / FIs Earmark and hold suspected funds	
Hotline 997 NSRC		Police · RMP Leads NSRC operations, investigation, and recovery	
		Regulator · BNM Detection baseline · liability rules	
OUTCOMES	~ 30 min fund tracing (–75%) +54% monthly earmarked amounts (Dec 2025) +149% mule accounts detected (Dec 2025)		
Singapore ScamShield · ASC			
Helpline 24/7 1799 Check or report (over 85% of calls are pre-scam checks)	ScamShield Suite Single consumer-facing entry point; reports flow to ASC with 7 co-located banks, Crypto Tracing Team extends tracing to digital assets; international intelligence via GSE & FRONTIER+.	Banks (7 co-located) Swift freeze & fund tracing at ASC	
App / web ScamShield app Website & alert channels		Police · ASC Restriction Orders (Protection from Scams Act 2025); case disruption	
		Regulator · MAS Shared Responsibility Framework; FIDReC dispute resolution	
OUTCOMES	15,000+ accounts frozen 2025 SGD 117.7 M fiat recovered (≈22.8 M crypto) 1799 4-digit single entry point		
Thailand CFR · AOC 1441			
Hotline 24/7 1441 1 call, 3 lines: victim · bank agent · police. One-stop service.	CFR Central Fraud Registry (Thai Bankers’ Association) – single case entry, suspends accounts across the whole transfer chain. AOC 1441 & TCSC provide the command layer.	Banks / PSPs Customer-level freeze (three-tier rule framework); incoming → outgoing	
Online Thai Police Online (thaipoliceonline.go.th); FI hotlines		Police · RTP / CCIB Case filed on-call; TCSC-guided tracing + AMLO restitution	
		Regulator · BOT CFR data mandated in real-time monitoring	
OUTCOMES	-42% victim loss reduction in 2026H1 vs 2025H1 21% recovery rate (Feb 2026)		

Multi-layered Interventions across the Fraud Life Cycle

While all four jurisdictions adopt a multi-layered approach that combines consumer empowerment, behavioral safeguards, rapid intervention, and ecosystem coordination, each emphasizes a different point in the fraud-mitigation life cycle.

Hong Kong SAR places greater emphasis on pre-transaction verification and shared fraud intelligence, using tools such as Scameter, FMLIT, and FINEST to help both consumers and financial institutions identify risks before funds move.

Malaysia centers its approach on rapid reporting, tracing, and recovery, linking consumers directly to the National Scam Response Centre and National Fraud Portal to accelerate intervention and fund recovery.

Singapore focuses on influencing consumer decision-making through behavioral friction, verification tools, and protective interventions that interrupt scams before payments occur.

Thailand connects consumer awareness, verification, and reporting directly to a national fraud-response architecture through AOC 1441, the CFR, and coordinated bank – law-enforcement mechanisms, transforming individual reports into ecosystem-wide intelligence and response.

Together, these experiences illustrate that while jurisdictions may pursue the same objective of strengthening consumer resilience, they can do so through different combinations of behavioral, operational, intelligence, and recovery-focused interventions.

Annex IV. Interventions across the fraud life cycle – Hong Kong SAR

1 Awareness & Education	2 Verification & Self-Defense	3 Behavioral Safeguards	4 Intelligence-Led Intervention	5 Recovery & Continuous Improvement
Empowering consumers to avoid scams • Anti-Scam Consumer Protection Charters • Anti-Deception Coordination Centre (ADCC) campaigns • Banking-sector awareness programs • Elderly and youth outreach • Scam awareness media campaigns	Tools to check and verify before acting • Scameter website • Scameter+ app • Verify phone numbers • Verify bank accounts • Verify websites and platforms • Money Safe (safeguard designated deposits and release in-person via anti-scam focused verification) • Guidance and self-defense tips for consumers	Behavioral frictions before funds move • Suspicious Account Alert System • FPS warnings • Mobile banking alerts • ATM warnings • Branch transaction warnings • Cooling-off prompts for higher-risk transactions • Deactivate high-risk unused functions • Authorized payment scam alerts	Shared intelligence and fraud detection • Scameter+ app • FMLIT • FINEST • Anti-Deception Alliance • Real-time monitoring by banks • Public-private information sharing • Authorized payment scam monitoring system • Upstream Scam Intervention alerts	Supporting enforcement and resilience • ADCC fund recovery efforts • Fraud intelligence sharing • Mule-network analytics • Ongoing enhancement of Scameter ecosystem • Supervisory reviews and industry collaboration • Consumer redress and support mechanisms
PURPOSE Build awareness and risk recognition	PURPOSE Empower consumers to self-protect and verify suspicious counterparties before payment	PURPOSE Interrupt high-risk transactions before execution	PURPOSE Detect fraud earlier and disrupt mule-account networks	PURPOSE Improve recovery and strengthen system resilience

 **KEY INSIGHT** | Hong Kong SAR's distinctive strength is using shared fraud intelligence to support both consumers and institutions before a payment occurs.

Whole-of-ecosystem collaboration

Hong Kong Police Force (ADCC), the Hong Kong Monetary Authority (HKMA), banks and stored-value facilities, the Faster Payment System (FPS), telecommunications and technology partners, and consumers and communities work together to prevent and combat fraud.

Outcomes and impact (illustrative)

 **Scameter**
verification
tools

 **Suspicious
Account Alert
System**

 **FMLIT**
public-private
partnership

 **FINEST**
interbank
intelligence
sharing

 **ADCC** rapid
fraud response

Annex IV. Interventions across the fraud life cycle – Malaysia

1 Awareness & Education	2 Verification & Self-Defense	3 Behavioral Safeguards	4 Intelligence-Led Intervention	5 Recovery & Continuous Improvement
Empowering consumers to avoid scams #JanganKenaScam campaign - BNM scam awareness programs - Financial education network outreach - Public scam alerts and advisories - Targeted outreach for vulnerable groups (e.g., elderly, youth) PURPOSE Build awareness and risk recognition	Tools to check and verify before acting - Check suspicious phone numbers / SMS information (ScamChecker) - Verify bank accounts / recipient details (SemakMule) - Check websites and links (URL check) - Set transaction alerts and limits - Guidance and self-defense tips for consumers PURPOSE Enable consumers to verify suspicious counterparties before payment	Behavioral frictions before funds move - Risk-based customer profiling and monitoring - Transaction limits and spending controls - Device binding and strong authentication (e.g., biometrics) - Warnings for high-risk transactions - Detection of unusual patterns using data and AI PURPOSE Interrupt high-risk transactions before execution	Shared intelligence and fraud detection - National Scam Response Centre (NSRC) 997 hotline - Cross-institution information sharing (banks, telecoms, law enforcement) - Real-time monitoring and fraud detection - Mule-account detection and network disruption - Data and intelligence sharing across agencies PURPOSE Detect fraud earlier and disrupt mule-account networks	Supporting enforcement and resilience - National Fraud Portal (NFP) for reporting and redress - Recovery and restitution efforts - Account freezing and fund recovery - Continuous monitoring and enhancement (e.g., data analytics, typology tracking, policy improvements) - Consumer feedback and support mechanisms PURPOSE Improve recovery and strengthen system resilience

 **KEY INSIGHT** | Malaysia's distinctive strength is the integration of reporting, tracing, and recovery.

Whole-of-ecosystem collaboration

Government agencies (BNM, PDRM, NFCC, MCMC), financial institutions, telecom operators, digital platforms, industry associations, and communities work together to prevent and combat fraud.

Outcomes and impact (illustrative)



Faster scam response



More effective tracing and fund recovery



Stronger deterrence: mule networks disrupted



Greater ecosystem resilience



Continuous improvement: data-driven policy and interventions

Annex IV. Interventions across the fraud life cycle – Singapore

1 Awareness & Education	2 Verification & Self-Defense	3 Behavioral Safeguards	4 Intelligence-Led Intervention	5 Recovery & Continuous Improvement
Empowering consumers to avoid scams - ScamShield public awareness campaigns - Government and industry outreach - Financial literacy initiatives for all age groups - Timely scam alerts and advisories - Targeted outreach for vulnerable groups (e.g., elderly, youth) PURPOSE Build awareness and risk recognition	Tools to check and verify before acting - Check suspicious phone numbers / SMS (ScamShield) - Check websites and links (URL check) via ScamShield - Set transaction alerts and limits - Guidance and self-defense tips for consumers PURPOSE Enable consumers to verify suspicious counterparties before payment	Behavioral frictions before funds move - Contextual warnings before transfers - Cooling-off period for high-risk transactions - Money Lock to partition funds from digital transferability - No clickable links in official SMS and emails - Detection of unusual patterns using data and AI PURPOSE Create time and reflection to prevent losses	Shared intelligence and fraud detection - Real-time monitoring and fraud detection - Sharing of scam enablers with tech partners via the Global Signal Exchange to provide leads and enable take-down of scam assets - Mule-account detection and network disruption - Intelligence-led disruption of scam networks PURPOSE Detect fraud earlier and disrupt scam networks	Supporting enforcement and resilience - Anti-Scam Centre (ASC) for reporting and support - Account freezing and fund recovery - Continuous monitoring and enhancement (e.g., data analytics, risk modeling) - Consumer feedback and support mechanisms - Ongoing policy, regulatory, and technology improvements PURPOSE Recover funds and strengthen system resilience

 **KEY INSIGHT** | Singapore's strength lies in a whole-of-ecosystem approach that connects consumer empowerment, verification, and rapid fraud intervention throughout the scam life cycle.

Whole-of-ecosystem collaboration

Government agencies, banks, telecom operators, digital platforms, industry associations, and communities work together to prevent and combat fraud.

Outcomes and impact (illustrative)



Faster scam response



Fewer consumer losses



Stronger ecosystem collaboration



Greater ecosystem resilience



Continuous improvement and innovation

Annex IV. Interventions across the fraud life cycle – Thailand

1 Awareness & Education	2 Verification & Self-Defense	3 Behavioral Safeguards	4 Intelligence-Led Intervention	5 Recovery & Continuous Improvement
Empowering consumers to avoid scams - National public awareness campaigns - Public alerts and advisories across multiple channels - Financial literacy programs for all age groups - Timely scam alerts and advisories - Targeted outreach for vulnerable groups (e.g., elderly, youth) PURPOSE Build awareness and risk recognition	Tools to check and verify before acting - Check suspicious phone numbers / SMS information (Whoscall, DE-fence app) - Verify bank accounts / recipient details (Name Check, PromptPay name check) - Check websites and links (URL check) - Set transaction alerts and limits - Guidance and self-defense tips for consumers PURPOSE Enable consumers to verify and avoid scams before payment	Behavioral frictions before funds move - Contextual warnings before transfers - Risk-based transaction limits - Stronger customer profiling and monitoring - Device binding and multi-factor authentication (e.g., biometrics) - No clickable links in official SMS and emails - Detection of unusual patterns using data and AI PURPOSE Interrupt high-risk transactions before execution	Shared intelligence and fraud detection - AOC 1441 one-stop hotline - Real-time fraud detection and fund tracing (e.g., FRx) - Mule-account detection and network disruption - Cross-agency and cross-sector information sharing (banks, police, AMLO) - Rapid takedown of scam infrastructure (websites, accounts, SIMs) - Intelligence-led investigation and coordination PURPOSE Detect fraud earlier and disrupt scam networks	Supporting recovery and resilience - Fund recovery and restitution to victims - Consumer support channels and case assistance (e.g., 1441, banks) - Account freezing and rapid response with financial institutions - Continuous monitoring and enhancement (e.g., data analytics, risk modeling) - Ongoing policy, regulatory, and technology improvements PURPOSE Recover funds and strengthen system resilience

 **KEY INSIGHT** | Thailand's distinctive strength is the coordinated, multi-layered approach, where rapid intervention creates multiple layers of protection.

Whole-of-ecosystem collaboration

Consumers, financial institutions, payment service providers, BOT, MDES, TCSC, police (RTP), AMLO, SEC, telecom operators, digital-asset operators, and online platforms share data, align safeguards, and coordinate responses.

Outcomes and impact (illustrative)



Faster scam response



Fewer consumer losses



Stronger ecosystem collaboration



Greater ecosystem resilience



Continuous improvement and innovation

Broadening the Scope, Strengthening the Response: Thailand's Framework for Safeguarding the Financial Sector from Illicit Activities

As fraud has become increasingly intertwined with broader illicit activities, the Bank of Thailand (BOT) has expanded its mandate beyond digital fraud to target channels used to move, conceal, or convert illicit proceeds. In collaboration with key authorities – including the Ministry of Finance, Ministry of Digital Economy and Society, Anti-Money Laundering Office (AMLO), Royal Thai Police, and Securities and Exchange Commission (SEC) – the BOT has strengthened safeguards across six critical areas: cash transactions, gold trading, foreign exchange, digital assets, customer due diligence, and suspicious transaction monitoring.

Operationally, these interventions enforce heightened controls on large cash withdrawals and gold purchases, alongside tighter limits on foreign exchange transactions. For digital assets, authorities have mandated customer profiling and Travel Rule compliance. Across the broader financial system, defenses are

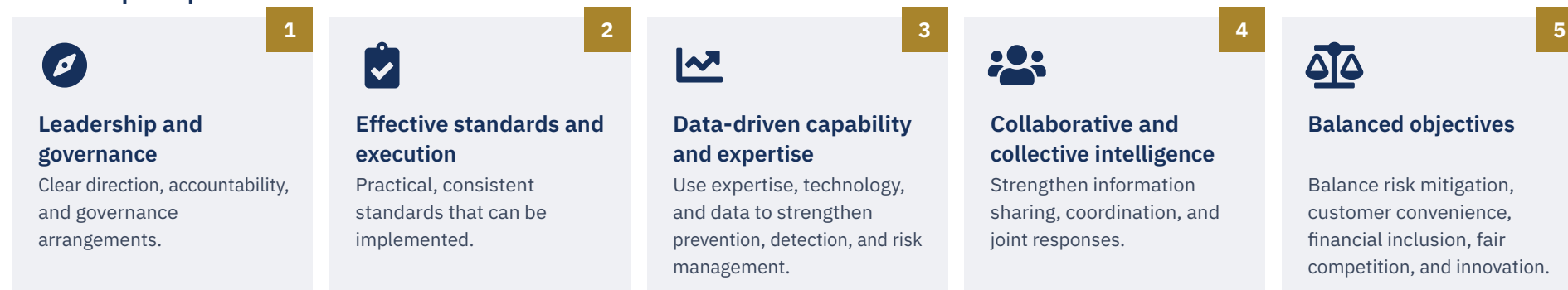
reinforced through upgraded Know Your Customer (KYC), customer due diligence (CDD), and enhanced due diligence (EDD) requirements, coupled with real-time monitoring of anomalous transaction patterns.

Building on these efforts, the BOT and the financial sector jointly launched the Framework for Safeguarding the Financial Sector from Illicit Activities. The initiative unifies supervised institutions across 11 industry associations – including commercial banks (TBA, AIB), state financial institutions (GFA), payment providers (TEPA), foreign exchange operators (TAFEXS), and six non-bank lending groups.

This shared commitment operationalizes collective defense into coordinated action across five core principles: leadership and governance; effective standards and execution; data-driven capability and expertise; collaborative and collective intelligence; and balanced objectives.

Annex V. Thailand's framework for safeguarding the financial sector from illicit activities

Five core principles



Collaborative efforts and key commitments across the financial sector

1 Bank of Thailand  - Strengthen regulatory standards and supervisory expectations - Analyze and share risk insights, patterns, and best practices - Coordinate with authorities and international counterparts	2 Banks and financial institutions  including state-owned and foreign banks - Strengthen KYC/CDD/EDD and customer verification - Set standards for high-risk accounts and transactions - Enhance monitoring of high-risk transactions	3 Payment service providers  - Strengthen KYM for merchant onboarding and KYC/CDD/EDD for customers - Provide transaction data and insights for system-wide monitoring
4 Foreign exchange businesses  - Strengthen customer due diligence, including risk and PEP screening - Establish AML/CFT industry guidelines - Build risk-management capacity and information sharing	5 Non-bank lenders  - Strengthen monitoring of high-risk customers and transactions - Share information on unusual transaction patterns and financial behavior	6 Digital-asset sector  in collaboration with the SEC - Apply customer profiling requirements - Implement the Travel Rule, especially for stablecoins such as USDT - Strengthen oversight and risk management



BANK OF THAILAND



PUEY UNGPHAKORN
INSTITUTE FOR
ECONOMIC RESEARCH