EPA ASIA

WORKING GROUP FOUNDING MEMBERS

HSBC sumsub aws

COMBATTING FRAUD AND SCAMS IN PAYMENTS

TOWARDS A WHOLE OF ECOSYSTEM SIGNALS-BASED FRAMEWORK

NOVEMBER 2026

1. Executive summary

Cyber-enabled fraud and scams have become a major concern for both the private and public sector, costing billions of dollars annually, harming consumers and adversely impacting trust. Fraud and scams increasingly involve complex global chains of contact, customer manipulation, payments and onward movement of monies. This white paper proposes an approach and direction for cross-sectoral cooperation across the Asia Pacific (APAC), so organisations can connect what they observe with timely, lawful and effective action. It builds upon recent efforts to forge a coordinated global strategy, most notably the Bangkok Blueprint for Fraud-Resilient Financial Services, developed by the IMF and World Bank Group in partnership with the Bank of Thailand and launched on 14 October 2026.

The principal recommendation is for EPAA to support its members as they work together, and with relevant public and private-sector initiatives, to develop a reference baseline for what participants should observe, assess, share and address, together with a pilot protocol. EPAA would engage in further policy work to define the legal and regulatory requirements needed to support robust intelligence sharing.

This is an industry contribution to the Bangkok Blueprint's key considerations (KCs) on a system-wide "Fraud-Detection Architecture" (KC5) and domestic collaboration (KC10), supporting prevention (KC4), response (KC6), cross-border cooperation (KC11) and consumer protection (KC12). Banks and payment service providers (PSPs); social media, marketplaces and other digital platforms; and telecommunications providers (telcos) should be expected to meet necessary duties, and national implementation should reflect risk, visibility and resources, using compatible standards that support lawful regional cooperation.

Signals indicate a possible fraud, scam or manipulation. Useful sharing requires reliable matching, evidence quality, an accountable recipient, timely action, feedback and correction. A risk score alone cannot establish wrongdoing or assign responsibility. Cooperation should enable upstream prevention as well as payment intervention, response and recovery. There should be a move to augment investigation and post-event intelligence-sharing with the pre-event stage, which unlike the former, often require decisions within seconds at point of payment. Liability frameworks that depend on whether payment was authorised means that most scam losses remain unaddressed.

The eight pillars in Section 6 describe what is needed to implement this approach. Start with a defined domestic use case or legally supported cross-border pilot, agreeing duties, signal standards and response procedures. The objective is earlier detection and disruption, reduced harm and effective recovery, with proportionate friction and safeguards against false positives. Wider adoption should follow evidence of mutual benefit, affordable participation and better customer outcomes.

2. Why current approaches miss the attack chain

Scams and fraud begin upstream and are increasingly sophisticated

Scams and fraud often begin through digital services or telecommunications well before the payment is made. Impersonation, grooming and coercion can make deception hard to recognise. The availability of AI tools means that scams and frauds are increasingly sophisticated and targeted, blunting the effectiveness of traditional customer education. The transfer of funds can be immediate and is increasingly the final step in a sustained attack.

Fragmented visibility across the ecosystem

The lengthy chain involving a number of unconnected organisations creates gaps that threat actors can exploit. Take a hypothetical investment scam. An individual sees an advertisement using the name and branding of a legitimate investment firm. The conversation moves to a messaging service or a phone call, and eventually the individual is given instructions to make a payment.

A social media platform may see the impersonation. An identity provider may notice something unusual during account opening. The sending institution sees a new beneficiary and a payment being made. The receiving provider may see unusual inflows followed by rapid onward transfers. The money may then move again and again, including across national borders.

Each organisation holds a different part of the picture. No one organisation should be expected to see everything on its own. In Thailand, 84% of transfers from victims to mule accounts recorded in the Central Fraud Registry cross institutional boundaries, so no single institution sees the full chain. [23] In many cases, it is technically impossible and legally prohibited to do so.

The practical problem is the handover. The organisation that sees the risk first is often not the organisation with the legal authority, customer relationship or technical capability to intervene later.

The immediate challenge is not necessarily 'how to build one giant database containing everything', which may be premature solutioning and carries its own risks and challenges. The challenge is more immediate and practical: what are the minimum useful signals, who can see them, who genuinely needs them, how quickly do they need them, and what are they expected to do when they arrive?

Common definitions and formats can help organisations make sense of data, while legal certainty allows the system to work in practice. Speed and quality will increasingly become important as the expectation moves from post-event investigation to upstream disruption.

Incomplete picture and the need for information sharing

The authorised and unauthorised classification of payments fraud remains useful for reporting and investigation and is well established within card payments. [1] However, this classification is of less value for account-to-account payments. It does not capture the full deception involved, does not identify opportunities for earlier intervention, and is not a reliable guide to who should bear the loss.Rules add to complexity, for example, Malaysia's rules prevent banks from treating a transaction as authorised only because the customer authenticated it. [26]

Many within the payments ecosystem are already subject to robust and regulated controls. Upstream activity and non-bank losses, which can harm the consumers well before any payment is made, may lack the same robust oversight and can be missed. Under-reporting, inconsistent classification and duplicate reports add uncertainty for organisations. In Thailand, for example, only 11.4% of surveyed victims who suffered losses reported them to the authorities. [23] Often, lower reported losses or complaints do not necessarily mean better prevention.

Yet information sharing between a wide group of disparate organisations without protections can expose organisations to reputational and legal risks, associated with privacy, data retention and tipping-off obligations. In addition to risk aversion, the sheer cost and inertia involved in sharing information will lead many organisations to do as little as possible, without an incentive to do so.

Low-quality data can overwhelm recipients and systems and make it difficult to distinguish signal from noise. Baseline standards should make signals understandable, proportionate and affordable to ingest.

The ideal is to strike the right balance. Incentives should reward useful, qualified and structured information, within a clearly defined legal framework.

Regulatory responses remain uneven

Shared responsibility regulatory regimes are emerging across APAC, though their approach and scope differ. Australia's Scams Prevention Framework (SPF) applies to the banking, telecommunications and digital platform sector, designated in May 2026, subject to transitional provisions, with expansion to PSPs expected later. [3, 4, 22] Singapore's Shared Responsibility Framework assigns duties to financial institutions and telcos for specified phishing scams. [11] In Malaysia and the Philippines, liability for fraud losses depends on whether the institution, the customer and, in the Philippines, third-party service providers met defined duties. [26, 27] Thailand's amended Emergency Decree has the widest reach, applying duties and proportional liability to banks, payment service providers, digital-asset operators, telcos and social media platforms. [23] Appendix A sets out some of these approaches in more detail.

The challenge is to link those organisational compliance obligations through timely and practical cooperation and to ensure support and encouragement for useful information sharing.

Regulatory challenges abound. In addition to privacy, data retention and tipping off concerns, requirements around bank secrecy, data localisation, and competition regulation can also inhibit cooperation and information sharing.

An illustrative scam journey

Figure 1 follows the hypothetical investment scam, from deceptive contact to movement of funds and recovery efforts. The actors, signals and actions are examples. Reporting and protective action can begin at any stage.

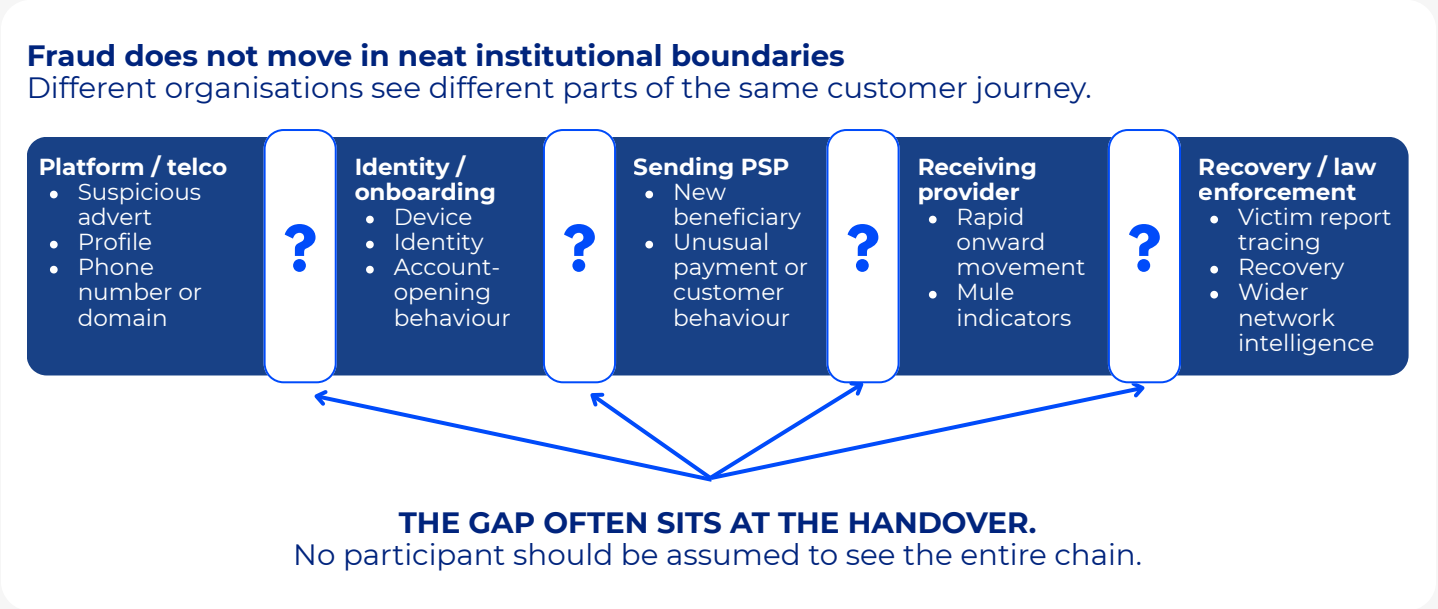


Figure 1: Scam journey and intervention points. Exchanges include crypto exchanges. Each participant acts within its lawful authority.

A social media platform may recognise a fraudulent advertisement but lack the beneficiary account, while a bank sees the account without the advertisement. Effective handover connects relevant, lawfully available identifiers, evidence and timing with a team within an organisation able to respond.

After payment, the same intelligence may support receiving-side investigation and prevent further movement. A request to trace, hold or return funds does not confer that power; legal authority, rules and procedures remain necessary, and effective operational mechanisms are needed for requests to be actioned efficiently.

3. The case for a signals-based framework

What signals are

Signals are observable indicators of possible manipulation or fraud in content, behaviour, identity, devices, channels or transactions. Banks and PSPs already use signals within their own organisations. Sharing signals between organisations adds context that helps distinguish an anomaly from an indication of wrongdoing.

Signals exist across the entire ecosystem

A social media platform's fraudulent-advertiser report and a receiving financial institution's unusual-transfer pattern may reveal a connected attack. Relevant observations can inform decisions at any stage, including reporting, tracing and recovery after payment.

The signal lifecycle

Figure 2 shows the information pathway and correction loop. Each recipient assesses the signal's relevance and its authority to act. Feedback should update confidence, validity and expiry so warnings do not remain unresolved indefinitely.

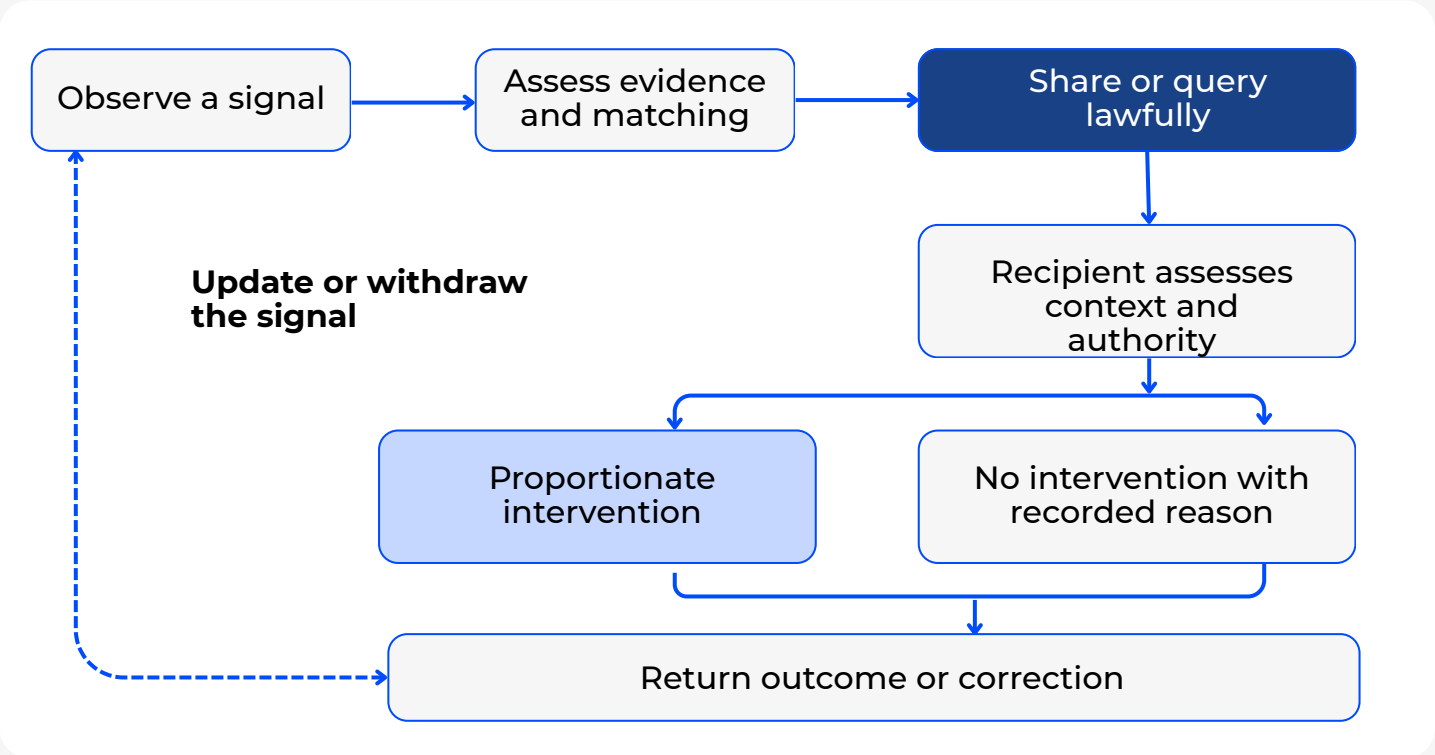


Figure 2: Signal lifecycle and correction. Sharing informs decisions; each participant retains its own prevention duties.

Signal pathways and scoring

Shared observations can connect the attack chain when timely, relevant and reliably matched. Recycled phone numbers, shared devices and duplicate reports can create misleading associations. Rules and practices on when a mobile number can be reassigned differ between jurisdictions, so matching needs to account for a number's history. Some authorities now help: India's Digital Intelligence Platform shares mobile numbers disconnected for reasons such as cybercrime involvement or failed re-verification with banks and other participants in near real time. [2]

A shared signal should ideally include its accountable source, unique case reference, observation and update times, relevant identifiers and matching context, reason and supporting evidence, confidence, urgency, permitted purpose and recipients, expiry or review date, and a correction contact. It is important to distinguish allegations, assessed suspicions and substantiated findings.

Alerts derived from one allegation are not independent corroboration. Common conventions can support local models without requiring one regional risk score.

Additional identifiers should only be used where necessary and lawful for the purpose. A phone number linked with account, device or transaction context may improve matching, but combined data can amplify error or expose personal information. Check recycled numbers, shared devices and common names explicitly.

Red, amber and green grades can support triage, with agreed meanings and calibration for each use case. Record confidence and urgency separately: an urgent allegation may remain unverified. The illustrative grades below include a distinct category for missing or unassessed information.

Grade	Meaning	Possible response
Red	Strong, relevant evidence of elevated risk. Record urgency separately.	Prioritise assessment and lawful, proportionate action. No automatic finding of wrongdoing.
Amber	Credible concern needing context or corroboration.	Verify, warn, monitor or refer for analyst review.
Green	No elevated risk found in the stated scope and period.	Apply ordinary controls. This is not an assurance of safety.
Unknown or unassessed	Missing, stale, unavailable or unassessed information.	Record the gap and use the appropriate fallback. Do not treat missing evidence as green.

Figure 3: Example of red, amber and green grades to support triage

Timely intervention

Interventions can include contextual warnings, independent verification, monitoring or escalation. Payment holds and account restrictions need a stronger evidential basis, legal authority, time limits and review. Signals should also support receiving-side investigation and recovery after payment. The Bangkok Blueprint recognises that containment can be triggered by risk indicators alone, without first attributing the fraud or determining liability (KC6). [10] In the Philippines, detection by an institution's fraud management system is one of the grounds for temporarily holding disputed funds while the transaction is verified. [25,27]

Authentication may not interrupt manipulation of the genuine customer by the threat actor. Interventions should address the suspected deception and provide trusted verification routes, while reaching receiving institutions where onward movement or recovery remains possible.

Timing should fit the decision window. That window can be very short: in Thailand, stolen funds leave the first mule account within about two minutes, and half leave the banking system within three minutes, while victims typically take around 30 hours to report. [23] Active payments may require rapid checks, while emerging campaigns may allow time for analyst review. Define fallback procedures for unavailable services and missing information. Absence of a flag is not evidence that a transaction is safe. Prevention needs to be the focus.

Signals support shared responsibility

Responsibility should follow visibility, capability, lawful authority and the ability to prevent harm at source, consistent with the Bangkok Blueprint's expectation that detection responsibilities reflect each entity's role and visibility (KC5) [10]. Signals can also show that a payment, although authorised, was made under deception. That is why they are a better guide to responsibility than authorisation status. Signals can inform what an organisation reasonably knew and how it responded, but prevention and compensation decisions have different evidential and procedural requirements. An organisation should not be treated as knowing information held in a shared system that it did not receive or could not reasonably match to its own customer or transaction in the time available. Baseline duties should discourage avoidable gaps in observation.

4. Implications for industry

Detection and disruption

Fraud detection increasingly connects upstream and cumulative evidence with existing controls. AI tools should be tested for accuracy and unintended effects, with accountable decision owners, human review of uncertain cases and audit trails.

Sending, receiving and upstream providers should connect their response capabilities where possible and explore the additional value and unintended effects of common data, rules, analyst judgement and statistical models through pilots and testing.

Response teams need authority to decide within the available time. Empower trained analysts, supported by automation and specialist escalation, with clear decision limits, audit trails and access to senior or legal advice.

Enabling technology, such as an intelligence sharing exchange operator, should be informed by local conditions but should be based on widely accepted standards that allow for interoperability across sectors and national borders.

Intelligence sharing

Ideally intelligence sharing between organisations should be informed by use case, while smaller providers need affordable access and proportionate integration support.

Participation should include useful contributions, responses and corrections. Common specifications and fair access terms reduce integration costs. Expectations should reflect information organisations lawfully hold or should reasonably observe in performing their own function, without rewarding indiscriminate collection. The objective should be high-quality and actionable data.

A minimum quality standard

Define minimum provenance, source validation, matching, recency, evidence, deduplication and correction requirements for each use case. Distinguish confirmed evidence from urgent unverified reports. One universal confidence threshold will not suit every situation, and weak or repetitive alerts should not improve apparent compliance.Verified organisation identifiers such as LEIs and BICs can support recipient validation; they can supplement use-case-specific matching of accounts, people and events.

Measure precision, meaning the share of assessed alerts identifying a substantiated relevant risk, alongside timeliness, coverage of confirmed scams and correction rates. Disclose sampling, unresolved outcomes and incomplete labels. If there are exchange operators, they should monitor contributors and use cases, with independent review and supervision. Use feedback for remediation and escalate severe or persistent failures.

Governed communities of trust

Governance should define membership, access criteria, contribution and response duties, security, auditability, dispute resolution and suspension. Identify the operator(s), compliance oversight and conflict procedures. Affordable access should support smaller providers and new market entrants. Shared intelligence should not lead to commercial exclusion or disclose unrelated competitively sensitive information. Privacy enhancing technologies can reduce unnecessary disclosure, but they do not establish legal permission or guarantee accurate matching.

Data collection and measurement

Distinguish victims, incidents, transactions and reports, and separate attempts from completed losses. Disclose coverage and reporting changes. Measure alert quality, missed scams, response times, wrongful restrictions, correction, repeat victimisation and recovery alongside loss. Report the channel through which funds left, such as a remittance to an overseas account, separately from the institution holding the fraudster's account, so that intermediaries acting on the victim's instructions are not inadvertently recorded as mule-account holders.

A blocked transaction may be legitimate, duplicated or attempted elsewhere; it is not automatically a prevented scam. Record gross loss, recovered funds, compensation and remaining victim loss separately to distinguish harm reduction from redistribution. A balanced scorecard that includes qualitative measures as well as monetary losses will assist in a more holistic approach. The Bangkok Blueprint's measurement annex makes similar points, noting that better reporting may at first increase recorded fraud and suggesting indicators such as time-to-freeze and reimbursement ratios also be considered. [10]

Responsibility and liability

Responsibility should reflect the function performed, reasonably available information, authority and ability to verify, maintain, share or act. Where several failures contribute, consider defined duties, causation and each organisation's contribution.

This matters where a scam payment passes through more than one provider before reaching the fraudster, for example where a customer funds an onward transfer through another provider. A provider acting on its own customer's instructions has a different role, and different information, from the institution holding the account into which the fraudster or mule receives the funds, and liability frameworks should recognise that distinction (KC5). [10]

Many liability regimes still turn on whether the customer authorised the transaction. That test is a poor guide to responsibility for scams, where a genuine customer authorises a payment under deception. The Bangkok Blueprint recognises that a transaction may be validly authorised yet still fraudulent when made under deception, manipulation or coercion (KC12), and that liability arrangements should cover both authorised and unauthorised fraud (KC6). [10] Regimes limited to unauthorised transactions leave most scam losses outside any framework: unauthorised transactions are only 3% of reported cases in Thailand, and authorised social engineering made up 81.8% of Singapore's scam cases in 2025. [23] Allocation should clearly turn on each participant's duties, information and fault across the attack chain, not on whether the final payment instruction was technically authorised.

Regional regimes differ in scope, trigger and allocation (see also Appendix A). Malaysia's framework covers unauthorised transactions only and places the loss on the bank unless it proves the customer was at fault. Singapore's covers specified phishing scams and places the loss on the party that breached a prescribed duty. The Philippines makes institutions and their service providers liable where they fail in defined duties. Thailand's applies across banks, PSPs, digital-asset operators, telcos and platforms, allocating liability in proportion to involvement, which may be waived on proof of compliance. Australia addresses the two separately: unauthorised transactions mainly through the ePayments Code, and scams, where the customer is typically deceived into authorising the payment, through the Scams Prevention Framework. Hong Kong SAR is considering a framework for authorised push payment fraud. [22, 23, 26, 27]

Legal liability for customer reimbursement requires its own evidential and procedural rules. [9] A signal or payment outcome alone cannot resolve liability.

Distinguish duties, breach and causation from the treatment of remaining customer loss. Compliance does not guarantee prevention, and loss alone does not establish a breach. Where all participants meet their duties, national policy must still determine access to reimbursement or other support and how any remaining loss is allocated. Remaining loss should not necessarily default to the payment provider closest to the customer. Any reimbursement arrangement should be funded across the ecosystem, including the digital platform and telecommunications providers through which scams originate, consistent with the Blueprint's recognition that liability may extend beyond financial service providers (KC6). [10]

Contracts may allocate organisational responsibilities but should preserve customer rights and accessible redress. Scheme and network rules should not shift scam losses between participants in ways that bypass statutory frameworks or disregard each participant's role, information and fault.

Figure 4 summarises duties when signals are shared. If a signal is wrong, assess each role's performance, the recipient's ability to verify and the contributor's representation of reliability.

Function	Signal contributor	Exchange operator	Acting institution
Signal handling	Collect lawfully Qualify evidence Maintain identifiers	Route eligible signals Protect data and access Track receipt	Check relevance and match Assess confidence and urgency
Response	Disrupt within own role Share or escalate	Apply exchange rules Escalate missed handovers	Act within authority Record reasons; support review
Correction	Correct or withdraw Notify recipients	Propagate corrections Confirm receipt; keep audit trail	Review affected decisions Restore access if appropriate

Figure 4: Responsibilities for shared signals. Roles can overlap; sharing does not discharge prevention duties or determine liability.

Limits of education

Education should support contextual warnings, trusted verification and accessible human help. A response to a warning should not alone determine negligence or redress. Protective design should accommodate language, disability and digital-access needs. Sophisticated, targeted attacks can defeat familiar warning signs, so education should complement preventive design and coordinated intervention. Evidence from Thailand shows that understanding specific manipulation techniques protects better than generic digital hygiene, but that awareness fails once a scammer exploits urgency, fear or misplaced trust. [23]

Correcting errors and managing data retention

False positives can restrict legitimate customers; false negatives can allow scams to continue. Measure both. Review confirmed scams and sampled decisions for missed interventions, recognising that under-reporting limits detection estimates.

Set review and expiry rules by signal type, confidence, purpose and law. Investigative retention does not justify keeping a temporary flag active indefinitely. Revalidate time-sensitive identifiers, remove stale signals from decision use and segregate longer-lived evidence with access controls. Retention schedules need documented reasons and review rather than one arbitrary regional limit.

Measure wrongful restrictions, their duration and time to restore access, including disproportionate effects on migrant remittances, shared devices and thin financial histories. Blanket restrictions on payments to licensed remittance and payment providers should be avoided: they shift risk rather than reduce it, contrary to the Blueprint's focus on reducing system-wide exposure (KC4). [10] The acting institution should provide an accessible complaint entry point, explain decisions where lawful, and set review and escalation windows. Contributors and operators should correct and propagate errors; recipients should confirm reassessment. Preserve access to essential services where lawful and feasible. Suspected mule status should not become automatic permanent exclusion.

Thailand's experience is illustrative. In September 2025, expanded fund tracing caught legitimate merchants and others at scale, and some merchants stopped accepting QR payments. Authorities responded by limiting holds to the disputed amount, committing to release verified innocent account holders within four hours and centralising appeals. [23]

Incentives and accountability for participation

Organisations need clear incentives and disincentives to provide high-quality and actionable signals. Incentives may include good-faith protection, reciprocal intelligence, clear regulatory expectations, feedback and integration support. Reward effective controls and customer outcomes, not volume, so as to prevent high-volume, low-quality data.

Enforcement should target breaches of clearly defined requirements, including unjustified non-sharing, reckless contributions, misuse and persistent failure to correct errors. Non-sharing will happen where no lawful gateway or safe harbour exists, or where sharing would breach secrecy, tipping-off, data localisation or other legal obligations, including in the receiving jurisdiction. Appropriately qualified uncertainty should not be penalised because a suspicion is disproved. Use monitoring and remediation before escalation where appropriate, with an incentive framework to mitigate both over-reporting and over-restriction.

5. Implications for policymakers and regulators

Global Push against Financial Crime

There is a strong push at the global level to address financial crime. The Bangkok Blueprint, released by the IMF and World Bank Group in partnerships with the Bank of Thailand on 14 October 2026, sets out 12 key considerations (KCs) across five pillars. [10] A companion report by the Bank of Thailand and the Puey Ungphakorn Institute for Economic Research draws implementation lessons from Hong Kong SAR, Malaysia, Singapore and Thailand. [23]

This white paper provides an industry contribution to KC5 while connecting detection to legal foundations, prevention, response, cooperation and consumer protection. Appendix D maps the relationship. [10] FATF's fraud work reinforces the need for coordinated action, while the OECD also recommends to policymakers that robust and comparable data are essential for understanding the scale, nature and evolution of scams and fraud. [7, 8] Comparable data are essential to evaluate results.

Regulation must reflect the attack chain

We are also increasingly seeing regimes where obligations to fight scams and fraud cover organisations beyond banks, to include other organisations involved in contact, payment initiation, receipt, onward movement, reporting and recovery. This whole-of-sector approach is the basis for the sharing of signals.

Regional examples of this emerging approach include Australia's Scams Prevention Framework, which will begin in 2027 and has wider sector coverage by including banks, larger social media platforms and telecommunication providers. The SPF regime may be extended to other sectors such as payment service providers and superannuation funds in the future. [3, 4, 22] Thailand's amended Emergency Decree goes further, extending statutory duties to telcos, digital-asset operators and social media platforms and introducing shared liability and statutory safe harbours. [23]

Australia, India, Malaysia, the Philippines, Singapore and Thailand offer different legal scopes and operational models to information sharing and response; they should not be treated as equivalent permissions for cross-sector or cross-border exchanges.

Importantly, these regimes need to be clear on their expectations and obligations, including any duty to disrupt as this will inform how signals are acted on.

The Blueprint's companion report notes that upstream prevention is far more cost-effective than downstream recovery, though upstream providers often lack commercial incentives to curb scam traffic in the absence of legal compulsion. [23] A whole of ecosystem approach means that responsibility to report and act as well as liability should exist where scams originate in addition to where funds move.

Baseline observation and response standards

Governments have an important role to play in guiding and enabling an ecosystem-wide approach to combatting fraud and scams. They should identify a coordination lead to resolve cross-sector gaps. Financial, communications, digital platform and privacy regulators, with law enforcement and other relevant authorities, should agree responsibilities, gateways and oversight within their respective mandates.

Importantly, policymakers and regulators should set minimum outcomes and safeguards for observation, prevention, sharing, response and customer protection, including digital platforms. Given the payments industry's long history of collaboration on data standards, regulators can build on industry standards where possible, rather than bespoke, prescriptive national approaches that are hard to make work across borders. Duties should reflect what each participant can reasonably observe and control but not erode the strong protections that many within the payment ecosystem already provide. The Bangkok Blueprint makes the same point, warning that divergent rules create arbitrage and weakest-link vulnerabilities across interconnected systems (KC11). [10]

National authorities determine enforceable duties and supervision. Industry should co-design interoperable technical profiles and response procedures within those requirements, with consumer, privacy and competition input.

EPAA could convene this work and publish a reference baseline and pilot protocol without replacing rule making or committing participants before agreement.

Appendix C illustrates participant baselines. Any working group should distinguish mandatory national requirements from voluntary reference practices and identify gaps that need regulatory action.

Enable lawful cross sector intelligence sharing

Policymakers and regulators also have a role in helping to define eligibility, oversight, and the legal basis for information sharing. This includes legal routes for collection, use, disclosure and transfer.

The scope of safe harbour

Policymakers and regulators have an important role to play in respect of safe harbours. This should protect the lawful collection and use of data and provide appropriate protection from privacy, data retention, competition law and tipping off obligations. National legal design should clearly define coverage so as to provide comfort to organisations, exchange operators and consumers.

The Bangkok Blueprint supports this: it notes that existing safe harbours are often underused because of unclear scope and weak incentives, and calls for clearer safe harbours, with protection against civil liability, regulatory sanctions and confidentiality claims and accountability for misuse (KC2, KC8 and KC10). [10] Regional precedents include Hong Kong SAR's Banking (Amendment) Ordinance 2025, which protects banks sharing intelligence, and Thailand's Emergency Decree, which exempts banks, payment service providers, digital-asset operators and telcos from privacy and confidentiality liability when contributing to the Central Fraud Registry.[23].

Separate protection for good-faith sharing, from protection for reasonable reliance and proportionate action and for a reasonable decision not to act on a signal that could not be verified or matched. An incorrect signal should not automatically remove protection, but reliance should require reasonable care, relevant matching, records, review and correction. Exclude malicious or reckless conduct, misuse and failures of an organisation's own prevention duties. Coverage remains jurisdiction-specific; Singapore's Scams (Countermeasures) and Other Matters Act 2026 illustrates protections tied to define activities and conditions. [21, 24].

Safe harbour protections need to address collecting, sharing, using, and acting otherwise risk will pool at the payment layer. Similarly, they need to ensure that an organisation is protected if it acts on a signal provided by another organisation and that signal proves to be incorrect. Safe harbour protections are not a general exemption from existing legislative requirements but rather a carefully crafted protections to support and encourage cooperation and information sharing.

Embed signals into liability frameworks

Signals may inform liability assessments, but a probabilistic signal alone should not establish liability or knowing involvement, nor should receipt of a signal before the recipient has had a reasonable opportunity to match and assess it. Liability framework should define observation, sharing and action duties separately from breach, causation and reimbursement and address the remaining-loss question described in Section 4 without discouraging useful, qualified sharing. The Bangkok Blueprint recommends allocation that reflects where control and information sit and recognises that liability may extend beyond financial service providers to other actors that fail to actively disrupt or mitigate fraud losses (KC6). [10]

Support shared infrastructure

Signal registries, mule intelligence and cross-border coordination can support cooperation. A controlled exchange or query service may suit the use case better than a raw-data repository, though the depth and functionality of any enabling technology or exchange operator will be determined by local conditions.

The companion report to the Blueprint describes three models currently in use in the region: identifier pools that let the public and banks check an account, number or URL before paying (Hong Kong SAR's Scameter); peer sharing of one bank's risk flag with other banks (Hong Kong SAR's FINEST); and transaction-level money-trail utilities that trace and freeze funds once a report is made (Thailand's Central Fraud Registry and Malaysia's National Fraud Portal). [6] The first two are easier to implement and support prevention; the third gives the strongest tracing and recovery. [23]

Funding of shared infrastructure should follow the Blueprint's principles. Basic fraud mitigation, including shared utilities, should not be charged to end users; costs may be shared among providers, ecosystem participants and authorities; and pricing should be transparent, subject to oversight and not weigh disproportionately on smaller providers (KC3 and KC4). [10].

FRIDA as a European design comparator

On 25 September 2026, the European Payments Council (EPC) launched a Request for Proposal to select a provider to deliver and operate the Central Platform for the Fraud Information Distribution Arrangement (FRIDA). The proposed scheme supports secure fraud-data exchange between PSPs for account-to-account payments in the Single Euro Payments Area and other account-to-account schemes within the forthcoming Payment Services Regulation (PSR). [16,17] It is also designed to help PSPs meet the PSR requirement to participate in a fraud data-sharing arrangement. [17]

FRIDA combines common inter-PSP rules, practices and standards with a hub-and-spoke platform that orchestrates exchanges and supports alert lifecycle management. The selected provider is to design and deliver the platform with the EPC, operate and secure it, and support onboarding and users. [16,17]

As of the date of this white paper, draft rulebook version 0.1, published on 11 September 2026, is under consultation until 10 December 2026. The EPC aims to publish version 1.0 and technical specifications by June 2027, with effect alongside the PSR, currently expected in Q4 2028. FRIDA remains under development; the procurement does not demonstrate operational effectiveness. [17]

For APAC, FRIDA offers a design comparator for common rules, interoperability and accountable platform operation. Its published PSP-focused scope differs from this paper's wider cross-sector proposal. Any adaptation needs local legal gateways, upstream participant duties, affordable access, correction and customer redress. These are recommendations for APAC, not claims that FRIDA already supplies them.

Regional coordination and legal readiness

The Financial Stability Board's recommendations address cross-border data interoperability and legal frictions while preserving privacy and fraud prevention. [14] The September 2026 Asia-Pacific Economic Cooperation (APEC) workshop report highlights the limits of bilateral sharing and recommends scalable regional cooperation with proportionate safeguards. [19]

There are existing services in the region such as the Australian AFCX and the Malaysian National Fraud Portal. As well, Project Nexus is designed to link domestic instant payment systems through a scheme and governance framework. Participating central banks incorporated Nexus Global Payments in 2025 to advance implementation.[13] Compatible fraud signals and escalation could be explored through that governance.

The Bangkok Blueprint also suggests examination of pre-negotiated standing protocols for high-risk cross-border payment corridors, covering immediate notification, coordinated tracing, preservation of evidence and provisional freezing of funds pending formal legal processes (KC11). [10] The companion report explores a similar approach, with 24/7 single points of contact, standardised data channels and interoperable emergency freezing protocols, and fraud controls built into cross-border fast-payment links such as Project Nexus. Operation FRONTIER+, which links anti-scam units across 14 jurisdictions, is an example of what standing arrangements can achieve. [23] National and regional systems may offer useful fields and workflows, but it will be important to test their adequacy for each new use case.

6. Recommendations

The eight pillars are implementation capabilities supporting the Bangkok Blueprint. Figure 5 maps them to the signal lifecycle and Appendices B and D set out practical evidence and alignment with the Blueprint. Together they describe the capabilities needed to operate the framework. Jurisdictions should adapt the following recommendations to their risks, market structure and capacity.

Pillar	Observe	Assess	Share	Act	Report	Recover	Improve
Public awareness and education	●			●	●		
Regulatory frameworks	●		●	●			●
Law enforcement		●		●	●	●	
Private sector collaboration			●	●		●	●
Technology and R&D	●	●					●
Cybersecurity capability	●	●	●	●	●	●	●
Industry codes of conduct		●	●	●			●
Monitoring and reporting					●		●

Figure 5: Eight pillars across the signal lifecycle. Dots show primary links; other stages may also apply. Improve includes feedback, review and correction. R&D means research and development.

1. Assign owners and define baseline capabilities and responsibilities. EPAA could identify and work with its members to input into relevant private and public sector initiatives (e.g. FATF, ACAMS, ISO/TC 68, X9) to define minimum data requirements. Authorities would specify enforceable outcomes and legal permissions. Participants should agree observation, prevention, sharing and response duties, with independent consumer and privacy input.
2. Connect intelligence to response. Agree signal fields, quality measures, recipients' acknowledgement, escalation, intervention and correction. Establish governed trust arrangements with fair access and resolve legal gateways and safe-harbour boundaries. Use the worked example to test a protocol and record unresolved legal or operational gaps.
3. Make interventions proportionate and reviewable. Define lawful thresholds, purposes, retention, expiry, conditional protections, rapid correction and accessible independent review.
4. Strengthen recovery and customer help. Agree tracing and preservation route, a complaint entry point and review windows. Explain recovery, reimbursement, insurance and complaints. Provide assistance while participants resolve responsibilities.
5. Pilot and expand on evidence. Select a domestic use case or legally supported corridor and agree owners, baseline and evaluation method. Assess harm, precision, missed cases, response, restoration of access, recovery and participation costs before expansion. Run these workstreams in parallel. Use tabletop or synthetic-data exercises for unresolved flows; begin live sharing on within established permissions.

Consumer protection, inclusion, privacy and redress apply across all eight pillars. Judge success by protection and fair customer outcomes.

7. Conclusion

The Bangkok Blueprint identifies system-wide fraud detection architecture as one of the 12 mutually reinforcing considerations for fraud-resilient financial services (KC5).

Building the architecture requires more than continuous real-time detection and analytics.

Shared signals are foundational and can enable earlier action when evidence is relevant, matching is reliable and recipients have authority and capacity to respond.

However, also critical is defining duties, connecting lawful and accountable handovers, and testing whether they reduce harm. The framework must support organisations that collect, provide and act on signals and ultimately benefit consumers who suffer the costs of fraud and scams. Closing the gap will also likely require enforceable duties on upstream sectors and clearly defined legal safe harbours.

This white paper recommends that EPAA convene participants to contribute to a reference baseline and pilot protocol to support cross-border interoperability and national implementation of the Bangkok Blueprint and to engage in further policy work to define the legal and regulatory requirements needed to support robust intelligence sharing.

EPAA members were involved in the development of this white paper through the working group process. However, any views expressed in this white paper are solely the views of EPAA and do not necessarily represent the views of individual working group members, their organisations, EPAA Ambassadors or EPAA Members.

Working Group Founding Members

The Hongkong and Shanghai Banking Corporation Limited

The Hongkong and Shanghai Banking Corporation Limited is the founding member of the HSBC Group. HSBC serves customers worldwide from offices in 56 countries and territories. With assets of US$3,445bn at 30 September 2026, HSBC is one of the world's largest banking and financial services organisations.

Sumsub is the first AI-powered trust infrastructure for compliance operations at scale. It connects identity and business verification, fraud prevention, transaction monitoring, and risk workflows, helping teams reduce manual work and enter new markets.

Trusted by over 4,000 clients across financial services, crypto, mobility, trading, marketplaces, education, and iGaming, including Bybit, Bitpanda, Wirex, Avis, Vodafone, Duolingo, and Kaizen Gaming.

Amazon Web Services (AWS) is guided by customer obsession, pace of innovation, commitment to operational excellence, and long-term thinking. By democratizing technology for nearly two decades and making cloud computing and generative AI accessible to organizations of every size and industry, AWS has built one of the fastest-growing enterprise technology businesses in history. Millions of customers trust AWS to accelerate innovation, transform their businesses, and shape the future. With the most comprehensive AI capabilities and global infrastructure footprint, AWS empowers builders to turn big ideas into reality. Learn more at aws.amazon.com.

Working Group Members

- Adrian Ng - GLEIF
- Alexander Sotnikov - CMA
- Angela Gill - PaymentsNZ
- Arif Perdana - Monash University
- Brad Pragnell - EPAA
- Brendan Choo - Hawk
- Camilla Bullock - EPAA
- Damian Welshe - Remitly
- Damon Madden - ACI
- Danelle Denny - EPAA
- David Newington - UATP
- Edric Lian - Hawk
- Emily McCallum - EPAA
- Emre Durusut - FIS
- James Hunt - Feedzai
- Jason Chan - Sumsub
- Jessica Geraghty - CBA
- Kaiwan Turel - HSBC
- Katherine Cloud - Sumsub
- Mahesh Narayan - EPAA
- Mathilde Bonneau - PayPal
- Matt Kurlanzik - PayPal
- Mira Dy - Amazon
- Monica Jasuja - EPAA
- Nafis Alam - Monash University
- Paul Walsh - Metacert
- Pete McCormick - FIS Global
- Quinn Pham - iPID
- Rob Tesoriero - FIS Global
- Robert Harris - Feedzai

Appendix A Regional examples

Regulatory approaches

International: FATF's fraud roadmap and revised Recommendation 16 work address cooperation, recovery and payment transparency. [7,8] The Bangkok Blueprint was launched on 14 October 2026, with a companion report on implementations in Hong Kong SAR, Malaysia, Singapore and Thailand. [10, 23] These initiatives require national implementation.

Australia: The banking, telecommunications and digital platform sectors were designated under the Scams Prevention Framework by an instrument made on 28 May 2026, and the SPF Rules were registered on 31 August 2026. The SPF codes had not been made at the date of this white paper [4, 22] Unauthorised transactions are addressed separately, mainly through the ePayments Code administered by ASIC (currently a voluntary Code). Separately, the SMS Sender ID Register commenced on 1 July 2026, requiring unregistered branded sender IDs to be labelled "Unverified". [5] An unverified message may still be legitimate; registration does not guarantee safe content.

Hong Kong SAR: The Banking (Amendment) Ordinance 2025 gives banks legal protection when sharing intelligence with each other, supporting the FINEST interbank platform, which was extended to personal accounts in late 2025. The police-run Scameter lets the public and banks check accounts, phone numbers and URLs for scam risk before paying. [23]

India: The Department of Telecommunications' Financial Fraud Risk Indicator (FRI), launched on 22 May 2025 under its Digital Intelligence Platform, rates mobile numbers as medium, high or very high-risk using citizen reports, the national cybercrime reporting portal and intelligence from telcos, banks and other financial institutions. The ratings are shared with banks, payment service providers, insurers, securities intermediaries and pension entities, and banks and UPI providers use them to stop or flag transactions in real time. The platform also distributes a list of mobile numbers disconnected for reasons such as cybercrime involvement.

Malaysia: Bank Negara Malaysia's policy document on unauthorised e-banking transactions, effective 1 October 2024, covers only transactions the customer did not consent to, initiate or authorise. Payments a scam victim approved are excluded, and banks may not treat a transaction as authorised only because it was authenticated. A bank must first assess its own controls and bears the loss unless it proves the customer acted fraudulently, refused to cooperate or breached specified security obligations. For individuals and small businesses, losses must be allocated fairly and proportionately where both are at fault, and an investigation running beyond 14 working days triggers provisional credit of up to RM5,000. [26]

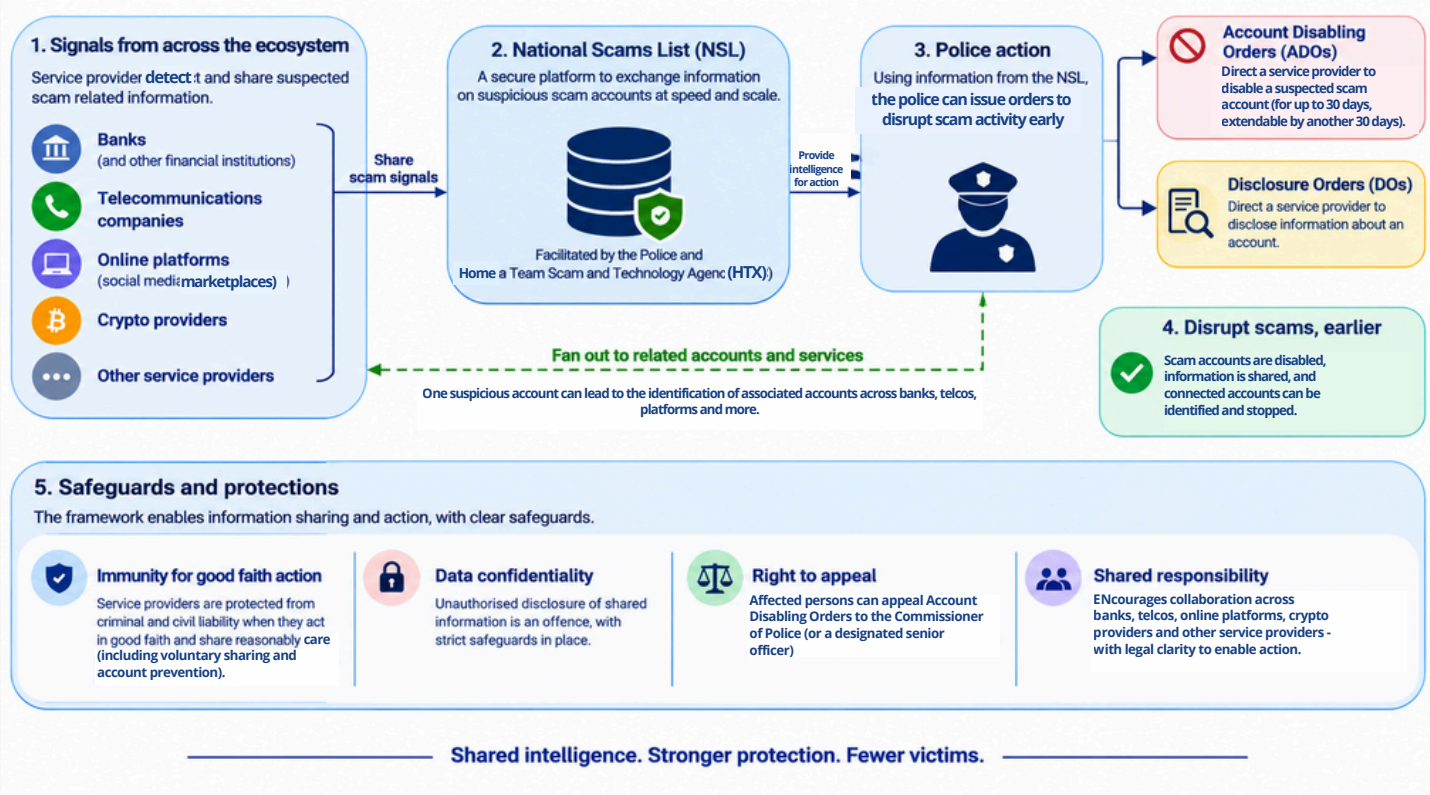
Philippines: Bangko Sentral ng Pilipinas (BSP) Circular No. 1214 of 2025 implements the Anti-Financial Account Scamming Act (AFASA) inquiry and authority-sharing process. It addresses bank secrecy and privacy restrictions within that process, with handling safeguards. [12] It does not establish a general private-sector gateway to exchange financial account data.

Separately, Circular No. 1215 of 2025 allows supervised institutions to hold disputed funds temporarily while the transaction is traced and verified. [25] Circular No. 1213 of 2025 requires real-time fraud monitoring and adopts a shared accountability framework, under which institutions and their service providers that fail in their duties may be liable for resulting losses. [27]

Singapore: The Shared Responsibility Framework took effect on 16 December 2024, assigning financial institutions and telcos duties for specified phishing scams and payout expectations where those duties are breached. [11] Its defined scope should be distinguished from a universal scam reimbursement model. The separate Scams (Countermeasures) and other Matters Act 2026 provides for police-provider exchange and specified account measures, rather than a general permission for unrestricted private-sector or cross-border sharing. [21, 24]

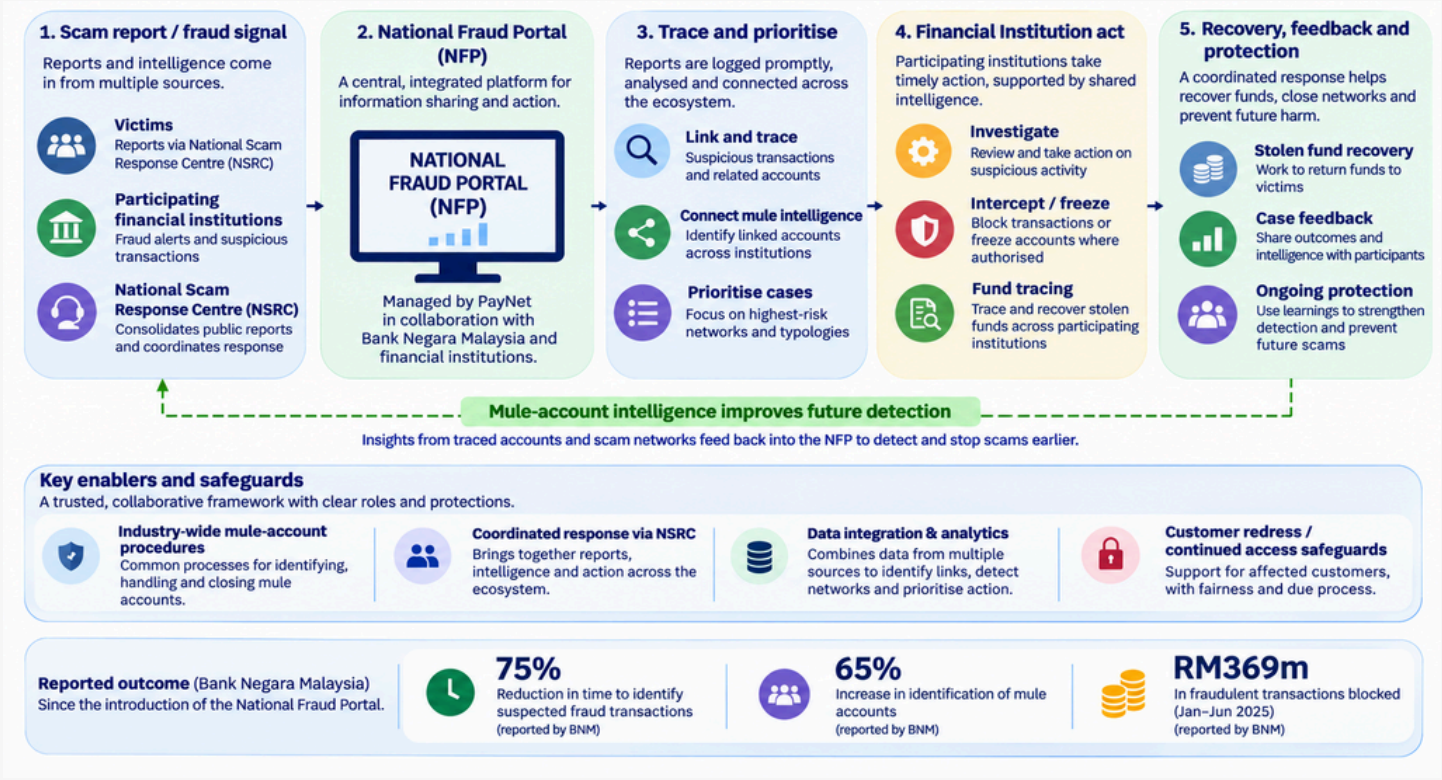
Thailand: The Emergency Decree on Measures for the Prevention and Suppression of Technological Crimes B.E. 2566 (2023) authorised 72-hour pre-complaint holds, criminalised mule accounts and SIMs, and established the Central Fraud Registry. Amendment No. 2 (2025) extended duties to telcos, digital-asset operators and social media platforms, introduced shared liability for negligence and statutory safe harbours for good-faith freezes and information sharing, and enabled fast-track asset return through the Anti-Money Laundering Office. [23]

Singapore: legally enabling the handover; and the action. Scams (Countermeasures) and Other Matters Act passed on 9 Sept 2026



EPAA illustration based on cited references.

Malaysia: From report to recovery



EPAA illustration based on cited references.

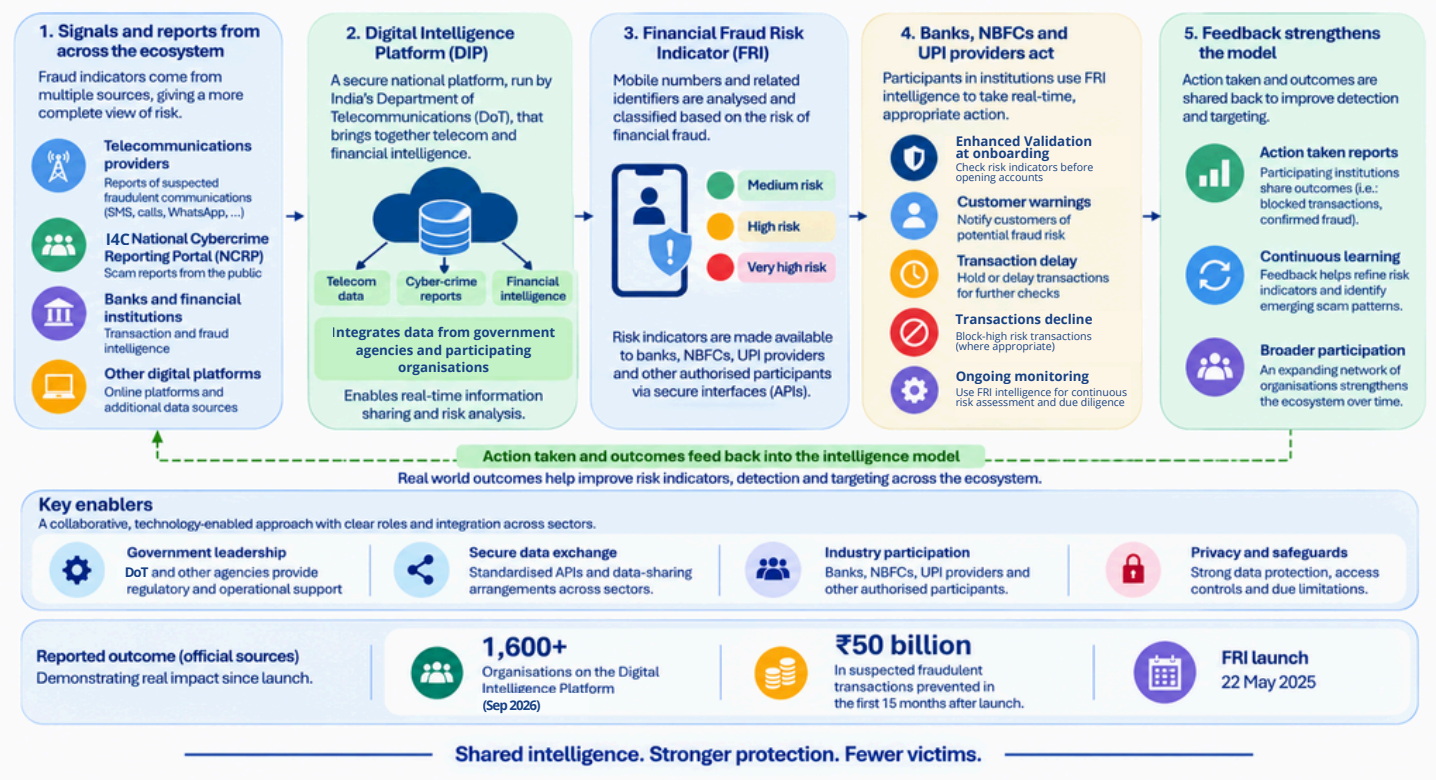
Report to recovery workflow

1 Report	2 Validate and trace	3 Financial institution response	4 Investigation and recovery	5 Feedback and safeguards
Victim reports through the NSRC or bank. NSRC validates the case.	The National Fraud Portal supports fund-flow tracing and information sharing among financial institutions.	Institutions assess linked activity and take authorised stapes to prevent onward movement and support recovery.	Law enforcement investigates; institutions and authorities coordinate tracing and recovery within their powers.	Record permitted outcomes, correct errors and preserve fair treatment and appropriate access to services.

Reported operational result: BNM's Annual Report 2024 records a 75% reduction in the time to obtain complete fund-flow information. This measure faster information gathering, not a 75% reduction in fraud. [20] The companion report records that in 2025 the National Fraud Portal reduced tracing times by 75% and increased mule-account detections by 149%. [23]

Illustrative workflow based on Bank Negara Malaysia's Annual Report 2024, with feedback and correction safeguards. Information exchange and intervention remain subject to applicable authority. [20]

India: From telecom signals to payment decision



EPAA illustration based on cited references.

Appendix B Applying the eight pillars across jurisdictions

Figure 5 summarises lifecycle links. The table below gives practical applications and evidence of implementation for each pillar.

This is an assessment tool, not a certification standard or country ranking. Adapt it locally and assess observable outcomes, including customer access and correction.

Pillar	Practical application	Evidence of effective implementation
1 Public awareness and education	Accessible warnings, trusted verification and reporting routes, and help suited to language, disability and digital-access needs.	Test comprehension, reporting and access to help. Measure behaviour and customer outcomes rather than campaign reach.
2 Regulatory frameworks	Define participant duties, lawful sharing, intervention powers, supervision, privacy safeguards and redress.	Duties and gateways are understood, auditable and usable. Cross-sector gaps are resolved, and customer protections operate.
3 Law enforcement	Usable referrals, evidence preservation, coordinated disruption, tracing and lawful cross-border cooperation.	Referrals reach the right authority with usable evidence. Assess disruption and recovery alongside investigation activity.
4 Private sector collaboration	Agree handling, reciprocal response and correction duties, trust governance and affordable access for smaller providers.	Alerts are acknowledged and assessed, with useful feedback. Examine failed handovers, coverage and participation costs.
5 Technology and research and development	Test detection, matching, interoperability and decision tools with proportionate data use and continuing validation.	Measure precision, missed cases, latency and cost against a baseline, including error and legitimate-customer impacts.
6 Cybersecurity capability	Protect credentials, signals, interfaces and evidence through access controls, integrity, resilience, incident response and supplier assurance.	Exercises demonstrate continuity and coordinate response if a participant, signal source or shared service is compromised.
7 Industry codes of conduct	Operational standards for quality, handling, escalation, intervention, retention, correction and customer help.	Monitor specific commitments. Codes support statutory duties and safeguards without creating otherwise absent powers.
8 Monitoring and reporting	Common definitions, deduplication, quality measures and outcome feedback for learning and oversight.	Distinguish attempts, loss, recoveries and compensation. Report wrongful restrictions, correction, missed cases and limitations.

Appendix C Illustrative participant baselines

These examples support the proposed baseline in Section 5. They do not prescribe final fields or create collection, disclosure or intervention powers.

Participant category	Examples of relevant observations	Response within the participant's role
Digital platforms	Advertiser or seller verification, listings, destination links, abuse reports and changed payment instructions.	Assess deception; address abusive accounts or content; preserve evidence and share lawful, scoped indicators.
Messaging services	Available account or channel metadata, impersonation reports, malicious links and abuse patterns.	Use lawful service controls and reporting. Do not presume access to encrypted or private content.
Telcos	Sender identity, spoofing, malicious-message reports, number status and reassignment.	Apply channel controls, validate number context and share timely indicators within applicable permissions.
Banks, PSPs, and wallets	Customer and payee context, transaction anomalies, account changes and received signals.	Assess payments and receiving accounts; intervene proportionately; support tracing, review and customer help.
Crypto exchanges and relevant virtual asset providers	Account or wallet identifiers, unusual transfers and evidence of scam proceeds within their service.	Assess service activity; act within authority; preserve evidence and coordinate referrals or recovery.
Identity providers and payment infrastructures	Verification inconsistencies, compromised identifiers, network patterns and inter-provider links.	Validate evidence, alert relevant participants and support matching and coordinated response.
MSMEs and other merchants	Suspicious orders, invoices, approaches and changes to settlement instructions.	Verify requests and report through accessible platform or PSP channels, with proportionate support.
Public agencies and law enforcement	Victim reports, linked cases, investigation intelligence and recovery requests.	Coordinate lawful referrals, preservation and investigations; return permitted outcomes or corrections.

Appendix D Alignment with the Bangkok Blueprint

The mapping is illustrative. The capabilities identity implementation capabilities and potential deliverables supporting the Blueprint's five themes and the key considerations shown [10]

Blueprint theme / key capabilities	Relevant public and private-sector capabilities	Proposed deliverable
Establish strategy and legal foundations (KC1 and KC2)	Regulatory framework; industry codes	Named coordination lead, defined duties, legal gateways and conditional protections.
Strengthen the fraud mitigation life cycle (KC3 and KC6)	Technology; collaboration; law enforcement	Tested signal and handover protocol, escalation and recovery routes.
Leverage existing risk mitigation and enforcement frameworks (KC7, KC8 and KC9)	Cybersecurity; law enforcement; monitoring	Integration with existing controls, incident handling and accountable review.
Expand domestic and cross-border coordination and cooperation (KC10 and KC11)	Private-sector collaboration; common standards	Governed participation, lawful corridor testing and compatible data profiles.
Promote consumer protection and resilience (KC12)	Education; monitoring; review and correction.	Accessible customer support, timely correction, restoration of access and outcome measures.

References

[1] Federal Reserve Financial Services. Stomp out Scams with the ScamClassifier Model. Source

[2] Government of India Ministry of Communications. 8 September 2026. Financial Fraud Risk Indicator prevents suspected cyber fraud transactions of over ₹5,000 crore. Source

[3] Australian Treasury Ministers. 28 May 2026. Albanese Government steps up industry protections to stop scams. Source

[4] Australian Federal Register of Legislation. 31 August 2026. Competition and Consumer (Scams Prevention Framework) Rules 2026, F2026L01140. Source

[5] Australian Communications and Media Authority. 1 July 2026. SMS Sender ID Register goes live to help protect Australians from scams. Source

[6] Bank Negara Malaysia and participating organisations. 20 August 2024. National Fraud Portal to solidify coordinated efforts in curbing financial scams. Source

[7] FATF. 2 July 2026. Event recording of the launch of the FATF Roadmap 2026–2028 on Combatting Fraud. Source

[8] FATF. 24 June 2026. Public consultation on guidance to increase payment transparency. Source

[9] Insurance Business, Roxanne Libatique. 8 September 2026. Bank impersonation scams surge as reimbursement and coverage lines blur. Industry commentary. Source

[10] International Monetary Fund and World Bank. Bangkok Blueprint for Fraud-Resilient Financial Services. Released 14 October 2026. Source

[11] Monetary Authority of Singapore and IMDA. 24 October 2024. Implementation of the Shared Responsibility Framework from 16 December 2024. Source

[12] Bangko Sentral ng Pilipinas. Circular No. 1214, Series of 2025. Rules for inquiry into financial accounts and sharing of financial account information by BSP pursuant to AFASA. Source

[13] Bank for International Settlements. Project Nexus. Project history, scheme development and handover to Nexus Global Payments. Source

[14] Financial Stability Board. 12 December 2024. Recommendations to Promote Alignment and Interoperability Across Data Frameworks Related to Cross-border Payments. Final report. Source

[15] UK Information Commissioner's Office. Pseudonymisation. Guidance on identifiability and data protection under UK law. Source

[16] European Payments Council. 25 September 2026. FRIDA Central Platform Request for Proposal. Source

[17] European Payments Council. Fraud Information Distribution Arrangement scheme overview and development timetable. Accessed 12 October 2026. Source

References

[18] Bank Negara Malaysia. 6 October 2026. Governor's special address at the 16th International Conference on Financial Crime and Counter Terrorism Financing. Source

[19] APEC Digital Economy Steering Group. September 2026. Workshop Summary Report APEC Workshop on Combatting Online Fraud and Scams. Source

[20] Bank Negara Malaysia. Annual Report 2024. Building a United Front Against Online Fraud Risk, pp. 98-102. Source

[21] Singapore Ministry of Home Affairs. 8 September 2026. Second Reading of the Scams (Countermeasures) and Other Matters Bill. Opening speech. Source

[22] Australian Federal Register of Legislation. Competition and Consumer (Scams Prevention Framework – Regulated Sectors) Designation 2026, F2026L00627, made 22 May 2026. Source

[23] Chantarat, S., Moenjak, T., Amarase, N., Suwannama, K. and Tosborvorn, T. October 2026. The Bangkok Blueprint in Action: Regional Experiences and Policy Lessons for Fraud-Resilient Financial Services. Bank of Thailand and Puey Ungphakorn Institute for Economic Research. Companion paper to the Bangkok Blueprint. Source

[24] Parliament of Singapore. Scams (Countermeasures) and Other Matters Bill, Bill No. 16/2026, passed 9 September 2026. Source

[25] Bangko Sentral ng Pilipinas. Circular No. 1215, Series of 2025. Regulations on the Temporary Holding of Funds Subject of Disputed Transactions and Coordinated Verification Process. 30 May 2025. Source

[26] Bank Negara Malaysia. 28 June 2024. Ensuring Fair Treatment for Victims of Unauthorised e-Banking Transactions (BNM/RH/PD 028-139), effective 1 October 2024. Source

[27] Philippines: Bangko Sentral ng Pilipinas. 30 May 2025. Circular No. 1213, Series of 2025. Amendments to Regulations on Information Technology Risk Management to Implement Section 6 of the Anti-Financial Account Scamming Act (AFASA). Source



EPA ASIA

The Emerging Payments Association Asia (EPAA) is a leading industry platform shaping the agenda for payments across Asia Pacific.

EPAA convenes members and organisations across the payments ecosystem to turn industry priorities into action through collaboration, policy engagement and thought leadership. Through Working Groups, industry forums, roundtables and collaborative outputs, EPAA provides a platform for organisations to contribute expertise, influence discussion and shape frameworks defining what comes next across the region's payments landscape.

This paper provides general information. It does not constitute legal, financial or professional advice, and should not be relied upon as such. While care has been taken in preparing this material, EPAA and the authors make no representations or warranties as to its accuracy, completeness or currency.

CONTACT US