Who Should Bear the Loss?
Liability Allocation for Authorised Push Payment Fraud in Real-Time Payment Systems

Comparative Evidence and Policy Design for Thailand's PromptPay

Thanatchon Chongmankhong

November 2026

Abstract

Real-time payment systems have shifted fraud from the theft of credentials to the manipulation of account holders into authorising transfers themselves. This *authorised push payment* (APP) fraud falls outside the unauthorised-transaction protections on which consumer payment law was built. This paper studies how regulators allocate APP losses among consumers, sending and receiving payment service providers (PSPs), telecommunications operators and digital platforms. It combines a comparative institutional analysis of the United Kingdom, Australia, the United States, Singapore, the European Union, Hong Kong, Malaysia, India, Brazil and Taiwan with a multi-party liability model. The model yields four results. First, any rule that merely redistributes the victim's loss (budget balance) induces every party to under-invest in prevention. Second, the best budget-balanced allocation assigns shares in proportion to each party's care productivity, and manipulation drives the consumer's optimal share to zero beyond a finite threshold. Third, when victims must prove a provider's breach, a nominally shared-responsibility regime collapses into *de facto* consumer liability. Fourth, decoupling compensation from penalties (compensation to victims plus fines to the state) restores first-best incentives. Applied to Thailand, the analysis shows that the 2025 amendment to the Technology Crime Decree adopted a modern shared-responsibility architecture but not the procedural machinery that makes it bite. The paper proposes a sequenced twelve-measure package centred on presumptive reimbursement for impersonation and phishing scams, a 50:50 split between sending and receiving PSPs, a binding financial ombudsman, multi-hop fund tracing on PromptPay and institution-level disclosure. In illustrative calibrations the package reduces the efficiency loss relative to the first best from about 85% under the current *de facto* regime to about 11%.

Keywords: authorised push payment fraud; fast payment systems; PromptPay; liability allocation; shared responsibility; social engineering; money mules; consumer protection
JEL: G21, G28, K13, K24, K42, O33

Note on sources. This version was compiled without live access to primary sources. Statistics, dates and penalty amounts reflect the author's best information as of mid-2026 and are approximate. Items marked † carry lower confidence and should be checked against the primary document before citation. All model parameters used in figures are illustrative and are not estimates.

1 Introduction

Fast payment systems (FPS) such as Thailand's PromptPay, the United Kingdom's Faster Payments, Singapore's PayNow, India's UPI and Brazil's Pix settle retail transfers within seconds, around the clock, and irrevocably (CPMI, 2016). Their success is remarkable. Their speed and finality have also changed the economics of fraud. When money moves instantly and cannot be recalled, the cheapest attack is no longer to steal a credential but to persuade its owner to press "send". This is *authorised push payment* (APP) fraud. The victim authorises the transfer, but only because a fraudster has deceived them.

APP fraud exposes a gap in the architecture of consumer payment law. From the US Electronic Fund Transfer Act (1978) to the EU Payment Services Directives, protection was built around *unauthorised* transactions. When the payer authorises the transfer, the default rule in most jurisdictions is that the loss stays with the payer. As fraud migrated into this gap, loss shifted onto those least able to prevent or absorb it.

The scale is large. Survey-based estimates by the Global Anti-Scam Alliance put global scam losses above US$1 trillion in 2024[†] (GASA, 2024). That figure is methodologically contested, but official national series show the same pattern (Fig. 5). For Thailand the problem has an additional dimension. The country sits beside the industrial-scale scam compounds of mainland Southeast Asia, where the UN human rights office estimated that at least 120,000 people in Myanmar and 100,000 in Cambodia were held in forced criminality (OHCHR, 2023).

This paper asks four questions.

Q1. How do central banks and regulators allocate APP losses, and with what results?

Q2. What do policy failures and reversals abroad, such as the UK's reduction of its reimbursement cap, teach?

Q3. Where does Thailand's current framework stand by comparison?

Q4. If social engineering cannot be eliminated, how should Thailand design its system to minimise losses and compensate victims promptly?

Contributions. The paper makes three contributions. First, it provides a structured comparison of APP-fraud regimes along eight dimensions, together with a fact-check of seven claims common in Thai public debate (Section 6). Second, it develops a multi-party liability model that formalises the joint-care problem among consumers, PSPs, telcos and platforms (Section 4). The model rationalises observed regime differences and yields testable predictions. Third, it translates these results into a sequenced, costed policy package for Thailand (Section 8).

Roadmap. Section 2 sets out a taxonomy of fraud and liability regimes. Section 3 reviews the literature. Section 4 presents the model. Section 5 reports the country cases. Section 6 compares the regimes and tests the seven claims. Section 7 asks whether social engineering is "unsolvable". Section 8 sets out policy design for Thailand. Section 9 outlines an empirical agenda, and Section 10 concludes.

2 Background and taxonomy

2.1 Three classes of payment fraud

We distinguish three classes because each places the point of failure, and therefore the natural locus of liability, in a different place.

Table 1. Four regimes for allocating APP losses.

Regime	Principle	Exemplar
Caveat emptor	Payer bears loss unless the transfer was unauthorised	United States (Reg E)
No-fault reimbursement	Reimbursement by default; exceptions for gross negligence	United Kingdom (2024)
Fault-based shared responsibility	Parties that breach defined duties compensate in a set order	Singapore (SRF); Thailand (2025)
Ecosystem duties + dispute resolution	Statutory duties on all sectors; an external body orders compensation; large fines	Australia (SPF Act 2025)

Unauthorised fraud. The fraudster initiates the payment without the account holder's consent, for example through malware that takes remote control of a phone. Most legal systems already protect consumers against this class.

Authorised impersonation fraud. The victim is deceived into believing they are dealing with their bank, the police or a government agency. Technical controls work best against this class: sender-ID registries, bans on links in bank messages, and cooling-off periods.

Authorised narrative fraud. The victim knowingly pays a counterparty they wrongly trust: an investment scheme, a romance or a fake job or purchase. Liability is hardest to assign here, and losses per case are largest.

In Thailand the line between the first two classes is blurred. Many "remote-access" cases begin with impersonation (class 2) and end with transactions executed by the fraudster's malware (class 1).

2.2 Four liability regimes

Across jurisdictions we observe four broad regimes (Table 1). Figure 1 positions jurisdictions on two axes: the *de facto* strength of consumer-facing reimbursement and the breadth of liability across the ecosystem.

3 Related literature

Economics of liability. The canonical starting point is Calabresi (1970): losses should fall on the *least-cost avoider*. Brown (1973) and Shavell (1980) formalise the comparison between strict liability and negligence. In bilateral-care settings a negligence rule with correctly set, verifiable due-care standards attains efficiency, whereas strict liability gives the victim no incentive to take care. Shavell (1987) and Landes and Posner (1987) extend these results and add risk allocation, which favours placing losses on the less risk-averse party. Holmström (1982) shows that when several agents' efforts jointly determine an outcome, no budget-balanced sharing rule induces efficient effort from all. This result is central to our multi-party setting. Becker (1968) and Polinsky and Shavell (1979) provide the theory of fines scaled by detection probability. Coase (1960) reminds us that liability assignments matter mainly when transaction costs prevent private reallocation, which is precisely the situation between atomised consumers and large firms.

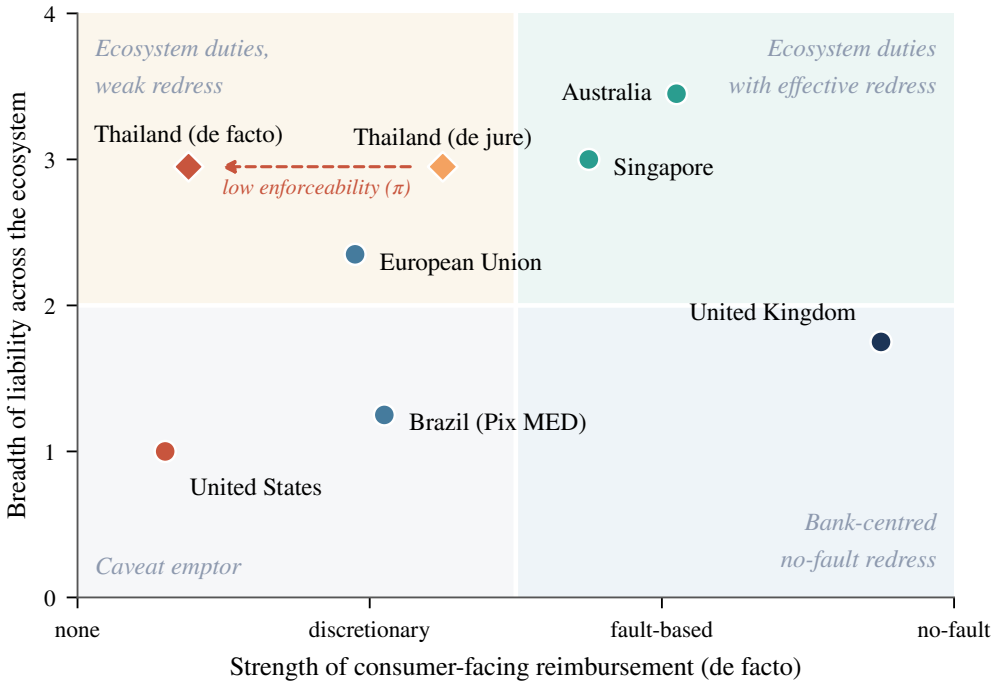


Figure 1. Conceptual map of APP-fraud liability regimes. Positions are the author's qualitative coding as of mid-2026. The arrow for Thailand shows how low enforceability (π) moves the *de jure* shared-responsibility design towards *de facto* consumer liability (Proposition 4).

Economics of security and payment fraud. Anderson (1993) documented that in British ATM fraud disputes, banks that could shift liability to customers invested less in security. That finding anticipates the modern APP debate. Anderson and Moore (2006) argue that misaligned incentives, not missing technology, explain most security failures. Moore et al. (2009) survey the economics of online crime and emphasise intermediaries as control points. Anderson et al. (2013) show that the indirect and defensive costs of cybercrime often dwarf direct losses.

Psychology of scam compliance. Stajano and Wilson (2011) identify principles that scammers exploit, including authority, urgency, herd behaviour and dishonesty. Cialdini (2006) documents the persuasion mechanisms underneath them. Modic and Lea (2013) find that susceptibility to persuasion predicts scam compliance. Kahneman (2011) explains why time pressure and fear move decisions from deliberative to automatic processing. Together this literature implies that consumer "care" is endogenous to manipulation, a point we formalise in Proposition 3.

Fast payments and public infrastructure. CPMI (2016) sets out the design trade-offs of FPS. Duarte et al. (2022) document how Brazil's central bank built Pix as public infrastructure, including the special return mechanism discussed in Section 5.5.

Gap. We are not aware of a study that (i) formalises liability allocation across all five actors in the APP chain, (ii) links the formal results to the observed regimes and (iii) applies them to Thailand. This paper aims to fill that gap.

4 A model of multi-party liability

4.1 Set-up

Five actors $i \in \mathcal{N} = \{C, S, R, T, P\}$ are the consumer, the sending PSP, the receiving PSP, the telecommunications operator and the digital platform. Each chooses a level of precaution $e_i \geq 0$ at cost

$$c_i(e_i) = \frac{e_i^2}{2k_i}, \qquad k_i > 0, \tag{1}$$

where a larger k_i means prevention is cheaper. A scam attempt succeeds with probability

$$p(\mathbf{e}) = p_0 - \sum_{i \in \mathcal{N}} a_i e_i, \tag{2}$$

a local linear approximation in which $a_i > 0$ is the marginal effectiveness of party i's care. A successful scam causes loss L. The planner minimises total social cost

$$\mathcal{W}(\mathbf{e}) = \sum_i c_i(e_i) + p(\mathbf{e})\, L, \tag{3}$$

which gives the first-best precaution $e_i^* = k_i a_i L$. We write

$$\theta_i \equiv a_i^2 k_i \tag{4}$$

for party i's *care productivity*. It combines how effective prevention is with how cheap it is.

4.2 Liability rules and the team problem

A liability rule assigns each party a share $s_i \geq 0$ of the loss. A rule is *budget-balanced* if $\sum_i s_i = 1$: compensation exactly equals the victim's loss. Allow also for imperfect enforcement. Party i expects to pay its share only with probability $\pi_i \in [0,1]$. The unpaid remainder reverts to the consumer. Party i's effective incentive share is $\sigma_i = \pi_i s_i$ for $i \neq C$, and the consumer's effective share is $\sigma_C = s_C + \sum_{i \neq C}(1 - \pi_i) s_i$. Each party minimises $c_i(e_i) + \sigma_i\, p(\mathbf{e})\, L$.

Proposition 1 (Team under-investment)**.** *Equilibrium care is $\hat{e}_i = \sigma_i e_i^*$. Under any budget-balanced rule with full enforcement, every party with $s_i < 1$ under-invests. Because $\sum_i s_i = 1$, all parties under-invest whenever at least two parties have positive care productivity and positive shares.*

The excess social cost of a regime has a simple closed form, which we use throughout.

Lemma 1 (Excess social cost)**.** *For effective shares σ,*

$$\Delta\mathcal{W}(\sigma) \equiv \mathcal{W}(\hat{\mathbf{e}}) - \mathcal{W}(\mathbf{e}^*) = \frac{L^2}{2} \sum_i \theta_i (1 - \sigma_i)^2. \tag{5}$$

Proposition 2 (Optimal budget-balanced shares)**.** *Among budget-balanced rules with full enforcement, social cost is minimised by*

$$s_i^* = \max\Big\{0,\ 1 - \frac{\lambda}{\theta_i}\Big\}, \tag{6}$$

where $\lambda > 0$ is the unique value that satisfies $\sum_i s_i^* = 1$. Shares increase in care productivity, and any party with $\theta_i \leq \lambda$ bears no share.

Proposition 2 generalises the least-cost-avoider principle. Because precaution costs are convex, the loss should be *divided*, with weights that rise with θ_i, rather than placed entirely on one party. This "water-filling" structure is shown in Fig. 2(b) for illustrative values of θ.

4.3 Manipulated consumers

The defining feature of APP fraud is that the fraudster attacks the consumer's decision process itself. Let $m \in [0,1]$ index the degree of manipulation, and let it scale down the effectiveness of consumer care, $a_C = (1-m)\bar{a}_C$. Then $\theta_C = (1-m)^2\bar{\theta}_C$ with $\bar{\theta}_C \equiv \bar{a}_C^2 k_C$.

Proposition 3 (Manipulation removes the consumer's share)**.** *Let λ_{-C} solve $\sum_{i\neq C}\max\{0, 1-\lambda/\theta_i\} = 1$. If $\bar{\theta}_C > \lambda_{-C}$, define*

$$\bar{m} = 1 - \sqrt{\lambda_{-C}/\bar{\theta}_C}. \tag{7}$$

Then $s_C^* > 0$ for $m < \bar{m}$ and $s_C^* = 0$ for all $m \geq \bar{m}$. If $\bar{\theta}_C \leq \lambda_{-C}$, then $s_C^* = 0$ for all m.

Because θ_C falls with the *square* of $(1-m)$, a moderate degree of manipulation is enough to make consumer liability inefficient. In the calibration of Fig. 2(c), $\bar{m} \approx 0.27$. Shifting loss onto a manipulated consumer barely improves care, but it does impose the whole loss on them.

Remark 1 (Risk bearing and first-party fraud). Two further considerations shape the consumer's share. First, if consumers are risk-averse and PSPs are diversified, moving loss to PSPs adds an insurance gain equal to the consumer's risk premium (Shavell, 1987). Second, full reimbursement invites false claims by "victims" who collude with the payee (first-party fraud). A small fixed excess and a complicity exception address the second concern without materially weakening the first.

4.4 Enforceability and the burden of proof

Proposition 4 (Enforcement wedge)**.** *Under a fault-based rule in which the victim must prove a provider's breach, π_i equals the probability that the victim succeeds. As $\pi_i \to 0$ for all $i \neq C$, $\sigma_C \to 1$ and $\sigma_i \to 0$. The regime converges to caveat emptor regardless of the nominal shares s_i.*

Victims cannot observe a bank's internal monitoring or a telco's filtering logs, so π_i is structurally low whenever the burden of proof sits with them. Figure 2(a) maps effective care $\hat{e}_i/e_i^* = \pi_i s_i$. A nominal share of 0.3 enforced with probability 0.2 delivers only 6% of optimal care. Foreign platforms without a local legal entity have low π_P for a different reason: cross-border enforcement is costly. This suggests a design rule. Liability towards the consumer should sit with high-π domestic entities (banks), which then pursue recourse against telcos and platforms. Inter-firm contracting is cheap; consumer-to-firm litigation is not (Coase, 1960).

4.5 Breaking budget balance

Remark 2 (Negligence with verifiable standards). If the regulator sets due-care standards $\bar{e}_i = e_i^*$ and can verify compliance perfectly, a negligence rule induces first-best care from firms, and the consumer, as residual bearer, also chooses efficiently (Brown, 1973). Singapore's Shared Responsibility Framework approximates this approach with a checklist of verifiable duties. It is efficient only to the extent that the duties are close to e_i^* and that breaches are verifiable.

Proposition 5 (Decoupling compensation and fines)**.** *Let each party pay compensation share s_i to the victim and a fine f_i to the state, so that $s_i + f_i = 1$ for all i. Equilibrium care then equals the first best for every party. If breaches are detected with probability q, the fine imposed upon detection must be*

$$F_i = \frac{f_i L}{q}. \tag{8}$$

Proposition 5 is the multi-party analogue of Becker's result. Fines break the budget constraint that drives Proposition 1. It gives a theoretical rationale for Australia's combination of compensation through the external dispute-resolution scheme and statutory penalties of at least A$50 million per contravention†. The risk is over-deterrence. PSPs facing large fines may freeze legitimate accounts too readily, so false-positive rates should be measured and penalised as well.

4.6 Channel displacement

Fraudsters allocate effort across channels $j \in J$ according to net returns $r_j = p_j L_j - \kappa_j$, where κ_j is the operating cost of the channel. Suppose regulation covers only a subset $J' \subset J$ of channels and the channels are substitutes. Then

$$\Delta\Lambda_{\text{total}} = \underbrace{\Delta\Lambda_{J'}}_{<0} + \underbrace{\Delta\Lambda_{J\setminus J'}}_{>0}, \tag{9}$$

so total losses fall by less than losses in the regulated channel. Figure 2(d) simulates this with logit substitution. Singapore's experience, discussed in Section 5.4, is consistent with the prediction.

4.7 Implications

Figure 3 applies Lemma 1 to seven stylised regimes. Three implications follow. First, the main lever is *not* the exact split of compensation. It is whether incentives are enforced (Proposition 4) and whether fines supplement compensation (Proposition 5). Second, a fault-based regime that leaves the burden of proof with victims performs almost as badly as caveat emptor. Third, the receiving PSP typically has high care productivity because it is the only node that can screen mule accounts across all scam types. That makes the 50% receiving-PSP share in the UK regime well grounded.

5 Country cases

Figure 4 summarises the regulatory chronology and Fig. 5 the reported losses. Definitions differ across countries, so we interpret within-country trends rather than cross-country levels.

5.1 United Kingdom: from voluntary code to mandatory reimbursement

The UK is the only jurisdiction studied that makes reimbursement of APP losses the default. Its history is the most instructive case in this paper.

Chronology. In 2016 the consumer group Which? lodged a super-complaint arguing that APP victims were unprotected. A voluntary Contingent Reimbursement Model (CRM) Code followed in May 2019, signed by around ten banking groups. Confirmation of Payee (CoP), which checks the payee's name before a transfer, began in 2020. Under the CRM Code, reimbursement covered roughly half of losses by value and varied widely across firms†. The Financial Services and Markets Act 2023 (s.72) then required the Payment Systems Regulator (PSR) to mandate reimbursement. The resulting policy statement, PS23/3 (PSR, 2023), set reimbursement within five business days, a 50:50 split between sending and receiving PSPs, and a proposed cap of £415,000.

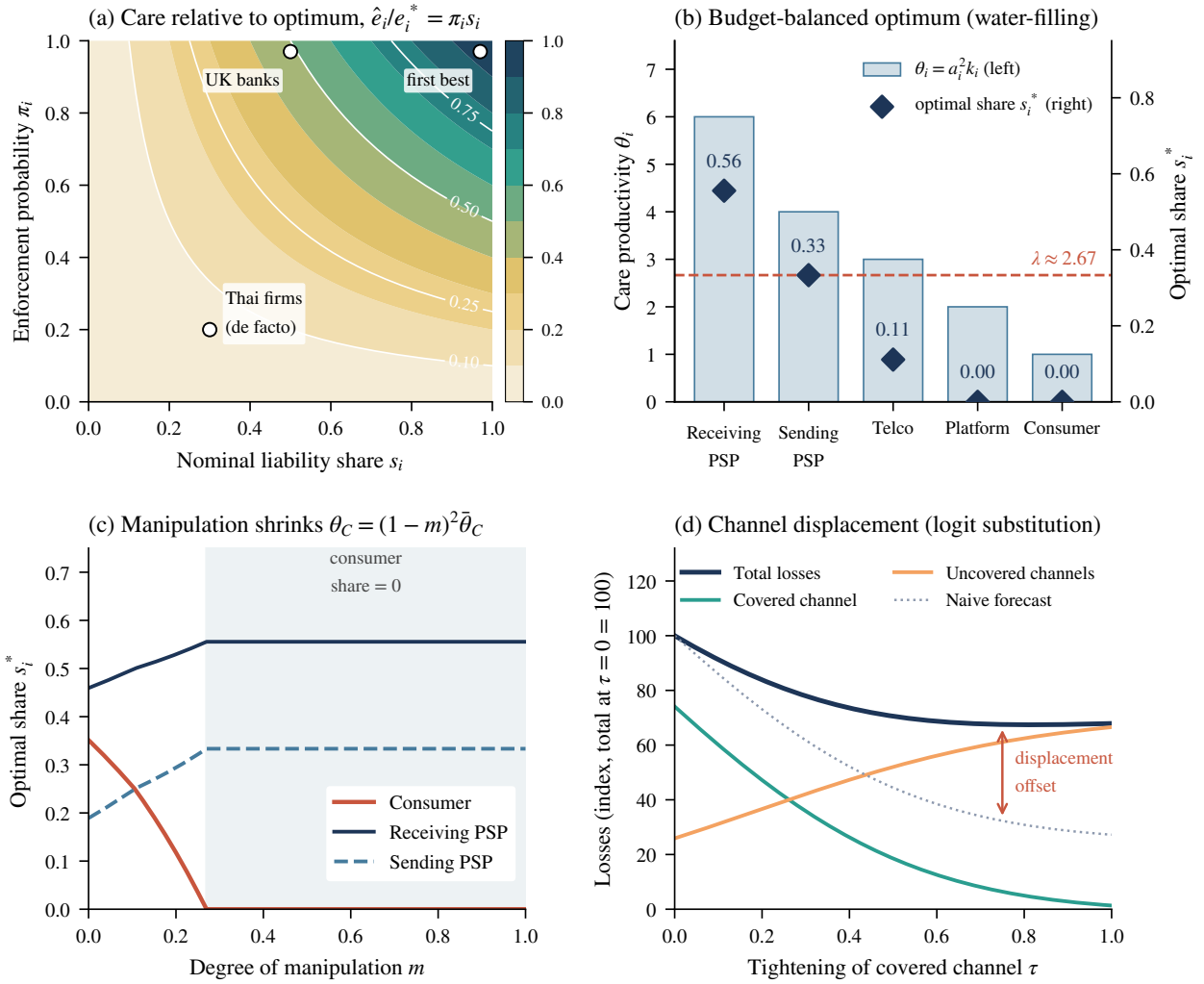


Figure 2. Model mechanics. (a) Effective care relative to the first best as a function of the nominal liability share and the enforcement probability (Proposition 4). (b) Optimal budget-balanced shares (Proposition 2): only parties with $\theta_i > \lambda$ bear loss. (c) As manipulation m rises, the consumer's optimal share falls to zero at $\bar{m} \approx 0.27$ (Proposition 3). (d) Tightening one channel lowers its losses, but substitution into uncovered channels offsets part of the gain. All parameters are illustrative; see Appendix B.

The reversal. After consultation, the PSR cut the cap to £85,000 in September 2024, aligning it with the deposit-protection limit, and allowed an optional excess of up to £100 (PSR, 2024). Industry had raised three arguments: (i) solvency risk for small PSPs and fintechs from a few large claims; (ii) incentives for first-party fraud; and (iii) the regime's failure to make telecoms and technology firms, where most scams originate, share the cost. The PSR stated that the lower cap still covered over 99% of claims by number†. The regime went live on 7 October 2024. In the same month, a legislative change allowed PSPs to delay outbound payments by up to four business days where fraud was reasonably suspected. In March 2025 the government announced that the PSR would be consolidated into the Financial Conduct Authority.

Outcomes. UK Finance reports APP losses of roughly £485m (2022), £460m (2023) and £451m (2024)† (UK Finance, 2025), while the share reimbursed rose markedly. Early PSR data suggested that around 85–90% of money lost was returned in the first year†. The regime changed *who bears* the loss far more than

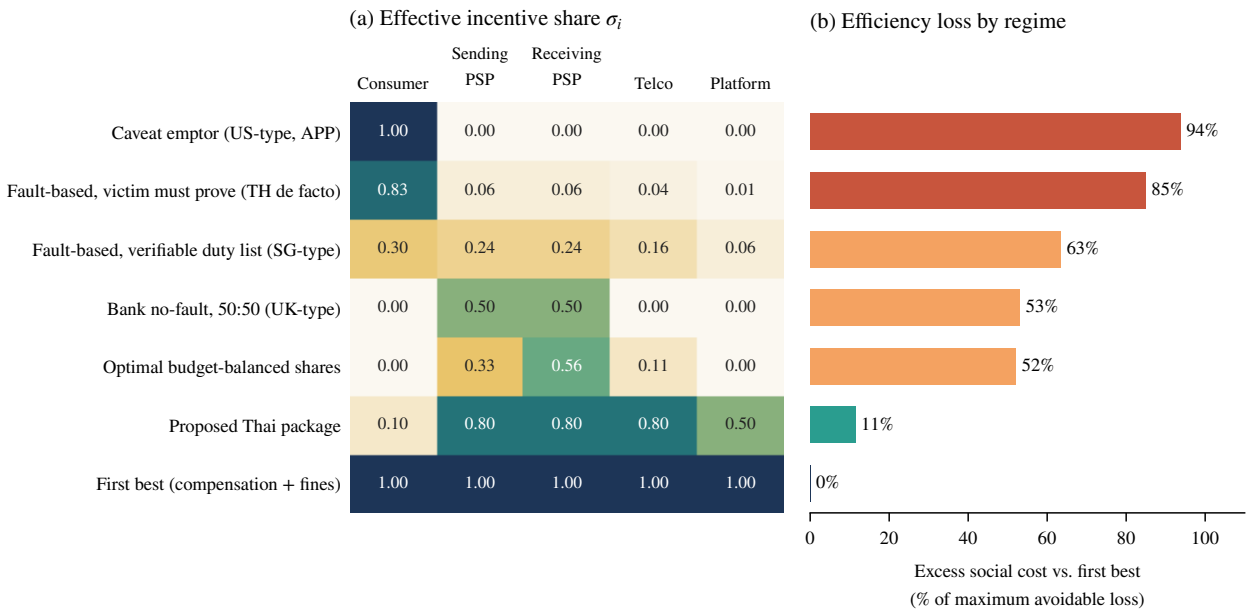


Figure 3. Stylised regimes in the model. (a) Effective incentive shares σ_i. (b) Excess social cost from Eq. (5), as a percentage of the maximum avoidable loss $\frac{L^2}{2}\sum_i \theta_i$. Within budget balance, re-allocating shares helps little: the UK-type 50:50 rule (53%) is close to the optimal budget-balanced rule (52%). Large gains require breaking budget balance or raising enforceability. Parameters are illustrative (Appendix B).

how large the loss is.

Lessons. The claim that the UK "imposed a harsh regime and had to retreat" is only partly true. The regulator retreated on the cap, not on the principle, and the UK remains the most protective regime studied. The key transferable elements are the receiving-PSP share, a cap anchored to an existing benchmark, and institution-level transparency. The unresolved weakness is platform liability. The Online Safety Act 2023 and the voluntary Online Fraud Charter (2023) do not make platforms contribute to reimbursement.

5.2 Australia: ecosystem duties and corporate-scale penalties

Australia chose a different path. It did not create default reimbursement. Instead it imposed statutory duties on banks, telecommunications operators and digital platforms simultaneously through the Scams Prevention Framework (SPF) Act, passed in February 2025[†].

The SPF Act designates sectors (initially banking, telecommunications, and digital platforms including social media, paid search advertising and messaging) and imposes six overarching principles: governance, prevent, detect, report, disrupt and respond. The Australian Competition and Consumer Commission (ACCC) is the general regulator, and sector codes set specific obligations. The most serious breaches carry penalties up to the greater of A$50 million, three times the benefit obtained, or 30% of adjusted turnover[†]. Victims can seek redress through the Australian Financial Complaints Authority (AFCA), which may order compensation from *any* non-compliant entity in the chain. Consumer groups criticised the absence of UK-style default reimbursement. As of mid-2026, effectiveness depends on sector codes that were still being finalised[†].

Complementary measures include the National Anti-Scam Centre (NASC, July 2023), the banking industry's Scam-Safe Accord (November 2023: CoP roll-out, biometric checks at account opening, friction on first-time payees), a telecommunications code on scam calls and SMS (2020), and an SMS sender-ID

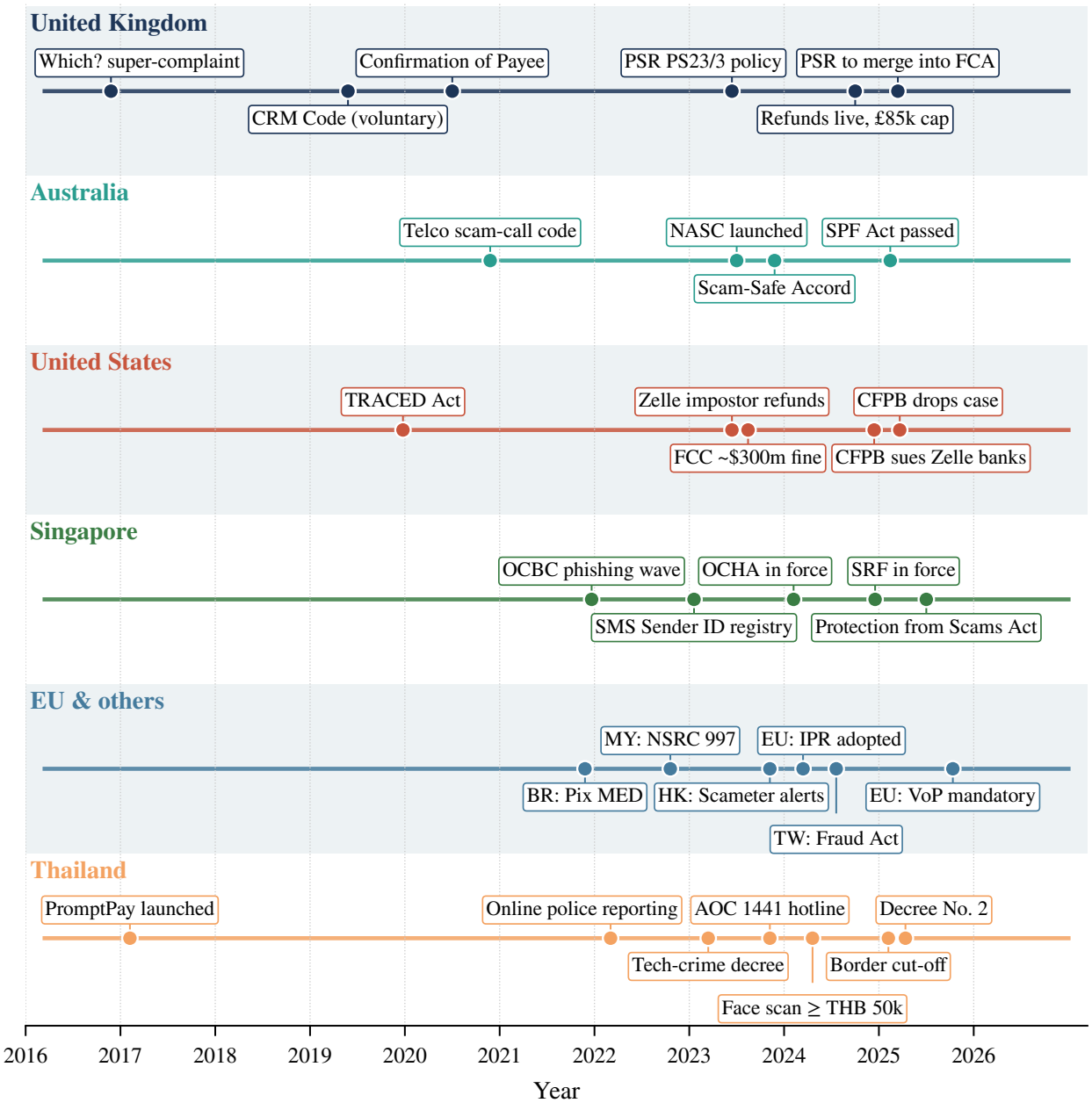


Figure 4. Chronology of major anti-APP-fraud measures, 2016–2026. Abbreviations: CRM, Contingent Reimbursement Model; PSR, Payment Systems Regulator; FCA, Financial Conduct Authority; NASC, National Anti-Scam Centre; SPF, Scams Prevention Framework; CFPB, Consumer Financial Protection Bureau; OCHA, Online Criminal Harms Act; SRF, Shared Responsibility Framework; BR, Brazil; MY, Malaysia (NSRC, National Scam Response Centre); HK, Hong Kong; TW, Taiwan; IPR, Instant Payments Regulation; VoP, verification of payee; AOC, Anti Online Scam Operation Center. Dates are approximate to the month; several carry † status in the text.

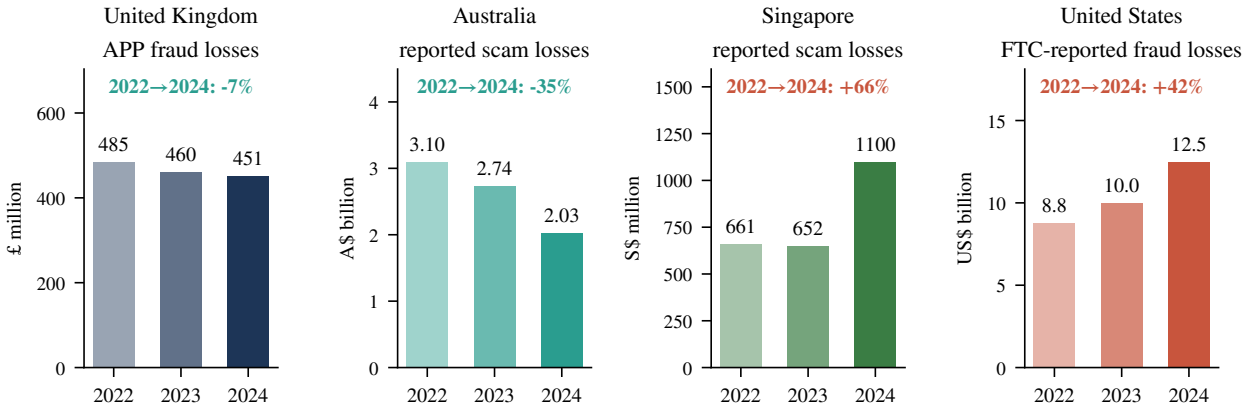


Figure 5. Reported fraud and scam losses, 2022–2024†. Series are not comparable across countries: the UK series covers APP fraud only (UK Finance), Australia's combines reports to several agencies (ACCC), Singapore's covers all reported scams (Singapore Police Force), and the US series covers all consumer-reported fraud (FTC Consumer Sentinel). No consistent annual series is published for Thailand.

register. Reported losses fell from about A$3.1bn (2022) to A$2.7bn (2023) and A$2.0bn (2024)† (ACCC, 2025). Australia is one of the few cases with a sustained fall in total reported losses, although changes in reporting behaviour may explain part of it.

Fact-check: "Australia fines Google and Facebook seriously". Australia has imposed substantial penalties on large technology firms, but mostly under consumer and competition law rather than scam law. Examples are A$60m against Google over location-data representations (2022), A$20m against Facebook and Onavo (2023), and roughly A$55m against Google over search-default agreements with Telstra and Optus (2025)†. The under-16 social-media law (effective December 2025) carries penalties of up to A$49.5m. Separately, Andrew Forrest's suit against Meta in a US court over scam advertisements using his likeness was allowed to proceed†. The accurate statement is that Australia has transplanted competition-law-scale penalties into scam regulation and has a record of enforcing against large technology firms, but no penalty under the SPF Act itself had been reported as of mid-2026†.

5.3 United States: severe on perpetrators, weak on redress

The United States records the largest losses in absolute terms. The FTC reported about US$12.5bn in consumer-reported fraud losses in 2024 (up about 25%), and the FBI's IC3 about US$16.6bn† (FTC, 2025; FBI, 2025). Yet it offers the weakest protection to APP victims among the cases studied.

The Regulation E gap. The Electronic Fund Transfer Act and Regulation E protect consumers against *unauthorised* electronic fund transfers. A transfer that the victim was deceived into authorising is generally outside that protection. The Zelle network, operated by bank-owned Early Warning Services, illustrates the consequences. After congressional scrutiny, the network adopted a rule in 2023 to reimburse government- and bank-impersonation scams. In December 2024 the CFPB sued Early Warning Services, JPMorgan Chase, Bank of America and Wells Fargo, alleging more than US$870m in losses over seven years (CFPB, 2024). In March 2025, under new leadership, the CFPB dismissed the case. A state-level action by the New York Attorney General followed in 2025†. Bills to extend Regulation E to induced transfers, such as the Protecting Consumers from Payment Scams Act, have not passed.

Where the US *is* severe. The TRACED Act (2019) and the STIR/SHAKEN caller-authentication framework bind carriers. In 2023 the FCC proposed a forfeiture of nearly US$300m against an auto-warranty robocall operation, its largest ever. Wire-fraud and money-laundering offences carry sentences of up to 20 years per count, and Treasury has sanctioned networks linked to Southeast Asian scam compounds.

Lesson. Harsh punishment of perpetrators does not compensate victims, because perpetrators are mostly offshore and funds leave within minutes. Protection that depends on agency enforcement discretion can also reverse with a change of administration, unlike statutory duties.

5.4 Singapore: shared responsibility and the telco tier

Singapore originated the "waterfall" model that Thailand later adopted.

Trigger. In December 2021 about 790 OCBC customers lost about S$13.7m to SMS phishing that impersonated the bank[†]. OCBC made full goodwill payments. The Monetary Authority of Singapore (MAS) responded with measures that included removing clickable links from bank SMS and email, a 12-hour cooling-off period for activating digital tokens on new devices, notifications to existing devices, and a customer "kill switch". Banks later introduced Money Lock, which lets customers ring-fence funds from digital transfers.

The Shared Responsibility Framework. The SRF, issued jointly by MAS and the Infocomm Media Development Authority (IMDA), took effect on 16 December 2024 (MAS and IMDA, 2024). It applies to *phishing* scams only and sets a waterfall of liability. Financial institutions pay first if they breached duties such as the cooling-off period, real-time alerts or round-the-clock reporting channels. Telcos pay next if they breached duties such as blocking unregistered sender IDs, labelling suspected scam SMS and blocking known malicious URLs. Consumers bear any residual. The popular claim that Singapore "fines telcos heavily" is therefore better described as *compensation liability* for duty breaches. IMDA's administrative fining powers continue alongside it.

Parallel instruments. The Online Criminal Harms Act (in force February 2024) empowers directions to platforms. In 2025 the government directed Meta to deploy facial-recognition measures against impersonation advertisements, backed by daily fines[†]. The Protection from Scams Act 2025 lets police issue restriction orders that limit a likely victim's banking transactions, even without consent. Criminal-law amendments in late 2025 introduced caning for scam offences and certain money-mule offences[†].

Limits. Despite these measures, reported losses rose from about S$650m (2023) to about S$1.1bn (2024)[†]. Most losses came from authorised scams outside the SRF's scope, such as investment and government-official impersonation. This is the displacement effect predicted in Section 4.

5.5 Other jurisdictions

Table 2 summarises other jurisdictions. None claims to have solved the problem. However, jurisdictions with fast recovery (Brazil) or warnings at the point of payment (Hong Kong) report reductions in loss per case.

Table 2. Selected measures in other jurisdictions.

Jurisdiction	Principal measures	Relevance for Thailand
European Union	Instant Payments Regulation (EU) 2024/886 mandates verification of payee for euro transfers (by October 2025). The proposed Payment Services Regulation would refund bank-employee impersonation and make platforms liable to PSPs for failing to remove notified scam content (provisional agreement late 2025)†.	Platform liability triggered by failure to act on notice.
Hong Kong	HKMA linked the police Scameter database to FPS (late 2023) to warn payers about reported accounts. Legislation in 2025 enabled bank-to-bank sharing on suspicious accounts†.	Thailand's Central Fraud Registry exists but does not warn the payer at the moment of decision.
Malaysia	National Scam Response Centre (hotline 997, 2022). BNM mandated migration from SMS OTP, single-device binding and cooling-off on new devices. Licensing of large social-media platforms (2025).	Closest regional comparator to Thailand.
India	RBI "zero liability" for unauthorised transactions reported within three days (2017). The AI tool MuleHunter.AI. A Financial Fraud Risk Indicator from the telecoms department rates phone numbers for banks and UPI apps (2025)†.	Live telco-to-payment risk signals.
Brazil	Banco Central's Special Return Mechanism (MED, 2021) obliges receiving banks to block and return funds. MED 2.0 traces funds across multiple hops†. Night-time Pix limits followed express kidnappings.	Closest structural analogue: a central-bank FPS used nationwide.
Taiwan	Fraud Crime Hazard Prevention Act (July 2024) requires platforms to verify and disclose advertisers, with fines†.	Facebook advertising is a primary scam vector in Thailand too.

5.6 Thailand

Context. PromptPay launched in 2017 under the National e-Payment strategy and is operated by National ITMX under Bank of Thailand (BOT) oversight. Thailand is among the world's leading real-time payment markets by volume. Retail transfers are free, which makes multi-hop layering through mule accounts almost costless for fraudsters.

Measures. Thailand's response has been extensive on prevention. In March 2022 police opened an online reporting portal. In March 2023 the BOT introduced a fraud-management framework: no links in bank SMS or email, one mobile-banking device per account, 24-hour hotlines, and mule-account sharing through a Central Fraud Registry (CFR). The *Emergency Decree on Measures for the Prevention and Suppression of Technology Crimes B.E. 2566 (2023)* took effect on 17 March 2023. It enabled temporary holds on suspicious transactions and information sharing among banks, telcos and agencies, and criminalised the opening, sale or rental of mule bank accounts and SIM cards (Thailand, 2023). The telecoms regulator NBTC introduced a +697/+698 prefix for inbound international calls, sender-name registration for SMS, and re-verification of bulk SIM holders. The digital-economy ministry launched the AOC 1441 hotline in November 2023. Biometric face verification applies to transfers of THB 50,000 or more per transaction, or THB 200,000 per day. In February 2025 the government cut electricity, fuel and internet supplies to scam hubs across the Myanmar border.

The 2025 amendment. The *Emergency Decree (No. 2) B.E. 2568 (2025)*, effective April 2025†, introduced shared responsibility. Financial institutions, telcos and digital platforms that fail to comply with measures

prescribed by their regulators must share liability for resulting losses. It also created a route to return frozen funds to victims without awaiting criminal judgment, extended coverage to digital-asset businesses and raised penalties for mule-account offences[†] (Thailand, 2025).

Scale. Figures cited from the police reporting system indicate cumulative losses since March 2022 in the order of THB 70–90bn by 2025, or tens of millions of baht per day, with frozen and returned amounts a small fraction of that[†]. No institution-level reimbursement data are published.

Gaps. Five gaps stand out:

(i) The burden of proof lies with the victim, who cannot observe whether a bank or telco met its duties. In terms of Proposition 4, π is low.

(ii) There is no statutory deadline for redress, comparable to the UK's five business days.

(iii) There is no independent ombudsman with binding authority. The BOT's Financial Consumer Protection Center (hotline 1213) mediates but cannot order compensation, so victims must litigate.

(iv) Receiving PSPs bear no direct financial cost from mule accounts. Their screening incentives are regulatory, not economic.

(v) Platform liability is hard to enforce against foreign entities without local presence (low π_P).

6 Comparative assessment

Figure 6 scores six jurisdictions on eight dimensions. Thailand matches Singapore on prevention and exceeds the United States on the formal breadth of liability. It trails the UK, Australia and Singapore on the speed, certainty and transparency of redress.

Table 3 tests seven claims common in Thai public debate. Three findings stand out.

First, Thailand's weakness is not the absence of a framework (H5) or ignorance of foreign models (H6). It is the absence of the *machinery* that makes a shared-responsibility framework bite: verifiable duty lists, a reversed burden of proof, deadlines and a binding adjudicator. Second, every regime studied has been revised after launch. The UK reduced its cap, the US withdrew its enforcement action, and Singapore had to legislate to restrict victims' own accounts because the SRF does not reach authorised scams. Third, the most stringent jurisdiction, Singapore, has moved towards *protecting victims from their own decisions*. That is an implicit acknowledgement of Proposition 3.

7 Is social engineering unsolvable?

Social engineering cannot be eliminated, but it can be made more costly for fraudsters and its harm to victims can be compensated. It attacks human judgment, not system vulnerabilities, so every technical control will eventually be circumvented. Each control layer nevertheless raises the fraudster's cost, and compensation directly reduces consumer harm.

Three mechanisms explain persistence. The first is *displacement*: closing one channel shifts activity to unregulated ones (Fig. 2(d)). The second is *authority and fear*: police and government impersonation suppresses deliberation in ways that on-screen warnings cannot reliably overcome (Stajano and Wilson, 2011;

	United Kingdom	Australia	United States	Singapore	European Union	Thailand
Scope of APP coverage	**3** All FPS	**3** All sectors	**0** Unauth. only	**1** Phishing	**1** Impersonation*	**2** Per regulator
Automaticity of redress	**3** Default	**1** Via AFCA	**0** Voluntary	**2** Waterfall	**1** Spoofing*	**1** Must prove
Clarity of compensation rules	**3** £85k cap	**2** Codes pending	**0** None	**3** Duty list	**1** Pending*	**0** Unspecified
Receiving-PSP liability	**3** 50%	**2** Duty-based	**0** None	**1** Limited	**1** Limited	**1** Unclear
Telco liability	**0** None	**3** Duty + fines	**2** FCC fines	**3** Waterfall	**0** None	**2** Decree No. 2
Platform liability	**1** Voluntary	**3** Duty + fines	**0** None	**2** OCHA	**2** Liable to PSPs*	**1** Enforceability
Speed of redress (time limit)	**3** 5 days	**1** EDR process	**0** None	**2** Not fixed	**1** Pending*	**0** None
Data transparency	**3** Per-bank	**2** NASC reports	**1** Aggregate	**1** Aggregate	**1** Aggregate	**1** Aggregate
	Total 19/24	**Total 17/24**	**Total 3/24**	**Total 15/24**	**Total 8/24**	**Total 8/24**

Figure 6. Comparative scorecard (0 = absent, 3 = strong). Scores are the author's qualitative coding of *de jure* design adjusted for evident enforcement, as of mid-2026. Asterisks mark EU provisions pending final adoption. Coding criteria are in Appendix C.

Table 3. Testing seven common claims.

	Claim	Verdict	Evidence
H1	The UK's reimbursement regime was so harsh that the regulator had to retreat	Partly true	Cap cut from £415k to £85k; principle retained; >99% of claims still covered[†]
H2	Australia seriously fines Google and Facebook over scams	Partly true	Large penalties are mostly from consumer and competition cases; SPF Act penalties are large but untested[†]
H3	The US has harsh anti-scam laws	Misleading	Harsh criminal and telecoms enforcement; weakest consumer redress for APP
H4	Singapore heavily penalises telcos	True in substance	The mechanism is compensation liability under the SRF, not primarily fines
H5	Thailand has virtually no redress for victims	Overstated	Shared liability since April 2025, but fault-based, victim-proven and little evidence of payouts
H6	Thai policymakers did not study foreign experience	Probably false	The 2025 decree closely mirrors Singapore's SRF and Australia's SPF
H7	Every country still suffers because social engineering cannot be solved	True but incomplete	Not eliminable, but losses to consumers can be cut sharply (Section 7)

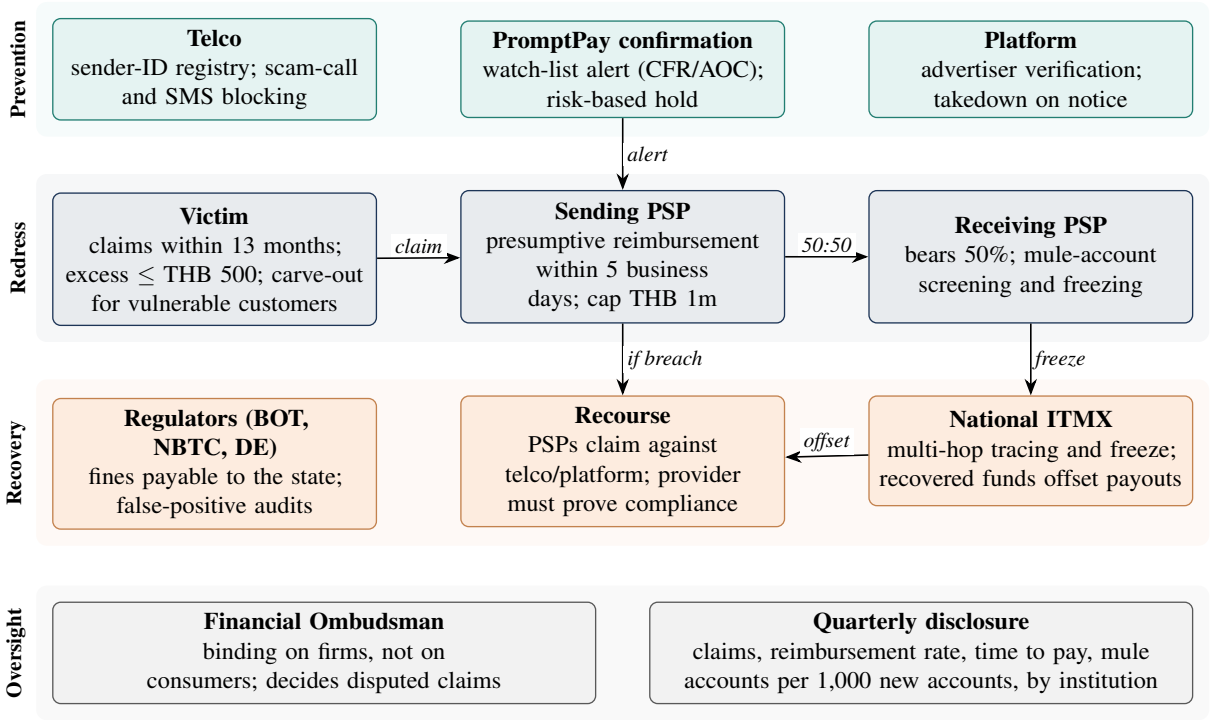


Figure 7. Proposed liability and redress architecture for PromptPay. Arrows show the flow of claims, information and funds. Monetary parameters (cap, excess, time limits) are proposals for consultation.

Kahneman, 2011). The third is *jurisdictional arbitrage*: perpetrators are offshore, and funds are converted to crypto-assets within hours.

The system nevertheless controls three points. At the *source*, it can reduce reachability through call and SMS filtering and advertiser verification. At the *decision point*, it can add risk-based friction, such as warnings when the payee is on a watch-list. At the *destination*, it can make mule accounts scarce and costly and recover funds before they exit. For Thailand the destination is decisive, because every scam type needs a domestic receiving account, the one element unambiguously within Thai jurisdiction.

Each control has costs. Payment holds reduce PromptPay's convenience. Facial verification burdens older users and those without recent smartphones. Account freezes harm innocent account holders. Mandatory reimbursement raises PSP costs that may be passed on. Controls should therefore be risk-based rather than uniform.

8 Policy design for Thailand

The central proposal is to move from "liability when breach is proven" to "reimbursement by default for defined scam types, within a cap and a deadline, with recourse among providers". The proposal uses the architecture of Decree No. 2. Figure 7 shows its structure and Fig. 8 its sequencing.

8.1 Short term (0–12 months): make existing law operational

M1. A verifiable duty checklist with a reversed burden of proof. Publish SRF-style duty lists for banks, telcos and platforms. When a loss occurs, the provider must show that it complied; the victim does not

have to show that it did not. This raises π directly (Proposition 4).

M2. Statutory deadlines. For example, require a decision on a claim within 15 business days and payment within 5 business days of a decision.

M3. Warnings at the point of payment. Integrate the CFR and AOC watch-lists into the PromptPay confirmation screen, following Hong Kong's Scameter model, and display the payee's name more fully on first-time payments.

M4. Quarterly institution-level metrics. Publish claims, reimbursement rate by value, time to pay, and reported mule accounts per 1,000 new accounts, by institution, as the UK's PSR has done.

8.2 Medium term (12–36 months): re-engineer incentives

M5. Presumptive reimbursement for impersonation, phishing and remote-access scams. The cap should be anchored to the Deposit Protection Agency limit of THB 1m, mirroring the UK's anchoring to its deposit-protection limit. Exceptions should cover gross negligence and complicity, with a carve-out for vulnerable customers (Proposition 3).

M6. A 50:50 split between sending and receiving PSPs, with recourse against telcos and platforms upon proof of breach (Proposition 2). This puts the cost of mule accounts on the institution that opened them.

M7. A financial ombudsman whose decisions bind firms but not consumers, modelled on the UK's Financial Ombudsman Service and Australia's AFCA.

M8. Multi-hop tracing and freezing. National ITMX should trace and freeze proceeds across successive hops within minutes, following Brazil's MED 2.0.

M9. Risk-based holds. Allow PSPs to delay high-risk transfers by one to four business days, following the UK, and make Money Lock-type features universal.

8.3 Long term (36+ months): ecosystem and cross-border

M10. Advertiser verification for financial advertising, following Taiwan, and a mandatory local representative for large foreign platforms (raising π_P).

M11. ASEAN freeze-and-return agreements, especially with Cambodia, Laos and Myanmar, covering cross-border QR payment links that could become exit channels.

M12. Open data and biennial review. Provide anonymised data to researchers and review the policy every two years, to avoid reactive adjustments like the UK's.

8.4 Risks and mitigations

Table 4 lists the main risks. In the model's illustrative calibration (Fig. 3), the package reduces excess social cost from about 85% of the maximum avoidable loss under the current *de facto* regime to about 11%. Most of the gain comes from raising enforceability and adding fines, not from the precise split of compensation.

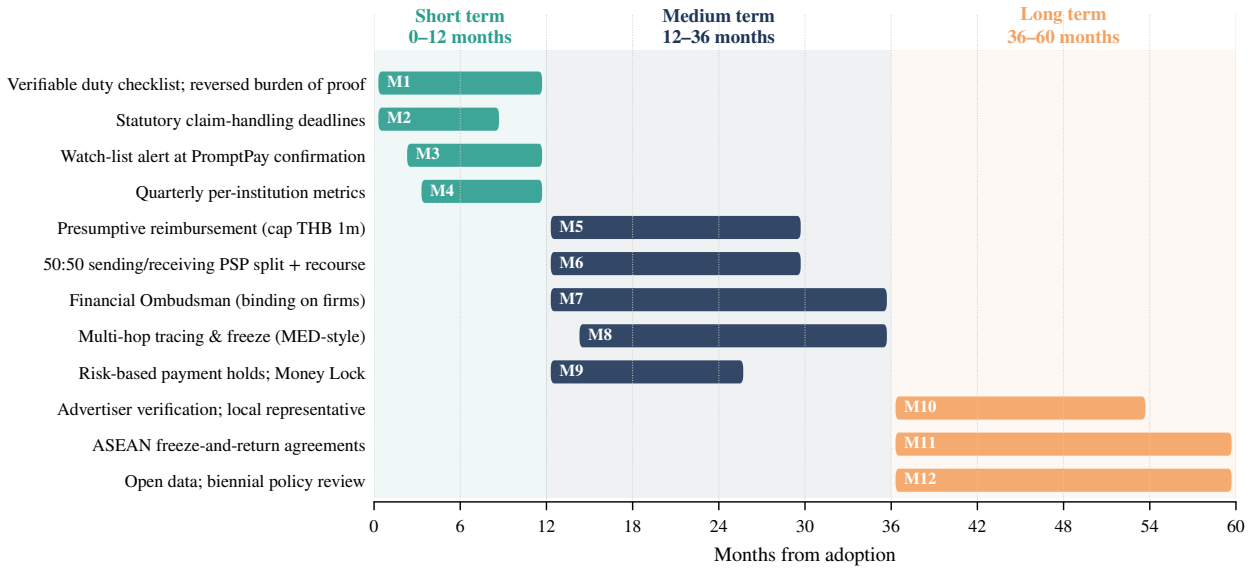


Figure 8. Indicative implementation roadmap for the twelve measures (M1–M12). Durations are indicative and assume legislative and regulatory capacity comparable to the 2023–2025 reforms.

Table 4. Principal risks of the proposed package.

Risk	Mitigation
Burden on small PSPs	Cap; receiving-PSP share; optional industry pooling fund
First-party fraud	Complicity exception; claim-history sharing through the CFR
Reduced consumer care	Small fixed excess; gross-negligence exception retained
Costs passed on as fees	Keep retail PromptPay free; place costs on non-compliant receiving PSPs
Wrongful account freezes	Appeals within 24–48 hours; publish false-positive rates
Over-deterrence from fines	Scale fines to detection probability (Eq. (8)); audit freeze decisions

9 Empirical agenda

The model generates four testable predictions.

P1. After the UK assigned 50% of liability to receiving PSPs (October 2024), mule-account closures and onboarding friction should rise more at receiving-heavy institutions. *Design:* difference-in-differences using the PSR's firm-level data, with treatment intensity given by each firm's pre-reform share of inbound APP volume.

P2. After Singapore's SRF (December 2024), the share of losses from out-of-scope scam types should rise. *Design:* an event study on scam-type composition from police statistics, with Malaysia and Hong Kong as comparison units.

P3. In Thailand, if the burden of proof remains with victims, compensation paid under Decree No. 2 should be very small relative to claims. *Design:* a descriptive audit of claims and payouts, complemented by a field survey of victims' attempts to claim.

P4. Jurisdictions that impose fines separate from compensation should show more preventive activity by telcos and platforms, such as blocked calls and removed advertisements. *Design:* a cross-country panel using regulator-reported blocking data.

Calibrating θ_i requires estimates of a_i, the marginal effect of each party's controls on scam success. Candidate sources include the staggered roll-out of CoP in the UK, Malaysia's device-binding mandate and Thailand's biometric threshold, which creates a natural discontinuity at THB 50,000.

10 Conclusion

The international experience does not show that the harshest regime wins. It shows that the regimes that work place losses on the parties best able to prevent them and return money to victims quickly. The UK shows that mandatory reimbursement is feasible even after a cap reduction. Singapore and Australia show that telcos and platforms can be brought inside the liability perimeter. The US shows that punishing perpetrators alone does not help victims. The model explains why. Budget-balanced sharing under-incentivises everyone, manipulation makes consumer liability inefficient, victim-proven fault rules collapse into caveat emptor, and decoupled fines restore first-best incentives.

Thailand already has a modern legal architecture. What it lacks is the operational detail that lets victims recover funds without litigation. The twelve measures proposed here build on existing law and focus on what Thailand controls most completely: domestic receiving accounts and a central-bank-overseen payment rail.

Limitations. This version relies on secondary information as of mid-2026, without live verification of primary sources; items marked † require confirmation. The model is static, assumes separable linear effects of care and treats losses as fixed. A fuller treatment would model a three-level game among regulator, providers and fraudsters and estimate a_i from data.

Acknowledgements

Drafting, figure generation and model exposition were assisted by an AI system (Claude, Anthropic). The author is responsible for the content, interpretation and any errors, and has verified, or flagged with †, the factual claims.

References

Australian Competition and Consumer Commission (2025). *Targeting Scams: Report of the National Anti-Scam Centre on Scams Activity 2024*. Canberra: ACCC.†

Anderson, R. (1993). Why cryptosystems fail. In *Proceedings of the 1st ACM Conference on Computer and Communications Security*, 215–227.

Anderson, R. and Moore, T. (2006). The economics of information security. *Science*, 314(5799), 610–613.

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T. and Savage, S. (2013). Measuring the cost of cybercrime. In R. Böhme (ed.), *The Economics of Information Security and Privacy*, 265–300. Berlin: Springer.

Becker, G. S. (1968). Crime and punishment: An economic approach. *Journal of Political Economy*, 76(2), 169–217.

Brown, J. P. (1973). Toward an economic theory of liability. *Journal of Legal Studies*, 2(2), 323–349.

Calabresi, G. (1970). *The Costs of Accidents: A Legal and Economic Analysis*. New Haven: Yale University Press.

Consumer Financial Protection Bureau (2024). *CFPB v. Early Warning Services, LLC, JPMorgan Chase Bank, N.A., Bank of America, N.A., and Wells Fargo Bank, N.A.*, complaint filed December 2024.

Cialdini, R. B. (2006). *Influence: The Psychology of Persuasion* (revised ed.). New York: Harper Business.

Coase, R. H. (1960). The problem of social cost. *Journal of Law and Economics*, 3, 1–44.

Committee on Payments and Market Infrastructures (2016). *Fast Payments – Enhancing the Speed and Availability of Retail Payments*. Basel: Bank for International Settlements.

Duarte, A., Frost, J., Gambacorta, L., Koo Wilkens, P. and Shin, H. S. (2022). Central banks, the monetary system and public payment infrastructures: Lessons from Brazil's Pix. *BIS Bulletin*, No. 52.†

Federal Bureau of Investigation (2025). *Internet Crime Report 2024*. Washington, DC: Internet Crime Complaint Center.

Federal Trade Commission (2025). *Consumer Sentinel Network Data Book 2024*. Washington, DC: FTC.

Global Anti-Scam Alliance (2024). *Global State of Scams Report 2024*.†

Holmström, B. (1982). Moral hazard in teams. *Bell Journal of Economics*, 13(2), 324–340.

Kahneman, D. (2011). *Thinking, Fast and Slow*. New York: Farrar, Straus and Giroux.

Landes, W. M. and Posner, R. A. (1987). *The Economic Structure of Tort Law*. Cambridge, MA: Harvard University Press.

Monetary Authority of Singapore and Infocomm Media Development Authority (2024). *Shared Responsibility Framework*. Singapore.

Modic, D. and Lea, S. E. G. (2013). Scam compliance and the psychology of persuasion. Working paper, University of Exeter. SSRN.†

Moore, T., Clayton, R. and Anderson, R. (2009). The economics of online crime. *Journal of Economic Perspectives*, 23(3), 3–20.

Office of the United Nations High Commissioner for Human Rights (2023). *Online Scam Operations and Trafficking into Forced Criminality in Southeast Asia: Recommendations for a Human Rights Response*. Bangkok: OHCHR Regional Office.

Polinsky, A. M. and Shavell, S. (1979). The optimal tradeoff between the probability and magnitude of fines. *American Economic Review*, 69(5), 880–891.

Payment Systems Regulator (2023). *PS23/3: Fighting Authorised Push Payment Scams – Final Decision*. London: PSR.

Payment Systems Regulator (2024). *Faster Payments APP Scams Reimbursement Requirement: Maximum Level of Reimbursement*, policy statement, September 2024. London: PSR.†

Shavell, S. (1980). Strict liability versus negligence. *Journal of Legal Studies*, 9(1), 1–25.

Shavell, S. (1987). *Economic Analysis of Accident Law*. Cambridge, MA: Harvard University Press.

Stajano, F. and Wilson, P. (2011). Understanding scam victims: Seven principles for systems security. *Communications of the ACM*, 54(3), 70–75.

Kingdom of Thailand (2023). *Emergency Decree on Measures for the Prevention and Suppression of Technology Crimes, B.E. 2566*. Royal Gazette.

Kingdom of Thailand (2025). *Emergency Decree on Measures for the Prevention and Suppression of Technology Crimes (No. 2), B.E. 2568*. Royal Gazette.†

UK Finance (2025). *Annual Fraud Report 2025*. London: UK Finance.

A Proofs

Proposition 1. Party i minimises $e_i^2/(2k_i)+\sigma_i(p_0-\sum_j a_j e_j)L$. The first-order condition gives $e_i/k_i=\sigma_i a_i L$, so $\hat{e}_i=\sigma_i k_i a_i L=\sigma_i e_i^*$. With full enforcement $\sigma_i=s_i$. If $\sum_i s_i=1$ and at least two parties have $s_i>0$, then $s_i<1$ for each of them, and each under-invests. A party with $s_i=0$ invests nothing. □

Lemma 1. Substituting $\hat{e}_i=\sigma_i k_i a_i L$ into Eq. (3) gives $\mathscr{W}=p_0L+L^2\sum_i\theta_i(\sigma_i^2/2-\sigma_i)$. At $\sigma_i=1$ this equals $p_0L-\frac{L^2}{2}\sum_i\theta_i$. The difference is $\frac{L^2}{2}\sum_i\theta_i(\sigma_i^2-2\sigma_i+1)=\frac{L^2}{2}\sum_i\theta_i(1-\sigma_i)^2$. □

Proposition 2. By Lemma 1, minimise $\sum_i\theta_i(1-s_i)^2$ subject to $\sum_i s_i=1$ and $s_i\geq 0$. The objective is strictly convex and the feasible set is convex, so the Karush–Kuhn–Tucker conditions are necessary and sufficient. They give $-2\theta_i(1-s_i)+\mu-\nu_i=0$ with $\nu_i\geq 0$ and $\nu_i s_i=0$. Writing $\lambda=\mu/2$, interior shares satisfy $s_i=1-\lambda/\theta_i$, and $s_i=0$ whenever $\theta_i\leq\lambda$. The function $\lambda\mapsto\sum_i\max\{0,1-\lambda/\theta_i\}$ is continuous and strictly decreasing on the region where it is positive, so λ is unique. □

Proposition 3. By Proposition 2, $s_C^*=0$ if and only if $\theta_C\leq\lambda$. When $s_C^*=0$, $\lambda=\lambda_{-C}$, which does not depend on m. Hence $s_C^*=0$ if and only if $(1-m)^2\bar{\theta}_C\leq\lambda_{-C}$, that is, $m\geq 1-\sqrt{\lambda_{-C}/\bar{\theta}_C}$. □

Proposition 4. This follows from the definitions $\sigma_i=\pi_i s_i$ and $\sigma_C=s_C+\sum_{i\neq C}(1-\pi_i)s_i$, taking the limit $\pi_i\to 0$. □

Proposition 5. Party i's total expected payment is $(s_i+f_i)p(\mathbf{e})L=p(\mathbf{e})L$, so its first-order condition coincides with the planner's. If a fine F_i is imposed with probability q, the expected fine equals qF_i. Setting $qF_i=f_iL$ gives Eq. (8). □

B Parameters for illustrations

All parameters are illustrative and are chosen to display mechanisms, not to estimate magnitudes. Care productivities are $\theta=(\theta_C,\theta_S,\theta_R,\theta_T,\theta_P)=(1,4,6,3,2)$, with θ_C already reflecting manipulation. In Fig. 2(c), $\bar{\theta}_C=5$, which gives $\lambda_{-C}\approx 2.67$ and $\bar{m}\approx 0.27$. The stylised regimes in Fig. 3 are defined as follows. *Caveat emptor:* $\sigma_C=1$ and all others 0. *Fault-based, victim proves:* nominal $(s_S,s_R,s_T,s_P)=(0.3,0.3,0.2,0.2)$ with $\pi=(0.2,0.2,0.2,0.05)$. *Fault-based with a verifiable duty list:* the same shares with $\pi=(0.8,0.8,0.8,0.3)$. *UK-type:* $s_S=s_R=0.5$. *Optimal budget-balanced:* Eq. (6). *Proposed Thai package:* $\sigma=(0.1,0.8,0.8,0.8,0.5)$, combining compensation, recourse and fines. *First best:* $\sigma_i=1$ for all i. Treating fault-based regimes as proportional incentives $\sigma_i=\pi_i s_i$ is a simplification of imperfectly verifiable negligence. The displacement panel uses a multinomial logit with three alternatives (covered channel, uncovered channel, outside option), sensitivity $\beta=4$, baseline success probabilities 0.9 and 0.7, outside return 0.35, and a covered-channel success probability of $0.9(1-0.85\tau)$.

C Coding of the comparative scorecard

Each dimension is scored from 0 to 3.

Scope: 0 = unauthorised only; 1 = one subclass of APP fraud; 2 = APP fraud as defined by regulator-specified measures; 3 = all APP fraud on the relevant rail.

Automaticity: 0 = voluntary; 1 = only after proof of breach or an external ruling; 2 = waterfall applied against defined duties; 3 = default reimbursement.

Clarity of compensation rules: 0 = unspecified; 1 = pending; 2 = framework set, details pending; 3 = caps and rules fixed.

Receiving-PSP, telco and platform liability: 0 = none; 1 = limited, voluntary or unclear; 2 = defined duties or penalties; 3 = compensation liability plus penalties.

Speed: 0 = no time limit; 1 = process-based; 2 = practice-based; 3 = statutory deadline.

Transparency: 1 = aggregate statistics; 2 = regular agency reports; 3 = institution-level data.