Continuum

PAYMENT PROVIDERS AND THE ROLE OF INSURANCE IN APAC

RISK INSIGHT SERIES

JULY 2026

Contents

Introduction

Payment providers across APAC sit at the centre of three overlapping pressures. Sponsor banks and correspondent banks require specific insurance as a condition of their partnerships. Regulators require safeguarding of customer funds and expect governance to bank standards. Operational risk arrives daily, in the form of transfer errors, cyber incidents, and social engineering attempts.

Each pressure shapes what a payment provider is required or expected to carry. What they often do not do together is produce a coherent picture. Providers assemble cover from multiple lines to satisfy multiple obligations. The gaps sit at the intersections between those obligations, and they usually surface only when a loss event tests the response.

The environment in 2026 has raised the stakes. MAS enforcement escalated materially through 2025, with composition penalties on nine financial institutions reaching S$27.45 million in a single week in July.[3] The HKMA imposed HK$16.2 million in AML-related fines on three banks over the same period.[6] Digital Payment Token providers faced separate action, with three DPT providers fined a combined S$4.8 million.[11] The direction of travel is clear: regulators now expect payment providers to operate at bank-standard governance, and the insurance question is following that expectation.

This report maps the insurance picture across the five categories that matter most for licensed payment providers in APAC. It sets out what the sponsor bank contract typically requires. It walks through the mechanics of a payment error PI claim. It explains where Cyber, Crime, and Social Engineering Fraud sit relative to each other. It covers the safeguarding obligations under the Singapore Payment Services Act[1] and the Hong Kong Payment Systems and Stored Value Facilities Ordinance.[5] And it addresses the regulatory liability picture for HKMA and MAS investigations, both of which have escalated materially through 2025.[3]

The consequences of leaving the picture incomplete rarely show up in the abstract. They surface at claim, and they surface in specific ways. A regulatory investigation defence exhausts a sub-limit within months. A social engineering fraud loss is denied under voluntary parting language. A payment error PI claim is rejected because the notification window was missed. A safeguarding failure at a custodian falls outside the wording of the Crime policy the provider believed would respond. Each of these is a recoverable exposure through targeted policy design. Each is unrecoverable once the loss has hit and the cover does not respond.

The through-line is straightforward. Payment provider insurance is not a discretionary buy. It is a compliance obligation, a contractual obligation, and an operational obligation, all at once. The firms that map their cover against all three, rather than any one in isolation, are the ones that avoid the surprises when a loss event actually occurs.

Background

Three Pressures Shaping the Insurance Picture for APAC Payment Providers

The APAC payment institution market has matured substantially over the past five years. Singapore's Payment Services Act took effect in January 2020 and now supervises hundreds of licensed providers across cross-border transfer, e-money, merchant acquisition, and digital payment token services.[1] Hong Kong's Payment Systems and Stored Value Facilities Ordinance has been the regulatory home for SVF licensees since 2016, with the framework refined most recently through the HKMA's October 2025 Practice Note on supervision.[5]

Two features of the APAC payment landscape shape the insurance conversation. The first is the density of banking counterparty relationships. The second is the density of regulatory expectation.

The Banking Counterparty Density

A licensed payment provider in Singapore or Hong Kong typically operates through one or more sponsor banks for local settlement, plus correspondent banks for cross-border flows, plus acquiring bank relationships for card processing where relevant. Each of those counterparties imposes its own insurance requirements as a condition of the partnership.

Sponsor bank agreements typically include a schedule naming required policies and minimum limits. Correspondent banks often ask for certificates of insurance before opening accounts. Acquirer agreements frequently require additional insured status and waiver of subrogation. The cumulative effect is that a mid-sized payment provider can find its insurance requirements dictated less by its own risk assessment and more by the contract review dates of its banking counterparties

The Regulatory Density

Payment providers in both jurisdictions operate under prescriptive rules on safeguarding, AML/CFT, capital adequacy, conduct, and reporting. MAS took enforcement action against five Major Payment Institutions in June 2025, imposing S$960,000 in composition penalties for AML/CFT breaches identified during compliance examinations.[2] Two weeks later, MAS imposed S$27.45 million in penalties on nine financial institutions in connection with a single major money laundering case.[316]

The HKMA has been similarly active. Three banks were fined a combined HK$16.2 million in 2025 for AML system lapses, with the HKMA signalling zero tolerance for weakness in monitoring and reporting systems.[6] Enforcement history is now a real consideration in the underwriting of any payment provider's regulatory liability cover, and disclosure obligations at renewal have tightened accordingly.[12]

The Insurance Market Response

The insurance response has been fragmented. Standard fintech PI wordings do not always contemplate the sponsor bank requirements. Cyber and Crime policies frequently sub-limit or exclude social engineering fraud.[8] PI often carves out regulatory matters. The result is cover that satisfies the sponsor bank checklist but does not respond to the actual loss when it arrives.

Five insurance questions arise from this picture. The rest of this report works through them.

The Contract Sets the Cover

What Sponsor Banks and Correspondent Banks Actually Require

The insurance a payment provider carries is shaped less by risk appetite and more by contractual obligation. Sponsor banks, correspondent banks, and acquirers set the floor. For most licensed providers in APAC, the insurance schedule attached to the sponsor bank agreement is the starting point of the cover conversation, and the renewal cycle is driven by contract review dates rather than the provider's own preference.

The Standard Schedule

Most sponsor bank agreements include a schedule naming required policies and minimum limits. The standard set typically includes Technology Errors and Omissions or Professional Indemnity cover, Cyber cover with a breach response component, and Crime cover including funds transfer fraud. Directors and Officers cover is often added as a condition of board approval on the bank side, particularly where the provider is early-stage or venture-backed.

Correspondent banks routinely request certificates of insurance before opening accounts, and refresh those certificates annually. Acquirer agreements frequently require additional insured status for the acquirer and waiver of subrogation. These are not decorative asks. They are contractual conditions of the counterparty relationship, and non-renewal or non-compliance can trigger review of the underlying account.

Where the Contract Diverges from the Risk

The schedule in the sponsor bank agreement is designed to protect the bank, not the provider. It sets minimum limits appropriate to the bank's exposure, which is typically a fraction of the provider's actual exposure. It names policies in generic terms, without specifying the wording extensions that make those policies responsive to the provider's actual loss patterns. And it locks the provider into a renewal cycle that may not align with when the provider's own exposure changes.

A payment provider carrying cover to the contract minimum typically finds two categories of gap. The first is the limit gap: the contract minimum is not enough to respond to a real event. The second is the wording gap: the cover satisfies the contract on paper but excludes the loss when it actually arrives. Both categories become visible only at claim, which is not the moment to discover them.

Renewal Alignment

Renewal cycles and contract review dates rarely line up. A provider that renews its cover in Q1 and reviews its sponsor bank agreement in Q3 can find itself compliant at the start of the year and non-compliant by the end of it, because the bank has updated its requirements in the intervening months. Coordinating the two calendars is straightforward in principle but often overlooked in practice. The disciplined approach is to build renewal reviews around the contract cycle rather than around the anniversary of the policy inception.

When a Payment Error Becomes a Claim

The PI Response and Where It Stops

Operational mistakes, not breaches, are a leading source of claims against payment providers. A transfer sent to the wrong account. An amount keyed in with an extra zero. A currency conversion applied incorrectly. A settlement delayed past the counterparty's cutoff. A refund misapplied between merchants. These are quiet errors, not headline events, and Professional Indemnity is the policy that decides whether the loss stays with the provider or is recoverable from the insurer.

The PI Trigger

For PI to respond, the loss must arise from professional services as defined in the policy schedule. That definition matters. A well-drafted PI policy for a payment provider will define professional services broadly enough to include the full range of payment processing, settlement, reconciliation, and reporting activities. A generic fintech PI wording may define professional services more narrowly, and the gap between the two can determine whether a routine wire error is covered or not.

Notification clauses are strict. Most PI policies require notification of a claim or a circumstance likely to give rise to a claim within a defined period, often as short as thirty days. Late notice voids cover regardless of the merits of the underlying claim. For payment providers processing high volumes of transactions, developing an internal escalation process that identifies notifiable circumstances promptly is a compliance discipline that has nothing to do with the underlying policy wording.

Common Exclusions

Standard PI wordings carry a set of exclusions that matter for payment provider claims. Contractual penalties are usually excluded, which means that a service level breach that triggers liquidated damages under a sponsor bank agreement is typically not recoverable through PI. Deliberate acts and gross negligence are excluded. Fines and regulatory penalties are excluded from most PI policies and require dedicated regulatory liability cover instead.

Sub-limits on consequential loss and currency movement quietly cap most settlements. A wire error that causes a counterparty loss of USD 500,000 in principal and an additional USD 100,000 in consequential business impact may find that the PI policy responds to the principal but sub-limits the consequential portion at USD 50,000 or less. Reading the sub-limits at placement, and stress-testing them against realistic loss scenarios, is the work that most fintech PI programmes have not done systematically.

Territorial Scope

Whether the cover follows the funds across borders depends on territorial scope. A PI policy issued in Singapore may or may not respond to a claim arising from a transfer routed through a Hong Kong correspondent bank and settled in Malaysia. Providers operating cross-border settlement should map their transaction flows against the territorial scope of their PI cover explicitly, particularly where a claim might involve courts or claimants in multiple jurisdictions.

The Typical Claim, Step by Step

The most common PI claim against a payment provider follows a familiar shape.

A wire is sent to a closed account. The receiving bank rejects the transfer. The originator is left without the funds. The provider is caught between reclaiming from the bank and compensating the originator for the delay or the associated business consequences.

The provider notifies its PI insurer within the policy's stated window. External claims counsel is appointed, transaction records are produced, and the insurer begins its coverage determination.
Whether the policy responds depends on the definition of professional services, the notification timing, the exclusions, the sub-limits, and the territorial scope. A well-structured programme addresses each point explicitly. A programme built to the sponsor bank minimum usually does not.

How Insurers Investigate a Payment Error Claim

Once notice is given, the insurer's response follows a defined pattern. External claims counsel is appointed. The circumstances of the error are documented through interviews with the operations team and review of the transaction records. Where the loss exceeds a threshold, forensic accountants are engaged to quantify direct and consequential loss separately. The insurer then issues a reservation of rights letter, preserving all coverage defences pending further investigation. This stage can last months. Providers with well-organised transaction logs, clear internal escalation records, and cooperative senior counsel typically move through it faster and with fewer coverage disputes.

Recovery from the Receiving Bank

Payment error claims often involve a parallel recovery process against the receiving bank. Where funds have been credited to a closed account or held pending clearance, the receiving bank may return the funds voluntarily or through interbank recovery mechanisms. Where the receiving bank has closed the account and the beneficiary has withdrawn the funds, recovery becomes contested. Most PI policies contain subrogation clauses that give the insurer the right to pursue the receiving bank after paying the claim. Coordinating the provider's own recovery efforts with the insurer's subrogation rights is a practical discipline that often determines net recovery.

> “A programme built to the sponsor bank minimum usually does not respond to the actual claim”

Cyber, Crime, and Social Engineering

Three Loss Types, Three Different Triggers

Cyber breaches, employee theft, and impersonation fraud all hit payment providers. They sit under different policies, with different triggers, and the boundaries between them are the single most common source of denied claims. Most payment providers align their cover against one of the three and discover, at claim, that the loss falls into another.

What Each Line Actually Covers

Cyber cover responds to losses arising from a security failure. Breach response costs, business interruption from a security incident, forensic investigation costs, notification obligations, regulatory defence for privacy investigations, and certain categories of extortion payment all sit within the standard Cyber wording. The trigger is the security event itself.

Crime cover responds to theft of money or securities. Employee dishonesty, forgery, robbery, and computer fraud all sit within the standard Crime wording. The trigger is the taking of the asset, and the loss must be quantifiable in monetary terms. Standard Crime wordings often carry a computer fraud extension, but that extension typically requires the loss to arise from unauthorised access to a computer system rather than from voluntary transfer by an authorised user.

Social engineering fraud is the voluntary transfer of funds triggered by deception. The employee is deceived into believing they are following a legitimate instruction, typically from an executive or a counterparty, and they voluntarily initiate the transfer. This is the fastest-growing category of payment provider loss and the most common source of coverage disputes.[14]

Where Social Engineering Sits

Both Cyber and Crime policies commonly sub-limit social engineering well below the main aggregate. A Cyber policy with a USD 5 million limit may sub-limit social engineering at USD 100,000 or USD 250,000. A Crime policy with the same overall limit may sub-limit social engineering similarly.[14] For a payment provider processing high-value cross-border transactions, those sub-limits are frequently a small fraction of the exposure they need to respond to.

The voluntary parting problem compounds the sub-limit issue. Voluntary parting language in a Crime policy excludes losses that result from the insured willingly transferring funds, even where that willingness was based on deception. Under a strict reading, a social engineering loss where the employee initiated the transfer can be denied as voluntary. This is the most common reason social engineering claims are denied, and it can defeat a claim regardless of the sub-limit that would otherwise apply.[8]

Funds Transfer Fraud and Vendor Compromise

Two adjacent categories deserve specific attention. Funds transfer fraud involves account takeover and unauthorised instruction: an attacker gains access to the credentials of an authorised user and initiates a transfer without the user's knowledge. This is often carved out of standard cover and requires a specific endorsement.

Vendor compromise is third-party impersonation in the payment chain: an attacker compromises a supplier's email or accounts and diverts a legitimate payment. The trigger question is whether the loss arose from the insured's own systems (Cyber and Crime typically respond) or from a compromise at the third party (many policies do not respond). Payment providers with meaningful supplier payment volumes should specifically address this category in their placement.

Best Practice: Aligning the Three

The disciplined approach is to align triggers, sub-limits, and notification requirements across Cyber, Crime, and any standalone Social Engineering Fraud cover the provider carries. Where the three policies have different limits, different triggers, and different notification windows, coverage disputes at claim become almost inevitable. Where they are aligned, the provider has a coherent response to the loss regardless of which of the three categories the event falls into. This is the work most fintech placements have not done systematically.

The Notification Trap Across Three Lines

Notification requirements differ across Cyber, Crime, and Social Engineering Fraud cover, and the differences matter. Cyber policies typically require notification of a security event within days of discovery. Crime policies often require notification within a defined window after the loss is quantified. Social Engineering Fraud endorsements sometimes carry their own separate notification clause with different triggers. A payment provider that identifies a suspicious transaction and takes a week to determine whether it is a security breach, employee theft, or social engineering fraud can find itself late on all three by the time the classification is settled. The disciplined response is to notify all three insurers on discovery and let the coverage analysis follow.

Five Questions to Ask at Renewal

1. What is the social engineering sub-limit across Cyber and Crime, and how does it compare to a realistic single-loss scenario?
2. Does the Crime policy contain voluntary parting language, and if so, has it been endorsed away?
3. Do the notification windows for Cyber, Crime, and SEF align, or do they require different actions on the same event?
4. Is funds transfer fraud endorsed specifically, or carved out?
5. How does the cover respond to a vendor email compromise where the loss arises from a third party's systems?

Safeguarding and the Insurance Behind It

What MAS Section 23 and the HKMA SVF Ordinance Require

Safeguarding is the first line of protection for customer funds held by a licensed payment provider. It is a regulatory obligation, not an insurance product. But when safeguarding fails, insurance is what is left to respond, and the alignment between the regulatory expectation and the insurance cover is rarely tested in advance.

Singapore: Section 23 of the Payment Services Act

Section 23 of the Singapore Payment Services Act sets out safeguarding requirements for Major Payment Institutions holding customer funds. The Act specifies three approved methods.[1] Funds can be held in a trust account at a Singapore bank or approved institution. They can be protected by a bank guarantee or insurance from an approved institution. Or they can be covered by an undertaking from a safeguarding institution.

MAS expects daily reconciliation of safeguarded funds against customer balances, and funds must be safeguarded within one business day of receipt.[4] The obligation extends to Digital Payment Token service providers under amendments introduced through 2023 and 2024, with the specific application to DPT providers refined through subsequent MAS notices.[17]

Hong Kong: The PSSVFO

Hong Kong's Payment Systems and Stored Value Facilities Ordinance imposes parallel obligations on SVF licensees. Customer funds must be segregated from the operator's own funds and held in a trust account with a licensed bank in Hong Kong, or protected through a bank guarantee.[7] The HKMA expects adequate risk management policies and procedures for managing the float and the SVF deposit, ensuring that sufficient funds are always available for redemption of the stored value.[13]

The HKMA's October 2025 Practice Note reinforced expectations around governance, control, and reporting for SVF licensees, with particular attention to AML/CFT systems and the reconciliation processes supporting safeguarding compliance.[5]

Where Insurance Responds When Safeguarding Fails

Safeguarding protects the customer. Insurance is what is left when safeguarding breaks. The common operational failures that expose the insurance layer include reconciliation breaks (customer balances no longer match segregated funds), commingling (safeguarded funds inadvertently mixed with operational funds), custodian collapse (the bank holding the safeguarded funds fails), and internal theft (an employee misappropriates safeguarded funds).

Crime cover may respond to internal theft of safeguarded funds, depending on the policy wording and whether the safeguarded funds qualify as covered property. PI may respond if the loss flows from a procedural error in safeguarding, such as a reconciliation failure that leads to a customer shortfall. Cyber may respond if the safeguarding failure originates from a security event. What none of these lines typically covers cleanly is the scenario where the safeguarding custodian itself fails, because that exposure sits at the intersection of banker liability, insolvency law, and the specific terms of the trust arrangement.

Stress-Testing the Response

Most providers do not stress-test their cover against a real safeguarding incident. The work of mapping each realistic failure scenario against the specific policy that would respond, with attention to sub-limits, exclusions, and notification requirements, is what separates a compliant safeguarding programme from an insured one. For providers operating in both Singapore and Hong Kong, the exercise needs to be run against both regulatory frameworks and against the specific custody arrangements in each jurisdiction.

Common Safeguarding Failures at Payment Providers

Regulators publish safeguarding failures in enforcement notices, and the pattern is consistent across jurisdictions. Reconciliation lags where customer balances are not reconciled against segregated funds within the required daily cycle. Commingling where operational funds are inadvertently transferred to the safeguarding account or vice versa. Late safeguarding where customer funds are received but not moved into the trust account within the required window. Insufficient float where the amount held in the trust account does not fully cover outstanding customer balances. Each of these is a technical compliance failure. Each can trigger regulatory action independently of any actual customer loss.

Stress-Test Scenarios for Your Safeguarding Cover

Test your insurance against each scenario. Identify which policy responds and at what limit.

1. Reconciliation identifies a shortfall between customer balances and segregated funds
2. Employee misappropriates funds from the safeguarding account
3. Safeguarding custodian bank becomes insolvent
4. Operational funds are commingled with safeguarded funds due to system error
5. Cyber breach compromises the settlement systems tied to safeguarding
6. Regulatory investigation identifies a systemic reconciliation failure over multiple periods

Regulatory Liability and Investigations

What HKMA and MAS Investigations Actually Cost

HKMA and MAS open investigations into payment licensees for AML, conduct, capital, and reporting failures. The defence is rarely covered by a standard PI policy, and the cover that responds is fragmented, often misaligned, and rarely placed in APAC with the specificity the exposure now demands.

What an Investigation Actually Involves

An HKMA or MAS investigation typically begins with a notice requesting document production. The scope of production can be substantial: transaction records, internal communications, compliance policies, board minutes, audit trails, and correspondence with counterparties. The investigation moves to interviews of senior management and compliance staff. External counsel is engaged. Independent forensic accountants are frequently appointed. The process can run for months or years, and defence costs accumulate throughout.

The MAS enforcement pattern over 2025 illustrates the scale. Composition penalties against five Major Payment Institutions totalled S$960,000 for a set of AML/CFT breaches identified during compliance examinations.[2] The subsequent action against nine institutions in connection with a single money laundering case reached S$27.45 million.[3] Digital Payment Token providers faced separate enforcement, with three DPT providers fined a combined S$4.8 million for AML failures.[11]

The HKMA enforcement pattern shows the same direction. The HK$16.2 million fines imposed on three banks in 2025 reflected supervisory findings on transaction monitoring, customer due diligence, and reporting.[6] The disciplinary actions list is public and now includes multiple SVF and payment institution licensees.[12]

What Regulatory Liability Cover Actually Does

Regulatory liability cover, sometimes packaged inside D&O and sometimes purchased separately, responds to the defence costs of a regulatory investigation and to certain categories of financial penalty. The investigation notice itself typically triggers cover, before any wrongdoing has been established. Defence costs are paid in advance under most regulatory liability wordings, which is critical because the costs accumulate long before any resolution.

Fines and penalties are typically excluded from cover. In some jurisdictions, insurers cannot indemnify a fine as a matter of public policy. In others, the exclusion is contractual rather than legal, but the practical result is the same. The value of regulatory liability cover sits in the defence costs and in certain associated exposures, such as costs of internal investigations required as a condition of resolution.

Where the Gaps Sit

Standard PI wordings commonly exclude regulatory matters entirely or sub-limit them well below the main aggregate. A payment provider relying on its PI policy for regulatory defence costs is often relying on a sub-limit that will exhaust in the first few months of an investigation. Notification timing is strict, and late notice voids cover. Dedicated regulatory liability cover is available in the APAC

market but is not routinely placed, and where it is placed the wording often needs specific negotiation to align with the actual regulatory processes the provider is exposed to.

Coordination between D&O, PI, and regulatory liability is where the largest gaps appear. A clean set of policies aligns triggers, defence cost advancement provisions, and notification clauses across all three lines, with an explicit understanding of how the three interact where multiple lines are engaged by the same event. Most payment provider placements have not done this coordination systematically.

The Continuum View

The right answer for a payment provider operating across APAC is rarely a single-line placement. It is a coordinated set of covers that responds to the contract requirements, the operational exposures, the safeguarding obligations, and the regulatory investigation risk, with alignment between the triggers, the sub-limits, and the notification requirements of each line.[18] The work of assembling that coordination, and revisiting it as the sponsor bank contracts and the regulatory expectations evolve, is what separates a compliant cover position from an insured one. Continuum's practice is built around exactly that coordination question for licensed payment providers and digital asset firms in Asia.

The First 72 Hours of a Regulatory Notice

The response window is short. The right sequence protects the firm.

1. Log the notice with a time stamp and preserve the original document
2. Notify the D&O, PI, and regulatory liability insurers within their respective windows
3. Retain external counsel with APAC regulatory experience
4. Freeze document retention schedules to avoid inadvertent destruction
5. Brief the board and appoint an internal response lead
6. Coordinate all external communications through counsel
7. Preserve legal privilege on internal analysis

Summary

Payment provider insurance is a compliance, contractual, and operational discipline. Treating it as one is what closes the gaps.

Payment providers in APAC face an insurance environment shaped by three overlapping forces. Sponsor bank and correspondent bank contracts set the minimum floor, often through detailed schedules of required policies and limits. Regulators set the safeguarding, AML, and conduct expectations, backed by an enforcement pattern that has escalated materially through 2025 across both MAS and HKMA.[36] Operational risk arrives daily, in the form of transfer errors, cyber incidents, and social engineering attempts that concentrate around the moments where money moves.

The cover assembled to respond to those three pressures is often not coordinated across them. Sponsor bank contracts drive the standard PI, Cyber, Crime, and D&O placements, but the wordings satisfying those contracts frequently miss the exposures the provider actually faces. Cyber and Crime policies typically sub-limit social engineering fraud well below the main aggregate, and voluntary parting language in Crime wordings can defeat social engineering claims entirely.[8] PI policies commonly exclude regulatory matters or sub-limit them at levels that exhaust in the first few months of an HKMA or MAS investigation.

The 2025 enforcement pattern crystallises the point. MAS took action against five Major Payment Institutions in June, then against nine financial institutions in July, with combined penalties exceeding S$28 million.[23] Three DPT providers were fined a combined S$4.8 million for AML failures.[11] The HKMA imposed HK$16.2 million on three banks for AML system weaknesses.[6] The direction of travel is unambiguous, and the insurance question follows.

For payment providers, the immediate action is to map the actual insurance cover in place against the sponsor bank contract requirements, the safeguarding obligations under the applicable regulatory regime, and the operational loss patterns the business actually faces. Sub-limits should be stress-tested against realistic scenarios. Triggers should be aligned across PI, Cyber, Crime, and any standalone SEF cover. Regulatory liability cover should be specifically evaluated rather than assumed to sit inside D&O or PI.

For insurers, the underwriting opportunity is real. The APAC payment institution market is large, growing, and increasingly regulated. Insurers that develop wordings responsive to the specific sponsor bank, safeguarding, and regulatory investigation exposures of the segment will write differentiated business. Those that rely on generic fintech wordings will find themselves declining claims at exactly the moments the market is most watching how they respond.

Payment provider insurance is a compliance obligation, a contractual obligation, and an operational obligation. The firms that treat it as one, rather than three, are the ones that avoid the surprises.

References

1. Monetary Authority of Singapore, "Payment Services Act 2019," 2019, amended through 2025. https://www.mas.gov.sg/regulation/acts/payment-services-act

2. Monetary Authority of Singapore, "MAS Imposes Composition Penalties against Five Major Payment Institutions for AML/CFT Breaches," June 2025. https://www.mas.gov.sg/regulation/enforcement/enforcement-actions/2025/mas-imposes-composition-penalties-against-five-major-payment-institutions

3. Monetary Authority of Singapore, "MAS Takes Regulatory Actions against 9 Financial Institutions for AML-Related Breaches," July 2025. https://www.mas.gov.sg/regulation/enforcement/enforcement-actions/2025/mas-takes-regulatory-actions-against-9-financial-institutions-for-aml-related-breaches

4. Monetary Authority of Singapore, "Ongoing Requirements for Payment Service Providers," 2025. https://www.mas.gov.sg/regulation/payments/ongoing-requirements-for-payment-service-providers

5. Hong Kong Monetary Authority, "Practice Note on Supervision of Stored Value Facility Licensees," October 2025. https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/PN_on_supervision_of_SVF_licensees_eng.pdf

6. AML Watcher, "Banks Fined HK$16.2M as HKMA Warns Zero Tolerance for AML Gaps," 2025. https://amlwatcher.com/news/hk-banks-hit-with-hk16m-dollors-penalties-for-aml-system-lapses/

7. Hong Kong Monetary Authority, "Regulatory Regime for Stored Value Facilities," 2025. https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/stored-value-facilities-and-retail-payment-systems/regulatory-regime-for-stored-value-facilities/

8. Ward and Smith, "Social Engineering Fraud and Your Crime Policy: Why Your Insurer May Deny the Claim and What You Can Do About It," 2025. https://www.wardandsmith.com/article/social-engineering-fraud-and-your-crime-policy-why-your-insurer-may-deny-the-claim-and-what-you-can-do-about-it

9. Waystone Compliance, "Navigating MAS Payment Services Act Changes 2023 to 2025," 2025. https://compliance.waystone.com/navigating-mas-payment-services-act-changes-2023-2025/

10. Bank for International Settlements, "Stablecoin Growth: Policy Challenges Approaches (BIS Bulletin No 108)," 2024. https://www.bis.org/publ/bisbull108.pdf

11. Bird & Bird, "MAS Takes Robust Regulatory Actions against Nine Financial Institutions," 2025. CNBC, "Stablecoin USDC Breaks Dollar Peg After Firm Reveals It Has $3.3 Billion in SVB Exposure," March 2023. https://www.cnbc.com/2023/03/11/stablecoin-usdc-breaks-dollar-peg-after-firm-reveals-it-has-3point3-billion-in-svb-exposure.html

12. Bankers Magazine, "MAS Fines Three Digital Payment Token Providers a Combined S$4.8 Million for AML Failures," 2025. https://bankersmagazine.com/intelligence/articles/mas-crypto-fines/

13. Hong Kong Monetary Authority, "Anti-Money Laundering and Counter-Financing of Terrorism: Disciplinary Actions," 2025. https://www.hkma.gov.hk/eng/key-functions/banking/anti-money-laundering-and-counter-financing-of-terrorism/disciplinary-actions/

14. Hong Kong Monetary Authority, "Guideline on Supervision of Stored Value Facility Licensees," 2024. https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Guidelines-on-supervision-of-SVF-licensees_Eng.pdf

15. Corvus Insurance (Travelers), "Social Engineering and Cyber Insurance Coverage," 2025. https://www.corvusinsurance.com/blog/cyber-coverage-explained-social-engineering-and-cyber-crime

16. Financial Action Task Force, "Targeted Update on Implementation of the FATF Standards on Virtual Assets and VASPs," 2025. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html

17. Ocorian, "MAS AML Penalties: S$28M Fines Issued to Financial Institutions," 2025. https://www.ocorian.com/knowledge-hub/insights/mas-takes-financial-institutions-task-anti-money-laundering-breaches

18. Flint & Battery LLC, "MAS 2023/4 Amendments to PSA: Regulatory Measures for Digital Payment Token Services," 2024. https://www.flintbattery.com/update-on-mas-2023-amendments-to-psa-response-to-mas-consultation-paper-p008-2022-proposed-regulatory-measures-for-digital-payment-token-services

19. Continuum, "Fintech Insurance," 2026. https://www.continuuminsure.com/coverage/fintech-insurance/

Continuum

Risk. Insurance. Technology.

hello@continuuminsure.com

www.continuuminsure.com