Deloitte.



Centre for
Regulatory Strategy
Asia Pacific

Asia Pacific Financial Crime Regulatory Report

Q3 2026

November 2026

Table of Content

Click icon to navigate to the relevant section

1	Executive Summary	3 - 4
2	Australia	5- 9
3	China Mainland	10 - 12
4	Hong Kong SAR	13 - 15
5	India	16- 17
6	Japan	18– 24
7	Malaysia	25- 26
8	New Zealand	27- 29
9	Philippines	30- 31
10	Singapore	32- 36
11	Taiwan (China)	37 - 40
12	Thailand	41- 45
13	Vietnam	46 - 51
14	Contacts	52- 53
15	Appendix	54 - 59



Executive Summary

The Deloitte Asia Pacific Centre for Regulatory Strategy (ACRS) is pleased to share the first edition of the Asia Pacific financial crime regulatory report, offering a quarterly review of financial crime regulatory developments across the region to help financial institutions (FIs) understand changing regulatory expectations on anti-money laundering and counter-terrorism financing (AML/CTF), scams and fraud. During the third quarter (Q3) of 2026, regulators extended AML/CTF coverage, sharpened scrutiny of control effectiveness, and strengthened responses to scams and technology-enabled fraud. Regulatory attention is focused on whether institutions can counter an increasingly complex financial crime ecosystem that stretches beyond traditional banking, while building robust, structural resistance against highly sophisticated, artificial intelligence (AI)-enabled attacks.

Regulators are extending financial crime oversight across a wider range of sectors and services to address existing gaps. Australia's expanded AML/CTF regime brought specified services provided by professional gatekeepers, including lawyers, accountants and real estate businesses, within scope, while legislative progress continued with the House of Representatives passing the AML/CTF Amendment Bill 2026 to introduce ministerial powers restricting high-risk products such as cryptocurrency automated teller machines (crypto ATMs). Vietnam legislated to include crypto-asset services in its AML framework from 1 December 2026 and strengthen beneficial ownership transparency, including for legal arrangements. This framework is complemented by a decree imposing administrative penalties of up to VND 200 million for pilot crypto-asset market violations, with non-compliance risking operational sanctions such as the suspension of trading for up to 12 months and service provision for up to six months. Meanwhile, Taiwan (China ('Taiwan')) strengthened its market abuse defences by passing the Virtual Asset Service Act. The legislation elevates oversight from an anti-money laundering registration framework to a comprehensive licensing regime, while explicitly criminalising fraudulent, deceptive, and price-manipulating activities with prison terms of three to ten years. Further, Singapore proposed technical amendments to clarify statutory supervision and cooperation powers relating to proliferation financing. These measures address different exposures but share a common purpose of ensuring that financial crime controls reach beyond traditional financial institutions to other participants that facilitate transactions, hold assets, or help establish ownership structures.

As coverage expands, regulators are also seeking stronger evidence that controls work in practice, especially where failure could lead to customer losses through scams. For instance, the Hong Kong Securities and Futures Commission (SFC) has stated that it will hold an internet broker or an SFC-licensed virtual asset service provider (VASP) accountable for client losses if the firm fails to implement adequate measures to prevent, detect and stop large-scale unauthorised transactions through client accounts following a hacking incident. Japan's Financial Services Agency (JFSA) stated in its Initiatives and Challenges in Anti-Money Laundering and Countering Financial Crime (July 2026) report that, with basic AML/CTF frameworks largely established, the focus remains on verifying their effectiveness, particularly in disrupting illicit fund flows from fraudulent activities. Similarly, the July information paper issued by the Monetary Authority of Singapore (MAS) highlights its expectation that digital payment token service providers (DPTSPs) conduct gap assessments and root-cause analyses and promptly address weaknesses in their anti-money laundering, countering the financing of terrorism, and countering proliferation financing (AML/CFT/CPF) controls in response to MAS's supervisory observations.

Source confirmation: "will hold … accountable for client losses" is a strong statement. Check the SFC source to ensure that the wording, conditions and scope of accountability are accurately represented and do not imply broader liability than intended. This review has not independently verified the regulatory claim.

Separately, MAS's newly issued payment service provider (PSP) audit guidelines allow external auditors to adopt a risk-based approach for subsequent annual AML/CFT reviews. Under this framework, auditors must test high-risk areas and previously identified deficiencies every year, while lower-risk areas can be reviewed on a rotational basis. Notably, for new licensees and those introducing new services, auditors are explicitly required to perform an end-to-end review of the adequacy and operating effectiveness of their ML/TF and technology risk controls one-year post-commencement. The Australian Transaction Reports and Analysis Centre (AUSTRAC) also emphasised reinforcing the role of compliance officers and board-level accountability. Thus, a documented framework is only a starting point, with supervisors seeking evidence that controls work in practice and weaknesses are addressed promptly.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Executive Summary

Authorities are strengthening cross-sector information sharing and coordinated action to detect scams and disrupt the movement of illicit funds. Singapore enacted the Scams (Countermeasures) and Other Matters Act 2026. Once the relevant provisions commence, police will be able to order service providers to disclose account information or disable suspected scam-linked accounts under specified conditions. The Australian Financial Complaints Authority (AFCA) was authorised on 1 July 2026 as the external dispute resolution scheme under Australia's Scams Prevention Framework. Entities providing regulated banking, telecommunications, or digital platform services were required to be AFCA members from 1 September 2026, ahead of the framework's operational commencement for scam-related complaints on 31 March 2027, , generally after the business's internal complaints process. The Reserve Bank of India (RBI) consulted on standardised procedures for temporary debit holds on suspected money-mule transactions or accounts, including customer notification, review and coordination with law enforcement. Taiwan's newly mandated cross-sector joint-defence notifications and centralised anti-fraud platform connect information across deposit-taking institutions, electronic payment providers, credit card companies, and VASPs to detect and disrupt fraud networks. The Philippine Amusement and Gaming Corporation's (PAGCOR) casino-sector risk assessment, circulated in July, highlights how funds moving across multiple institutions can limit individual institutions' visibility, making information sharing important for detecting suspicious activity.

At the same time, technology-enabled threats are prompting more specific expectations for authentication and transaction monitoring. A verified customer relationship offers limited protection if criminals subsequently compromise the account or bypass authentication. Hong Kong SAR and Japan addressed this exposure through phishing-resistant authentication and access monitoring, while Thailand consulted on facial recognition safeguards designed to withstand deepfakes. Additionally, AUSTRAC's warnings on synthetic identities and insider-enabled fraud reinforce the need to examine how controls can be bypassed at different stages. Its September supervisory findings on money-mule activity at foreign bank subsidiaries similarly emphasised the need to connect AML/CTF and fraud prevention controls across the customer lifecycle.

Recognising that stronger controls carry costs, regulators are seeking to ease burdens in lower-risk situations while strengthening controls over activities that are more vulnerable to financial crime. The Hong Kong Monetary Authority (HKMA) reinforced differentiated treatment of politically exposed persons (PEPs), with PEP-specific enhanced due diligence required for current non-Hong Kong PEPs but applied to current Hong Kong and international organisation PEPs only where assessed risks are high. In New Zealand, the Department of Internal Affairs became the single AML/CFT supervisor from 1 July 2026. New Zealand's AML/CFT National Strategy 2026–2030 similarly seeks simpler treatment of lower-risk customers, addressing concerns that overly prescriptive requirements increase costs, slow onboarding, and contribute to financial exclusion. Alongside this emphasis on proportionality, regulators are addressing vulnerabilities in specific transaction channels. Mainland China consulted on revised rules for multi-purpose prepaid cards, while Thailand consulted on extending cash-transaction checks to deposits and currency exchange. Greater traceability is also a priority for digital asset transfers, with Japan expanding its Travel Rule designations and Thailand issuing new Travel Rule requirements effective from 27 February 2027. Australia's Travel Rule for virtual-asset transfers also took effect on 1 July 2026, alongside expanded coverage of virtual-asset services.

Overall, financial crime regulation in the Asia Pacific region is expanding beyond traditional institutions and towards greater accountability by relevant stakeholders. This is supported by emphasis on shared information, coordinated action between different agencies, and stronger testing of controls to ensure that they work in practice. The detailed updates that follow outline these developments by jurisdiction, while other notable updates from across the region are captured in the appendix.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Australia



Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Australia (1/4)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	**AUSTRAC**	**AUSTRAC CEO Publishes Mid-Year Update Ahead of Tranche 2 AML/CTF Commencement**	On 30 June 2026, the Australian Transaction Reports and Analysis Centre (AUSTRAC) published a mid-year update from Chief Executive Officer Brendan Thomas, reviewing the first half of the year and setting out regulatory priorities for the second half. The update was issued the day before the 1 July 2026 commencement of Australia's expanded anti-money laundering and counter terrorism financing (AML/CTF) regulatory framework, which extends obligations to Tranche 2 entities. Key achievements cited include the release of intelligence products and updated risk assessments, 2026 updates to money laundering, terrorism financing, and proliferation financing threat assessments, and a not-for-profit risk assessment, as well as updates to the Statement of Regulatory Expectations and enhanced supervisory activities targeting higher-risk sectors. Looking ahead, AUSTRAC will focus on supporting Tranche 2 entities to build compliance capability under the expanded regime, while preparing for Australia's Financial Action Task Force mutual evaluation expected to commence later in 2026. AUSTRAC CEO Publishes Mid-Year Update Ahead of Tranche 2 AML/CTF Commencement | AUSTRAC	Tranche 2 AML/CTF obligations commence on 1 July 2026.
2	**AUSTRAC**	**AUSTRAC Announces Commencement of AML/CTF Obligations for Tranche 2 Entities**	On 1 July 2026, AUSTRAC commenced the expanded AML and CTF laws to include newly regulated sectors such as real estate, conveyancing, legal services, accounting and precious stones and metals, marking the largest expansion of Australia's AML/CTF regime since the original AML/CTF Act 2006 was enacted. Newly regulated entities must have an AML/CTF programme, appointed compliance officer, and trained staff in place from that date, as set out in the AML/CTF Rules 2025. Newly regulated entities had until 29 July 2026 to enrol with AUSTRAC. AUSTRAC Announces Commencement of AML/CTF Obligations for Tranche 2 Entities | AUSTRAC	Enrolment deadline for newly regulated entities: 29 July 2026.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Australia (2/4)

#	Issuing Authority	Title	Regulatory Update	Key Dates
3	**AUSTRAC**	**AUSTRAC Publishes CEO Address on Evolving Financial Crime Threats Delivered at the AFIA Risk Summit**	On 6 July 2026, AUSTRAC published remarks delivered by Chief Executive Officer Brendan Thomas to the Australian Finance Industry Association (AFIA) Risk Summit in Melbourne, reviewing progress in the non-bank lending sector's compliance with anti-money laundering and counter-terrorism financing (AML/CTF) obligations and outlining the evolving threat landscape. AUSTRAC reported a 12 per cent uplift in suspicious matter report (SMR) volumes from the sector in the first half of 2026 compared with the same period in 2025, alongside a 20 per cent increase in the number of reporting entities lodging SMRs—a clear improvement from the previous year's campaign findings, which had characterised controls as poor. AUSTRAC's CEO identified four key emerging threat typologies requiring heightened vigilance: • **AI-enabled fraud** including synthetic identity generation, automated movement of digital assets, and deepfake verification bypass; • **Professionalised global money laundering networks** operating with corporate-like structures and cross-jurisdictional logistics; • **Insider-enabled fraud**, where compromised employees or contractors help criminals bypass technical controls; and • **Micro money laundering through structured small-value transactions** designed to evade detection thresholds. Thomas also highlighted a significant mortgage fraud pattern detected across ten of Australia's largest lenders through the Fintel Alliance, exposing weaknesses in traditional credit verification processes. Finally, Thomas reinforced AUSTRAC's expectations under AML/CTF reforms that commenced on 31 March 2026, including mandatory chief money laundering officer appointments and stronger board-level accountability for articulating and managing AML risk. AUSTRAC Publishes CEO Address on Evolving Financial Crime Threats Delivered at the AFIA Risk Summit | AUSTRAC	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Australia (3/4)

#	Issuing Authority	Title	Regulatory Update	Key Dates
4	**Parliament of Australia**	**AML/CTF Amendment Bill progresses with revised safeguards and implementation timing**	Originally introduced on 12 March 2026, the Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2026 proposes new powers to restrict or prohibit reporting entities from using "high-risk" products, services or delivery channels when providing designated services, with cryptocurrency automated teller machines (crypto ATMs) a primary target. It also updates the definition of financing of terrorism to reference existing state-sponsor offences and introduces technical amendments. Following the Parliamentary Joint Committee on Intelligence and Security's (PJCIS) report on 11 August, the House of Representatives passed the amended Bill on 16 September 2026. The amendments agreed by the House would: • **Strengthen Ministerial Accountability**: Shift the proposed restriction/prohibition power from the Australian Transaction Reports and Analysis Centre (AUSTRAC) Chief Executive Officer (CEO) to the responsible Minister, who would be required to seek and consider advice from the AUSTRAC CEO before acting. • **Increase Consultation Transparency**: Require legislative instruments imposing or extending restrictions or prohibitions to be accompanied by explanatory statements describing any consultation undertaken. • **Allow More Preparation Time:** Delay the proposed commencement of the high-risk-mechanism power from 1 January 2027 to 1 July 2027. • **Status:** Following House passage on 16 September 2026, further parliamentary passage (the Senate) and Royal Assent are required before the Bill becomes law. Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2026 – Parliament of Australia	Bill passed the House of Representatives on 16 September 2026.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Australia (4/4)

#	Issuing Authority	Title	Regulatory Update	Key Dates
5	**ASIC**	**ASIC Prioritises Scams and AI-Related Threats to Market Integrity in its 2026–27 Corporate Plan**	On 26 August 2026, ASIC published its 2026–27 Corporate Plan, identifying scams and emerging AI-related risks among its priorities. ASIC will focus on areas where consumer harm can spread quickly or have lasting consequences, and examine how AI affects consumers, investors and market integrity, including the potential for AI-driven market manipulation, deepfakes and misinformation. The plan also outlines investment in ASIC's data, intelligence, AI and cyber capabilities to support its regulatory work. For financial crime teams, it signals continued attention to scam prevention and technology-enabled misconduct, rather than introducing new compliance requirements. Key priorities include: • Examine the impact of AI on consumers, investors and market integrity; • Reduce regulatory burden through simpler guidance, improved digital services, more efficient licensing processes and closer regulatory coordination; • Strengthen supervision of managed investment schemes and continue efforts to improve market integrity; and • Support responsible digital finance and innovation while building ASIC's data, intelligence, AI and cyber capabilities. ASIC Sets Plan to be Easier to Deal with, Harder to Avoid | ASIC ASIC Corporate Plan 2026–27	-
6	**AUSTRAC**	**AUSTRAC Highlights Money Mule Risks in Retail Banking**	On 30 September 2026, AUSTRAC published a supervisory follow-up on its late-2025 review of foreign bank subsidiaries in Australia. It highlighted lessons for the wider Australian banking sector. Key updates include: • **Previously reported in April:** AUSTRAC had identified money mule risks at onboarding, during account use and in cross-border transfers. It urged the banks reviewed to strengthen controls and report suspicious activity to AUSTRAC. • **Additional campaign detail in September:** AUSTRAC described coordinated account openings, repeated use of contact details, and many small, scam-related transactions sent offshore via digital currency exchanges, remittance providers and cash. • **Practical steps highlighted in September:** AUSTRAC encouraged fraud prevention and anti-money laundering and counter-terrorism financing teams to work together throughout the customer relationship. It suggested screening for reused or varied customer details at account opening and considering limits on how many accounts one person can open. It reinforced the importance of effective suspicious matter reporting and highlighted onboarding, biometrics and transaction monitoring as areas for stronger controls at banks with more complex operations. Managing money mule risks in banking | AUSTRAC	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

China Mainland



Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

China Mainland (1/2)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	NFRA	NFRA Establishes a Three-Year Serious Dishonesty List with a Credit Repair Exit After One Year	On 3 July 2026, China's National Financial Regulatory Administration (NFRA) issued Order 2026 No. 3, establishing new trial rules to manage its financial-sector "blacklist" starting 1 October 2026. An entity is only listed under this trial framework if it has received an administrative penalty and its actions were deemed exceptionally egregious. **1. How Entities Get Blacklisted** • **Severe Penalties:** Automatic listing for revoked business licenses, lifetime banking/insurance bans, or permanent cancellation of management qualifications; • **Specific Breaches:** Severe misconduct including licensing or loan fraud, shareholder/controller abuse, illegal fundraising, or unauthorized financial activities; and • **Court Enforcement:** Refusal to comply with an outstanding NFRA penalty, leading to a court-enforced execution order. **2. Consequences** Blacklisted entities face negative weighting in license and procurement reviews, significantly more frequent regulatory inspections, disqualification from fast-track administrative processes, and public disclosure of their status. **3. Due Process & Appeals** Before listing, entities have a 10-working-day defense window. The NFRA must verify and respond within 20 working days (extendable by 20 days). Blacklisting or removal decisions made by prefectural or lower offices require provincial-branch approval. **4. Removal from Blacklist** • **Standard Exit:** Automatic removal after three years, or immediately if the underlying penalty is overturned. • **Early Exit:** Eligible after one year if the entity fully corrects its behavior and pays all penalties. Providing false materials to secure early exit restarts the three-year term from zero. NFRA Establishes a Three-Year Serious Dishonesty List with a Credit Repair Exit After One Year | NFRA NFRA Provisions on the Management of the List of Seriously Dishonesty Entities (Trial) | NFRA	Effective on 1 October 2026.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

China Mainland (2/2)

#	Issuing Authority	Title	Regulatory Update	Key Dates
2	**PBOC**	**PBOC Consults on Replacing the 2012 Prepaid Card Measures with a Stored Value Account Regime**	To curb shadow-banking, money laundering, and financial crime (such as fraud and tax evasion), and to return multi-purpose prepaid cards to low-value consumer use, the PBOC on 24 July 2026 opened a consultation on the Measures for Class II Stored Value Account Operation Business (Draft for Comment). This implementing rule under State Council Order No. 768 governs prepaid card issuers, excludes single-purpose store cards, and repeals PBOC Announcement 2012 No. 12. For FSIs, this tightening should redirect corporate transaction volumes back into formal banking channels and may trigger payment-sector consolidation. Under the draft, cards divide into: 1. **Registered** (capped at RMB 5,000, no expiry, supports loss reporting and redemption); and 2. **anonymous** (capped at RMB 1,000, minimum 3-year term, extendable). Real-name ID is mandatory for registered card purchases and anonymous purchases of RMB 10,000 or more. Non-cash bank transfers are required for corporate purchases of RMB 5,000 or more and individual purchases of RMB 50,000 or more. Card sales are confined to physical outlets, except for public transport cards (capped at RMB 200 per card and RMB 10,000 annually per payer). Usage is strictly limited: a single payment cannot exceed RMB 10,000, and cards cannot fund cash withdrawals, other prepaid cards, or external bank transfers. Online payments are barred except for utility bills, the issuer's physical merchants' online stores, or Class I account top-ups (capped at RMB 5,000 annually). Registered cards can be refunded starting three months after purchase. Finally, payment firms must directly sign and manage 100% of their partner merchants—completely banning core outsourcing—under a two-year transition period. PBOC Consults on Replacing the 2012 Prepaid Card Measures with a 57-Article Class II Stored Value Account Regime | PBOC Explanatory Statement on the Proposed Measures for the Administration of Class II Stored Value Account Operation Business | PBOC	Public consultation ended on 7 August 2026.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Hong Kong SAR



Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Hong Kong SAR (1/2)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	SFC	**SFC Mandates Phishing-Resistant Authentication and Suspicious Activity Surveillance for Internet Brokers and Virtual Asset Service Providers**	Under the banner of cyber-enabled financial crime and fraud prevention, the Hong Kong Securities and Futures Commission (SFC) has issued strict new rules to eliminate OTP-based account takeovers. On 9 July 2026, the Securities and Futures Commission (SFC) issued a circular (26EC35, reference SFO/IS/021/2026) requiring licensed corporations engaged in internet trading and SFC-licensed virtual asset service providers (VASPs) to deploy phishing-resistant authentication and adequate monitoring and surveillance measures. The circular addresses licensed corporations holding Type 1, Type 2, Type 3, or Type 9 licences alongside VASPs; associated entities are not named in the addressee line. Firms must adopt passkeys based on public-key cryptography and device binding for client login. The SFC states expressly that it does not consider a one-time password to be a phishing-resistant authentication solution and that internet brokers and VASPs should not use one for the processes covered. Transaction monitoring must flag abnormal trading patterns, unusual timing, large trades in illiquid stocks, and activity following password resets or device changes. Key requirements include: • Clients may not bind or register more than three passkeys and three devices for their internet trading accounts; • Client notification of successful logins, new device binding and suspicious activity must be delivered through multiple communication channels where applicable, such as email, SMS or push notification; • Hacking incidents must be reported to the SFC immediately, alongside containment, asset protection and client notification procedures; • The Manager-In-Charge of Overall Management and Oversight and the Manager-In-Charge of Information Technology are ultimately responsible for implementation; • The SFC states it will hold a firm accountable for client losses where measures are inadequate; and • No size-based exemption is provided; the SFC states it will take a pragmatic approach where systems require updating and expects large internet brokers to implement immediately rather than at the outer deadline. SFC Mandates Phishing-Resistant Authentication and Suspicious Activity Surveillance for Internet Brokers and Virtual Asset Service Providers | SFC	**Effective on 9 July 2026.** **Full authenticati on rollout deadline: 8 July 2027.**

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Hong Kong SAR (2/2)

#	Issuing Authority	Title	Regulatory Update	Key Dates
2	HKMA	**HKMA Issues Version 2.0 of the Politically Exposed Persons Smart Tips on Risk-Based AML/CFT Controls**	On 28 August 2026, HKMA issued a circular on risk-based anti-money laundering and counter-financing of terrorism (AML/CFT) controls for politically exposed persons (PEPs). It was addressed to the chief executives of all authorised FIs and stored value facility (SVF) licensees, and enclosed version 2.0 of the "Smart Tips on the Treatment of Politically Exposed Persons", dated August 2026. The HKMA stated that, since the Smart Tips were first issued in November 2025, engagement with FIs and SVF licensees indicates institutions have been proactively changing their PEP-related controls to meet its expectations on proportionality and fair treatment, while room for improvement remains. Version 2.0 retains the differentiated treatment at the core of the guidance. PEP-specific enhanced due diligence (EDD) is required for non-Hong Kong PEPs regardless of the level of risk, with its extent proportionate to the PEP-related risk. Hong Kong PEPs and international organisation PEPs are treated as regular customers, unless the customer risk assessment reveals a high money laundering or terrorist financing risk. Middle-ranking and more junior officials fall outside the PEP definition. EDD comprises reasonable measures to establish source of wealth and source of funds, senior management approval to establish or continue the relationship, and enhanced ongoing monitoring including annual customer due diligence reviews; for former PEPs, continued classification and EDD turn on a holistic risk assessment. The updated Smart Tips also record good practices brought to the HKMA's attention since November 2025. These include a dedicated team serving PEP customers, and proactive oversight of frontline staff through customer satisfaction surveys and compliance reviews. A further practice is holistic relationship-based review that treats a PEP and family members as a group, while allowing individual risks to be assessed independently. The HKMA noted that some institutions are exploring technology solutions, including artificial intelligence, to improve customer experience during PEP-related reviews, and will continue to support these efforts through its AML/CFT technology adoption support programme. Authorised FIs and SVF licensees are expected to consider adopting the updated good practices, and the HKMA will undertake a round of thematic examinations later in the year to test how effectively they have been implemented. HKMA Issues Version 2.0 of the Politically Exposed Persons Smart Tips on Risk-Based AML/CFT Controls | HKMA Smart Tips on the Treatment of Politically Exposed Persons Version 2.0 | HKMA	Thematic examinations to be conducted later in 2026.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

India



Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

India (1/1)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	RBI	RBI Consults on Proposed Standardised Procedures for Temporary Debit Holds on Suspected Money-Mule Accounts	On 11 September 2026, Reserve Bank of India (RBI) published draft amendments that would add a standard operating procedure to its Know Your Customer (KYC) Directions, 2025. It would govern how commercial banks, including payments banks, and urban co-operative banks place, review and lift bank-initiated temporary debit holds linked to suspected money-mule activity or cyber-enabled financial fraud. Key updates include: • **Identification:** the draft defines a suspected money-mule transaction as one of ₹1,000 or more flagged by the bank's monitoring systems as suspected to involve proceeds of money-mule activity or cyber-enabled financial fraud. • **Temporary debit holds:** on identifying a suspected transaction, banks would immediately place a debit hold on the amount concerned. A hold on an entire suspected mule account would be a last resort, reserved for exceptional circumstances. • **Customer notice and review:** banks would notify customers immediately if communicating digitally, or by the end of the next day otherwise. Customers would have 20 calendar days from the hold to respond. Banks would decide within 10 days of receiving a response, or within 30 days of the hold if none is received. • **Police referral and release:** if a bank maintains the hold after review, it would refer the case to the relevant police authority. If it receives no legally backed direction to continue within 30 days of referral, it would lift the hold on day 31 from referral. Absent contrary instructions from law enforcement or another competent authority, the overall cap would be 60 calendar days from the start of the hold. RBI invites comments on the Draft "Reserve Bank of India (Know Your Customer) Amendment Directions, 2026	Public consultation ended on 2 October 2026. Supreme Court Order: 4 August 2026. Proposed Go-Live Date: 1 April 2027.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix



Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Japan (1/6)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	JFSA	**JFSA Publishes 2026 Report on AML/CFT and Countering Financial Crime**	On 3 July 2026, Japan's Financial Services Agency (JFSA) published *Initiatives and Challenges in Anti-Money Laundering and Countering Financial Crime (July 2026)*, summarising the JFSA's initiatives, the status of responses by financial institutions and international developments, mainly covering the 2025 programme year (July 2025 to June 2026). The report states that almost all financial institutions covered by the review have largely established basic anti-money laundering and countering the financing of terrorism (AML/CFT) risk control frameworks. The continuing focus is on verifying their effectiveness and making improvements based on institutions' own assessments, including in preparation for Japan's Financial Action Task Force (FATF) fifth-round mutual evaluation. The JFSA has been assessing effectiveness-verification efforts through inspections and other supervisory activities since July 2025. Key areas covered include: • **AML/CFT effectiveness:** supervisory inspections of how financial institutions verify the effectiveness of their AML/CFT frameworks, together with continued enhancement of governance, staffing, internal coordination and internal audit. Inspections identified shortcomings at some institutions in risk-based testing coverage, sampling methods and coordination between relevant departments. • **Guidelines and international developments:** the March 2026 revisions to the JFSA's AML/CFT Guidelines and frequently asked questions (FAQs), including clarified expectations for detecting and responding to account misuse and overseeing outsourced AML/CFT functions; FATF fifth-round mutual evaluation developments; the risk-based approach; revisions to FATF Recommendation 16; and developments relating to crypto-assets and stablecoins. • **Financial crime:** measures addressing increasingly sophisticated online and telephone scams, phishing and fraudulent transactions, including efforts to strengthen detection and prevent fraudulent use of accounts. A November 2025 follow-up survey found limited progress on controls requiring system changes, including identity-document chip verification, detection based on users' access environments and automated restrictions on detected fraudulent transactions. It also highlighted scams in which victims themselves are deceived into authorising transfers. • **Information sharing and cooperation:** stronger information sharing among financial institutions and greater public-private cooperation, including with law-enforcement authorities. The report also notes that financial institutions are expected to continue strengthening their AML/CFT and financial crime controls in response to emerging risks, including crypto-assets, stablecoins and online casinos. FSA publishes "Initiatives and Challenges in Anti-Money Laundering and Countering Financial Crime (July 2026)": FSA	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Japan (2/6)

#	Issuing Authority	Title	Regulatory Update	Key Dates
2	**JFSA**	**JFSA Extends Crypto Travel Rules to Five New Jurisdictions**	On 7 July 2026, Japan's Financial Services Agency (FSA) finalised amendments expanding the geographical scope of its Travel Rule for cryptoasset and stablecoin transfers. Effective from 3 August 2026, the amendment adds Anguilla, Botswana, Dominica, Cuba and Oman, increasing coverage for cryptoasset transfers from 58 to 63 jurisdictions. The expansion extends existing requirements for Japanese cryptoasset exchange and electronic payment instrument service providers to transmit originator and beneficiary information when making covered transfers to providers in the newly designated jurisdictions. It changes geographical coverage rather than the underlying information requirements. Key features include: • **Information sharing:** Transmit originator and beneficiary details, including names and blockchain addresses or equivalent identifiers, together with the prescribed originator address or customer identification information.l • **Transfer coverage:** Apply the requirements regardless of transfer amount or cryptoasset type, including regulated stablecoins, subject to specified exclusions; • **Record retention:** Retain all Travel Rule information transmitted and received; and • **Jurisdictional equivalence:** Cover foreign jurisdictions with notification requirements equivalent to Japan's, assessed using FATF evaluations, follow-up reports and local legal frameworks. Transfers to individuals and unregistered providers fall outside these notification requirements. The expansion requires affected Japanese providers to incorporate the five jurisdictions into their Travel Rule processes so that covered transfers carry the required information. Applicable requirements to collect and retain wallet-owner information continue to apply to transactions involving wallets outside that duty. Publication of the finalized "the Partial Amendment to the Designation of a country or region under Articles 17-2 and 17-3 of the Order for Enforcement of the Act on Prevention of Transfer of Criminal Proceeds" after public consultation | FSA	Effective from 3 August 2026.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Japan (3/6)

#	Issuing Authority	Title	Regulatory Update	Key Dates
3	**National Diet**	**Japan's Stronger Account-dealing Penalties and New Remittance Offences Enter Into Force**	On 10 July 2026, provisions of the amended *Act on Prevention of Transfer of Criminal Proceeds* came into force, increasing penalties for unlawful account dealing and introducing new remittance offences. The amendments, outlined by the National Polica Agency (NPA) were promulgated on 10 June 2026. The reforms respond to account misuse by anonymous, fluid criminal networks, which exploit traded accounts and recruit individuals via social media to move funds. Key changes include: • **Account trading penalties:** Maximum penalties for unlawful dealing in passbooks, cash cards or credentials for specified financial services have increased from one year's imprisonment, a fine of 1 million Japanese yen (JPY), or both, to three years' imprisonment, a JPY 5 million fine, or both. The scope includes bank accounts and certain payment and crypto-asset service accounts. • **Account dealing as a business:** Penalties under this existing category have increased from three years' imprisonment, a JPY 5 million fine, or both, to five years' imprisonment, a JPY 10 million fine, or both. • **New remittance offences:** These cover specified transfers for payment or other consideration without legitimate justification. They apply to qualifying transfer requests, those carrying them out with knowledge of the requester's purpose, and certain recruitment or solicitation. Legitimate commercial and financial transactions are excluded. Maximum penalties are two years' imprisonment, a JPY 3 million fine, or both. Requesting or executing the offences as a business carries maximum penalties of three years' imprisonment, a JPY 5 million fine, or both. • **Fictitious-name investigative accounts:** A separate part of the amendments will permit police to request specially designated accounts under fictitious names and use them to prevent account misuse. It also provides for custody and return of funds received and victim-recovery payments under specified conditions. 2026 amendments to the Act on Prevention of Transfer of Criminal Proceeds - NPA Order to Partially Amend the Enforcement Regulations of the Act on Prevention of Transfer of Proceeds from Crime | FSA	Effective from 10 July 2026. Fictitious-name investigative accounts will have separate effective date to be determined by Cabinet Order, within one year of 10 June 2026.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Japan (4/6)

#	Issuing Authority	Title	Regulatory Update	Key Dates
4	JFSA	**JFSA Sets Phishing-Resistant Authentication and Anti-Phishing Expectations for Online Services of Insurers, Money Lenders and Payment Firms**	On 17 July 2026, JFSA published the results of its public consultation and applied amendments to eight sets of supervisory and administrative guidelines. The purpose is to strengthen the response to cyber risks that have increased in recent years. The amendments create dedicated sections on online (internet) transactions in the guidelines for insurance companies, small-amount and short-term insurance providers, money lenders, prepaid payment instrument issuers and funds transfer service providers, and extend related expectations to insurance brokers, financial services intermediaries and the electronic payment services of banks. They build on the JFSA's Guidelines for Cybersecurity in the Financial Sector. Uniform implementation is not required and each firm should assess its own risks, and that where system development takes time a phased rollout by customer segment is acceptable, although early implementation is encouraged. Firms are also expected to ensure that outsourced service providers implement equivalent fraud prevention measures. Key changes include: • **Phishing-resistant multi-factor authentication (MFA):** Phishing resistant MFA such as passkeys or certificate-based log-in, is expected to be implemented and made mandatory by default for important operations such as logging in, withdrawing money and changing the account to which funds are paid; until then, firms are expected to offer another multi-factor method and tell customers when the stronger method will arrive; • **Customer opt-out:** Customers may switch this authentication off only where they are unable to use it for unavoidable reasons, such as not having a suitable device, in which case firms are expected to offer an alternative multi-factor method and monitor how many customers opt out; • **Access monitoring:** Firms are expected to alert customers to log-ins, transactions and withdrawals they may not recognise, lock accounts after repeated failed log-in attempts, and analyse log-in behaviour to detect unauthorised access; • **Login Links in Communications:** Emails and text messages are in principle not to contain links to log-in pages or pages asking for passwords unless there is no alternative, and firms are expected to adopt sender authentication technology and seek the takedown of phishing sites; • **Response and Reporting:** Firms are expected to respond sincerely to customers who suffer losses from fraudulent transactions, including through compensation, and to report unauthorised access or transactions to the authorities promptly in a crime occurrence report; and • **Intermediary Security Verification:** Financial institutions partnering with financial services intermediaries are expected to verify that those intermediaries implement sufficient cybersecurity and anti-phishing measures, while the intermediaries themselves must directly apply these measures where it is more effective for protecting their customers. JFSA Sets Phishing-Resistant Authentication and Anti-Phishing Expectations for Online Services of Insurers, Money Lenders and Payment Firms | JFSA	Effective on 17 July 2026.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Japan (5/6)

#	Issuing Authority	Title	Regulatory Update	Key Dates
5	**SESC**	**SESC Publishes Monitoring Priorities for Securities Businesses (July 2026- June 2027)**	On 31 July 2026, the Securities and Exchange Surveillance Commission (SESC) published its Monitoring Priorities for Securities Businesses (July 2026–June 2027). While this annual programme outlines broader supervisory priorities covering customer-oriented business conduct, suitability principles, and systemic risk, the SESC places significant emphasis on financial crime. Key priorities include anti-money laundering and countering the financing of terrorism (AML/CFT), and cyber-enabled fraud. The SESC will continue a risk-based approach to selecting Financial Instruments Business Operators (FIBOs) for on-site inspections. Within this broader supervisory context, the key financial crime-related priorities include: **1. AML/CFT control frameworks** • **Established controls:** The SESC will verify whether FIBOs have developed and strengthened their internal control frameworks in accordance with the required actions in the existing AML/CFT Guidelines. • **Audit and follow-up:** Inspectors will evaluate whether management implements effective improvements and measures to prevent recurrence following findings from internal audits or examinations by Self-Regulatory Organisations (SROs). **2. Market abuse and investment fraud** • **Market abuse:** Review od trade surveillance, corporate information management and underwriting review controls at major globally active Japanese securities groups. • **Investment fraud**: Review of funds claiming high returns and whether underlying projects exist, covering Type II FIBOs and relevant qualified institutional investor business operators. **3. Customer due diligence (CDD) and trade monitoring** • **Cybercrime controls:** Reflecting increasingly sophisticated methods involving unauthorised access and transactions, the SESC will conduct cross-sectional reviews of online securities firms' cybersecurity, CDD measures when transactions take place, and trade-monitoring frameworks. This includes firms with face-to-face operations that also offer internet trading. • **Frontier AI threats:** Guided by wider, industry-wide system risk priorities, the SESC will review firms' responses to changing cyber threats associated with frontier AI. **4. Action against fraudulent solicitation and unregistered operators** • **Combating investment scams:** The priorities reference record losses in 2025 from special fraud and social media-based investment and romance scams. They also reference the July *2026 Emergency Measures to Prevent the Spread of Damage from Fraud and Stalking*, including action against celebrity impersonation advertisements. • **Enforcement against unregistered firms:** The SESC will use its investigative authority to seek court prohibition and stay orders against illegal conduct and disclose the names and illegal conduct of unregistered operators. • **Social media monitoring and cooperation:** The SESC will strengthen vigilance over social media advertisements and investor warnings, working with domestic authorities and foreign authorities on cross-border cases. Monitoring Priorities for Securities Businesses (July 2026 – June 2027) | SESC Monitoring Priorities for Securities Businesses (July 2026 – June 2027) – English version | SESC Summary of Monitoring Priorities for Securities Businesses (July 2026 – June 2027) | SEC	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Japan (6/6)

#	Issuing Authority	Title	Regulatory Update	Key Dates
6	JFSA	**JFSA Publishes Strategic Priorities for July 2026 - June 2027**	On 15 September 2026, Japan's Financial Services Agency (JFSA) published its *FSA Strategic Priorities: July 2026–June 2027*. Whilst this annual programme outlines a broader financial regulatory and supervisory agenda supporting sustainable growth, financial stability and household asset building, financial crime was one of the key themes covered. Key financial crime-related priorities include: • **Financial crime mitigation:** Strengthening measures against fraud and unauthorised transactions, including information sharing on misused accounts, early detection and rapid account freezing. The JFSA will also promote stronger anti-money laundering frameworks ahead of the Financial Action Task Force's (FATF) fifth-round mutual evaluation of Japan. • **Market abuse and integrity:** The Securities and Exchange Surveillance Commission (SESC) will conduct investigations and inspections where legal breaches are suspected, including large shareholdings and acquisitions designed to evade applicable rules, and unregistered financial instruments business conducted through social media. • **Cyber resilience**: Addressing cyber threats associated with artificial AI, through broader supervisory monitoring, cybersecurity exercises and self-assessments to strengthen financial institutions' defences and incident preparedness. • **Crypto-related fraud:** Following up on the August 2026 request for crypto-asset exchanges to strengthen anti-fraud measures. The programme also includes progressing regulatory work on a cooling-off period before customers can transfer crypto-assets from newly opened exchange accounts to unhosted wallets. **Broader context:** As part of broader supervisory modernisation, the JFSA plans to expand its use of data analytics and generative AI in supervision, monitoring and market surveillance, and enhance its joint data platform with the Bank of Japan. FSA publishes "FSA Strategic Priorities: July 2026 - June 2027" : FSA	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Malaysia



Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Malaysia (1/1)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	BNM	**BNM Finalises Interoperable Transfer Framework with Fraud Prevention Safeguards**	On 30 June 2026, BNM issued the Interoperable Fund Transfer Framework (IFTF), together with an accompanying feedback statement. The framework promotes interoperable payments through shared infrastructure. It generally took effect that day, subject to specified transition arrangements. The provisions relevant to financial crime include: • **Shared visibility of payments**: BNM reiterates that both "on-us" and "off-us" quick response (QR) fund transfers must route through the shared payment infrastructure. This is intended to support system-wide transaction monitoring and coordinated fraud detection and response. The exception for certain proprietary arrangements under paragraph 9.13 remains applicable. • **Access safeguards**: Other regulated entities in Malaysia seeking access must demonstrate compliance with relevant BNM standards covering customer and merchant onboarding, protection measures, and anti-money laundering and countering the financing of terrorism (AML/CFT) risk management. Compliance must be independently assessed by an external party. • **Consumer safeguards:** Financial institutions must provide online transaction-limit management and instant notifications for outgoing and incoming transfers, protect financial consumer data against loss, theft or unauthorised access, and take reasonable steps to provide timely safety guidance. Notifications may be disabled at the consumer's request and with consent, after the risks have been explained. BNM Policy Document on Interoperable Fund Transfer Framework | BNM BNM Feedback Statement on Interoperable Fund Transfer Framework | BNM	Deadline for full phase-out of proprietary QR code scheme networks: 30 June 2028.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

New Zealand



Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

New Zealand (1/2)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	MOJ	**AML/CFT National Strategy Launches Four-Year Reform Programme and Industry Levy**	On 1 July 2026, New Zealand's Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) National Strategy 2026–2030 came into effect and its four-year work programme commenced. The reforms respond to issues identified through New Zealand's 2021 Financial Action Task Force (FATF) mutual evaluation and the 2022 statutory review of the AML/CFT Act. The Strategy targets six areas for reform, with actions phased over the programme period: • **Risk-based regulation:** Current requirements are considered overly prescriptive in some areas, limiting proportionate treatment of lower-risk customers and contributing to compliance costs, slow onboarding and financial exclusion. Proposed responses include legislative changes, simplified customer due diligence for lower-risk situations, and sector-specific guidance and training. • **Supervisory consistency:** The previous three-supervisor model was found to produce inconsistent interpretation, risk-rating, guidance and enforcement. The Department of Internal Affairs (DIA) became the sole supervisor on 1 July 2026. The work programme provides for regular off-site and on-site supervision of the five major banks. Other banks are subject to risk-based supervision, with on-site inspections at intervals no longer than five years. • **Intelligence and information sharing:** Risk assessments have been produced intermittently, while financial intelligence has often been used reactively to support ongoing investigations. The programme proposes more frequent national, sectoral and thematic risk products, improved reporting to the New Zealand Police Financial Intelligence Unit (FIU), and stronger public-private information sharing. • **Detection and enforcement:** Planned changes include additional FIU tools and powers, improved suspicious activity reporting, investment in analytical technology, and a wider range of enforcement responses. • **Targeted financial sanctions:** The programme plans legislative changes, guidance and risk-based supervision to embed terrorism and proliferation-financing sanctions into the AML/CFT system. • **International standards:** The reforms are intended to address outstanding FATF findings and prepare New Zealand for its fifth-round FATF/Asia/Pacific Group on Money Laundering (APG) mutual evaluation. FATF's indicative timetable shows a possible on-site assessment in February 2029 and possible plenary discussion in October 2029, subject to change. Delivery will require capability and technology investment across the participating agencies. More timely intelligence and guidance are intended to help reporting entities allocate resources according to risk. The programme will be part-funded through a new industry levy alongside Crown funding. Banks and deposit takers will contribute 85.25% of levy costs, with liability based on reported asset value. Annual levy collection of 27.33 million New Zealand dollars (NZD) is scheduled to commence from 1 July 2027, including recovery of costs incurred before collection begins. AML/CFT National Strategy 2026-2030 | MOJ	Levy collection commences from 1 July 2027. FATF/APG mutual evaluation currently scheduled for on-site assessment in February 2029.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

New Zealand (2/2)

#	Issuing Authority	Title	Regulatory Update	Key Dates
2	DIA	**DIA Becomes Sole AML/CFT Supervisor and Launches a 23-Document Guidance Suite for Reporting Entities**	On 1 July 2026, the Department of Internal Affairs (DIA) became New Zealand's sole supervisor under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009, taking over from the Reserve Bank of New Zealand and the Financial Markets Authority and ending the tripartite supervisory model. Acting Director AML/CFT Caroline BridglandHill framed single-agency supervision as an opportunity for greater consistency and clearer expectations. The change covers all reporting entities, including registered banks, licensed insurers, non-bank deposit takers and securities and investment entities. The DIA marked the transfer by publishing 23 pieces of guidance and educational material, spanning risk assessment, country risk, customer due diligence across corporate and trust structures, designated business groups, audit, and wire transfers. The suite follows DIA's June 2026 release of updated AML/CFT Compliance Programme and Enhanced Customer Due Diligence guidance, issued to support implementation of the AML/CFT Amendment Act 2026. Two interpretive changes carry direct operational consequence. Non-bank financial institutions that do not physically transfer funds are now within scope of prescribed transaction reporting for international transfers, reversing prior FMA guidance. Separately, a three-step territorial scope test now governs whether the Act applies, weighing whether activities occur in New Zealand and whether sufficient New Zealand connections exist. DIA Becomes Sole AML/CFT Supervisor and Launches a 23-Document Guidance Suite for Reporting Entities | DIA	Effective on 1 July 2026.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Philippines



Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Philippines (1/1)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	**BSP**	**BSP Tightens Anti-money Laundering Controls on Casino Junkets**	On 2 July 2026, The Bangko Sentral ng Pilipinas (BSP) issued guidance requiring banks and other supervised financial institutions to strengthen anti-money laundering (AML) controls over casino junket operators. The guidance follows a thematic review of selected universal, commercial and thrift banks with exposure to junkets, which arrange travel, credit and casino bookings for high-value players. The review identified vulnerabilities arising from cash-intensive operations, cross-border transfers, limited transparency over players' identities and sources of funds, and the use of intermediaries and layered transactions. Cash and cheques remain the primary means of moving funds, with frequent transfers involving casinos, junket operators, financiers, players and money service businesses. **Key areas highlighted include:** • **Customer due diligence**: Strengthen checks on customer identities, ownership structures and business activities, including identifying players or financiers who are also junket operators or beneficial owners; • **Tailored risk controls:** Adopt policies reflecting junket operators' transaction patterns and business risks, beyond their existing classification as high-risk customers; • **Transaction monitoring**: Enhance scrutiny of transactions inconsistent with declared sources of funds, unexplained large cash and cheque deposits, and chip purchases using small-denomination cash followed by minimal gaming; • **Suspicious transaction reporting:** Strengthen reporting processes and consider warning signs, including failures to report transactions required under junket agreements; and • **Information sharing:** Improve coordination between the BSP, the Philippine Amusement and Gaming Corporation (PAGCOR) and financial institutions. The BSP noted that limited official information on registered and delisted junket operators and their beneficial owners continues to hinder risk assessment. Closer information sharing will be critical to addressing these gaps and strengthening oversight of the sector. Guidance Paper on Risk Management Practices for Customers Engaged in Casino Junket Operations | BSP	Issued on 2 July 2026
2	**PAGCOR**	**PAGCOR Second Casino Sector Risk Assessment**	On 13 July 2026, the Philippine Amusement and Gaming Corporation (PAGCOR) circulated its second casino sector risk assessment, covering 2021–2024. It rated sector-wide money laundering risk High and terrorism financing risk Medium-High. PAGCOR provided guidance to the entities it regulates on using the findings in their institutional risk assessments and compliance frameworks. PAGCOR Advisory No. 2026-005 and risk assessment	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Singapore



Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Singapore (1/4)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	**MAS**	**MAS Sets Out AML/CFT Supervisory Expectations for Digital Payment Token Services Providers**	On 13 July 2026, MAS published an information paper setting out its observations and supervisory expectations for digital payment token service providers' (DPTSPs) anti-money laundering, countering the financing of terrorism, and countering proliferation financing (AML/CFT/CPF) controls. Drawing on MAS inspections and ongoing engagements with licence applicants and licensees, the paper covers seven areas: new product and digital payment token (DPT) listing risk assessment, enhanced customer due diligence for higher-risk customers, value transfer requirements, ongoing monitoring, screening, partner and outsourcing due diligence, and training and staff expertise. The paper supplements MAS Notice PSN02 on Prevention of Money Laundering and Countering the Financing of Terrorism – Digital Payment Token Service and its accompanying Guidelines. Pre-listing DPT assessments should consider risks directly associated with the token, its track record and governance, market and economic indicators relating to manipulation and fraud, and smart contract and blockchain vulnerabilities, with ongoing adverse news monitoring formalised and documented. MAS expects DPTSPs to conduct a gap analysis of their existing frameworks and controls against the practices and supervisory expectations in the paper, taking into account their enterprise-level risk profile, with Board and senior management oversight of the assessment, root cause analysis, and timely remediation. Key requirements include: • **Documentation of Listing Deviations and Approvals:** Deviations from DPT listing policies, including cases where DPTs do not meet the DPTSP's risk appetite, should be documented with justifications, appropriate compliance or control function sign-off on the risk assessment and properly documented senior management approval; • **Assessment Thresholds and Criteria:** The reasons supporting DPT assessment thresholds and criteria, such as minimum market capitalisation and average daily traded volume, should be documented to facilitate periodic review and provide clarity on the risks to be mitigated; • **Enhanced Monitoring of Higher-Risk Customers**: Higher-risk customers are subject to enhanced monitoring through more frequent periodic reviews and/or enhanced transaction-monitoring rules; • **Source of Funds/Wealth Corroboration:** For source-of-funds assessments where incoming funds are DPTs, insights from blockchain analytics and/or other surveillance tools should augment or complement off-chain information. Where a customer's source of wealth is derived from virtual-asset activities, DPTSPs should understand the customer's virtual-asset exposure and obtain relevant supporting documents to corroborate the customer's virtual-asset transactions and holdings; • **Integration of Risk Frameworks and Indicators:** Customer risk frameworks should adequately consider on-chain and off-chain risk information and clearly set out the approach and risk indicators used to identify politically exposed persons and higher-risk customers, including the assessment of jurisdiction risks; • **Tailored and Role-Specific Training Programs:** Training should be tailored to staff members' functions, responsibilities and experience. Staff should be minimally equipped with a baseline understanding of blockchain technology, cryptocurrencies, the ML/TF risks arising from the DPTSP's products and services, and associated regulatory developments; and • **Committee Governance and Representation:** Relevant committees overseeing decision-making for key frameworks and controls should have balanced representation of technical DPT, AML/CFT and compliance expertise. MAS Sets Out AML/CFT Supervisory Expectations for Digital Payment Token Services Providers | MAS	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Singapore (2/4)

#	Issuing Authority	Title	Regulatory Update	Key Dates
2	**MAS**	**MAS Clarifies Financial Crime Audit Expectations for Payment Service Providers**	On 16 July 2026, the Monetary Authority of Singapore (MAS) issued the Guidelines on Audit of Payment Service Providers (PS-G04), applying to all holders of a payment service licence. The guidelines clarify supervisory expectations within the existing statutory annual audit framework, including assessment of anti-money laundering and countering the financing of terrorism (AML/CFT) controls. Key financial crime expectations include: • **Risk-based annual coverage:** Auditors should review AML/CFT controls annually, with higher-risk areas and previously identified weaknesses reviewed and tested each year. Lower-risk areas may be covered on a rotational basis. Coverage should reflect the provider's business model and emerging money laundering techniques and typologies. • **End-to-end control testing:** Newly licensed payment service providers (PSPs), and PSPs commencing newly licensed payment services, are expected to arrange an end-to-end review one year after operations or the relevant services commence, through the applicable annual audit. The review assesses control adequacy and operating effectiveness through sample testing, covering areas including risk assessment, customer due diligence, name screening, ongoing monitoring, transfer controls, suspicious transaction reporting, record-keeping and governance. • **Findings and remediation:** Findings, observations and recommendations should be documented in the auditor's management letter and submitted to MAS through Form 4. Annual audits should cover remediation of previous external audit and MAS inspection findings, and continued eligibility for any product exemptions under MAS Notice PSN01. • **Immediate escalation:** Auditors' existing statutory reporting duties include immediately notifying MAS when, during their work, they are satisfied that serious regulatory breaches or criminal offences involving fraud or dishonesty have occurred. PSPs are separately expected to notify MAS immediately of serious breaches or systemic and severe control gaps, irrespective of auditor reporting. Guidelines on Audit of Payment Service Providers [PS-G04]	Effective for annual audits with financial year ending 31 December 2026 onwards, i.e for Form 4 submissions due from 30 June 2027 onwards.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Singapore (3/4)

#	Issuing Authority	Title	Regulatory Update	Key Dates
3	MAS	**MAS Proposes Explicit Proliferation Financial Coverage in Financial Services Legislation**	On 8 September 2026, the Financial Services and Markets (Amendment) Bill 2026 (Bill No. 19/2026) was introduced for first reading in Parliament and subsequently passed by Parliament on 6 October 2026. Its financial crime provisions propose technical amendments to the Financial Services and Markets Act 2022 to align with updated Financial Action Task Force (FATF) Standards on countering proliferation financing (CPF). The proposals would: • **Clarify definitions and scope:** Define proliferation financing as financing the proliferation of weapons of mass destruction and expressly include proliferation-financing risk in the prohibition-order framework's definition of "specified risk". • **Clarify supervisory powers and cooperation:** Expressly include proliferation financing within the statutory powers of the Monetary Authority of Singapore (MAS) to impose financial crime prevention requirements and assist domestic and foreign supervisory authorities, with corresponding terminology and cross-reference updates. • **Extend an existing digital-token-provider duty**: For licensed digital token service providers, the designated representative already required to be physically present at their Singapore office must now also explicitly handle queries on countering proliferation financing (CPF), alongside existing money laundering and terrorism financing matters. MAS has clarified that financial institutions already had to mitigate proliferation-financing risks under pre-existing frameworks. These amendments make the statutory coverage more explicit. Explanatory Brief on Financial Services and Markets (Amendment) Bill 2026 | MAS	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Singapore (4/4)

#	Issuing Authority	Title	Regulatory Update	Key Dates
4	**Ministry of Home Affairs (MHA)**	**Singapore Passes Scams (Countermeasures) Bill**	On 9 September 2026, Singapore's Parliament passed the Scams (Countermeasures) and Other Matters Bill (Bill No. 16/2026), which will amend five statutes to strengthen scam detection, disruption and deterrence. The Bill introduces powers to restrict scam-enabling services and facilitates information sharing between the police and service providers, including financial institutions, telcos, payment providers and online platforms. The framework covers financial and communication services, including bank accounts, payment and digital payment token accounts, telephone lines, online accounts, credit facilities, web hosting and domain registration. Key measures include: • **Service Limitation Orders:** Require providers to restrict a named person's access to scam-enabling services for up to three years where officers suspect or have reason to believe the services will facilitate scams; • **Account Disabling Orders:** Require providers to disable accounts suspected of supporting scam-related offences for up to 30 days, extendable once for a further 30 days; • **Disclosure Orders:** Require providers to disclose compliance, account or user information where statutory conditions are met. All three order types apply regardless of where recipients or data are located; • **Protected voluntary action:** Provide statutory immunity for qualifying information disclosures made in good faith and with reasonable care. Providers may also voluntarily restrict accounts for up to 30 days where suspicions are based at least partly on information from existing disabling or disclosure orders; and • **Stronger online enforcement:** Allow specified Online Criminal Harms Act directions based on computer-program assessments, subject to responsible-officer authorisation, and strengthen penalties for non-compliance. Administrative penalties for breaches of OCHA codes of practice will rise from S$1 million to S$10 million per instance. A new compliance-order mechanism will address breaches of implementation directives, while failure to comply with a compliance order will attract criminal fines of up to S$10 million, plus up to S$300,000 daily for continuing offences. Scams (Countermeasures) and Other Matters Bill	The Act received presidential assent on 24 September 2026 and will take effect on a date appointed by the Minister through notification in the Gazette.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Taiwan (China)



Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Taiwan (China) (1/3)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	**Executive Yuan**	**Taiwan's Virtual Asset Services Act Strengthens Measures Against Fraud and Market Manipulation**	On 30 June 2026, Taiwan's Legislative Yuan passed the Virtual Asset Services Act, broadening oversight of virtual asset service providers (VASPs) beyond the existing AML registration framework. For financial crime compliance, the key development is the Act's prohibition of fraudulent, deceptive and price manipulation activities, with violations potentially attracting imprisonment of three to ten years and fines of NTD 10 million to NTD 200 million. The Act also establishes licensing and internal control requirements for VASPs, supporting greater accountability for their operations. Existing AML-registered operators will need to transition to the licensing regime within the prescribed periods following commencement. The FSC will develop implementing regulations and consult stakeholders. Taiwan Promulgates the Virtual Asset Services Act Establishing a Licensing Regime for Virtual Asset Service Providers | Executive Yuan	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Taiwan (China) (2/3)

#	Issuing Authority	Title	Regulatory Update	Key Dates
2	**FSC**	**Explanatory Notes to the Amendments to the Anti-Fraud Compliance Regulations for Financial Institutions and Virtual Asset Service Providers (VASPs)**	On 20 July 2026, FSC amended the Regulations Governing Compliance by Financial Institutions and Virtual Asset Service Providers for the Prevention of Fraud Crime. These amendments align the regulatory framework with broader anti-fraud legislation passed earlier in the year. The amended rules apply to deposit-taking institutions, electronic payment institutions, credit card institutions, and VASPs and took effect on issuance. The update comprehensively revises existing rules and introduced cross-sector inquiries, a cross-institution anti-fraud platform, cross-sector joint-defence notification, and rules on refunding victims. Key changes include: • **Definitions:** the anti-fraud platform and its participating institutions are defined, and the definition of a virtual asset account is clarified (Article 2); • **Warning signs:** the criteria for identifying suspected fraud accounts and credit cards now cover foreign holders whose residence permits were cancelled before expiry, who have overstayed or whose whereabouts are reported unknown, and holders reported as missing persons; accounts listed by judicial police as suspected domestic fraud accounts are also covered, except for credit cards (Articles 3, 6, 9 and 12); • **Cross-sector inquiries:** an institution in any of the four sectors may ask an institution in another sector about a suspected fraud account by phone, email, the anti-fraud platform or another accepted method, and the institution asked must provide specified information within five business days, extendable only by agreement where there is practical difficulty (Articles 5, 8, 11 and 14); • **Records:** all inquiry records must be kept, not only those from same-sector inquiries (Articles 15, 18, 21 and 24); • **Joint defence:** deposit-taking institutions, electronic payment institutions and VASPs must follow a cross-sector joint-defence notification mechanism (Articles 27, 28 and 30, among others); • **Refunds:** any judicial police agency, not only the one that originally reported the account, may instruct a refund of remaining funds or virtual assets, and victims may apply with a case-acceptance certificate or other document issued by a judicial police agency (Articles 52 to 67); • **Virtual assets:** VASPs may sell the remaining virtual assets in a warned account and refund the proceeds (Article 64); and • **Anti-fraud platform:** the documents needed for FSC approval, the uses participating institutions may make of the platform and the scope of customer data it may collect are prescribed, and platforms set up after being reported to FSC before 20 July 2026 are deemed approved (Articles 70 to 72). FSC Amends Fraud Prevention Rules to Add Cross-Sector Inquiries and an Anti-Fraud Platform | FSC Explanatory Statement and Comparison Table for the Amendment to the Fraud Prevention Regulations for Financial Institutions and Virtual Asset Service Providers | FSC	Effective on 20 July 2026.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Taiwan (China) (3/3)

#	Issuing Authority	Title	Regulatory Update	Key Dates
3	FSC	**FSC Amends Deposit Account Regulations to Expand Class 2 Account Criteria and Align with the Fraud Prevention Framework**	On 31 August 2026, FSC amended its rules on bank deposit accounts and suspicious or unusual transactions to strengthen early warning of accounts misused for crime. As the first major update to these rules since August 2014, the amendment aligns with rules with Article 8 to 11 of the Fraud Crime Hazard Prevention Act and its sub-regulations, and draws on law enforcement experience and banks' practical suggestions. To bolster early-stage fraud prevention, the updated rules expand the criteria for flagging suspicious accounts and grant banks the authority to restrict transactions when suspicious activity is suspected, without waiting for illegal conduct to be legally verified. The update also removes redundant transaction-tracing rules that are now covered by broader cross-sector fraud-prevention frameworks. Alongside these amendments, the FSC officially designated the Joint Credit Information Center (JCIC) as the central hub for tracking restricted accounts, meaning financial institutions must report when a watch-list warning is issued, extended, or lifted. Key changes include: • **Article 4:** Five additional Class 2 account criteria are introduced, covering accounts held by non-Taiwanese nationals with cancelled, overstayed, or missing status, as well as accounts sharing a registered mobile number with an existing warning account where criminal abuse is suspected. Additionally, the criteria now include repeatedly flagged virtual accounts, customers reported as missing persons, and domestic financial accounts identified by judicial police as suspected of fraud; • **Articles 5 and 10:** For over-the-counter withdrawals, transfers, or outward remittances from derivative controlled accounts, banks may require transaction-related supporting information and may refuse the transaction if no reasonable explanation is provided. Where a Class 2 account presents a risk of unlawful or manifestly unusual transactions, a bank may notify the judicial police authorities and take some or all of the measures applicable to Class 1 accounts; in serious or urgent cases, it may also notify the Taiwan High Prosecutors Office. This replaces the previous requirement that unlawful conduct first be verified. In addition, notifications concerning the reporting, release, or continued designation of warning accounts must be made to an institution designated by the FSC, replacing the fixed reference to the JCIC; • **Article 7:** The provisions governing transaction tracing and interbank notifications where funds have been transferred onward from a warning account are deleted; • **Article 9:** The transitional provisions governing warning accounts reported before 1 January 2015 are deleted because the applicable warning periods have expired; and • **Article 11:** Subject to the conditions specified in Article 11, the existing residual-funds return procedure continues to apply to accounts reported as warning accounts on or before 31 March 2025. Accounts reported on or after 1 April 2025 are governed by the applicable fraud-prevention compliance regulations. FSC Amends Deposit Account Rules to Widen Suspicious-Account Triggers and Align Them with the Fraud Prevention Framework | FSC Explanatory Statement and Article Comparison Table for the Amendment to the Regulations Governing the Deposit Accounts and Suspicious or Unusual Transactions | FSC Financial Institutions Receiving Reports, Releases, or Extensions of Warning Accounts | FSC	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Thailand



Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Thailand (1/4)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	BOT	**BOT Consults on Extending Cash Transaction Risk Management Rules to Cash Deposits and Money Exchange**	On 5 August 2026, BOT published a consultation paper on revising its risk management rules for cash-related transactions, with a draft notification that would apply to all financial institutions and specialised financial institutions (SFIs) and repeal BOT Notification No. 16/2569 dated 18 March 2026. BOT noted that the existing rules focus on cash and uncrossed-cheque withdrawals. The draft would extend the definition of cash-related transactions to cash deposits, deposits by cheque and funds received from the public outside deposit accounts, and to money exchange, namely the exchange of baht banknotes (excluding damaged banknotes), the receipt of cash to issue cheques and drafts, and the purchase, sale or exchange of foreign banknotes. Institutions would be required to have customers or their authorised representatives identify or verify themselves before every cash-related transaction (for baht banknote exchange, only from THB 5 million per transaction), and to encourage customers making high-value cash transactions to use safer, traceable methods first. Where a transaction is unusual, or a customer's cash-related transactions reach THB 5 million or equivalent in one day, institutions would have to obtain the purpose of a withdrawal, the source of funds for a deposit, and both for money exchange. Transactions showing inconsistency, unreasonableness or grounds for suspicion would be classed as high risk and subject to enhanced customer due diligence (EDD). For legal-entity customers engaged in foreign banknote exchange, real estate, gems, gold and precious metals, or high-value luxury goods, institutions would additionally request, in specified circumstances, the source of funds of the persons whose transactions generated the cash. Where EDD cannot be completed, a transaction could proceed if the customer shows appropriate reasons or necessity and an executive above branch manager level approves it; otherwise it would be declined and reported to the Anti-Money Laundering Office, and reconsidered only once the institution's set period for awaiting its orders has passed. Public consultation on revisions to the risk management rules for cash-related transactions | BOT	Public consultation ended on 3 September 2026; Proposed to take effect on 15 October 2026, with additional source-of-funds requirements for specified legal-entity customers proposed to take effect on 15 April 2027.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Thailand (2/4)

#	Issuing Authority	Title	Regulatory Update	Key Dates
2	**SEC**	**SEC Proposes Securities Ownership Reporting and Transaction Suspension Powers**	On 11 September 2026, the Securities and Exchange Commission (SEC) published a consultation on draft amendments to the Securities and Exchange Act B.E. 2535 (1992). Two proposals are particularly relevant to market integrity: • **Beneficial ownership reporting** (proposed sections 194/2–194/4). Certain foreign service providers, including brokers using pooled client accounts and intermediaries holding securities for others, would report information on the ultimate beneficial owners of securities to the SEC under rules set by the Capital Market Supervisory Board. Corporate clients that are not the ultimate owners would have to provide the owners' names to their provider on request. This could help the SEC identify who is behind pooled holdings when examining suspected market abuse. For banking groups, the proposal is primarily relevant to in-scope brokerage and custody businesses. • **Temporary suspension of transactions** (proposed section 266/4). With SEC Board approval, the SEC could temporarily suspend, by written order, transactions entered into or proposed by listed companies, securities firms or other entities specified by ministerial regulation. The power would apply to transactions that could take advantage of investors or cause serious harm to investors or the public interest. The initial suspension could last up to 60 working days, with a court extension possible. SEC Consults on Draft Securities and Exchange Act Amendments on Short Selling, Beneficial Ownership Reporting, Share Encumbrances and Transaction Suspension Powers | SEC Draft Act amending the Securities and Exchange Act B.E. 2535 | SEC	Public consultation ended on 13 October 2026.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Thailand (3/4)

#	Issuing Authority	Title	Regulatory Update	Key Dates
3	**BOT**	**BOT Consults on Draft Security Guideline for Facial Recognition Used to Verify or Authenticate Financial Service Users**	On 14 September 2026, BOT opened a public consultation on a draft BOT Guideline on the Security of Biometric Technology of the Facial Recognition Type for Verifying or Authenticating Service Users. BOT stated that threats targeting facial recognition are becoming more sophisticated, particularly presentation attacks using AI deepfakes, which raise the risk of impersonation for unauthorised transactions. The draft would repeal the Guideline on the Use of Biometric Technology in Financial Services issued under BOT Circular No. Thor Por Thor. For Nor Chor. (09) Wor. 689/2566 dated 29 September 2023. It would apply to BOT-supervised providers that use facial recognition through mobile applications: financial institutions, specialised financial institutions, regulated payment service providers, and regulated personal loan and nano finance operators. Providers would be required to secure facial recognition systems, presentation attack detection (PAD) systems and biometric data across face data capture, signal processing, storage, face comparison and decision. Key proposals include: • **Vulnerability assessments at least every three months and penetration tests at least annually**, and on any significant change, with penetration tests covering at least presentation attacks, video injection attacks and attacks through APIs; • **Event logs retained for at least 90 days**, or as required by law, and protected against unauthorised alteration or destruction; • **Verification refused on detection of a rooted or jailbroken device**, an emulated environment, application tampering, a face image below the provider's quality criteria or a presentation attack; • **Face data, biometric references and other personal data stored separately** with at least logical separation, biometric data encrypted at rest and in transit and accessed with multi-factor authentication, and third-party providers not permitted to retain users' face data unless required by law; • A False Match Rate (FMR) of no more than 0.01% and an Impostor Attack Presentation Accept Rate (IAPAR) of no more than 4% for each type of attack instrument; • **Performance tests under the annexed frameworks at least annually and on any significant change**, using at least 300,000 test transactions and 776 test subjects for a target FMR of 0.01%, and PAD tests that include deepfake and live-stream video shown on a monitor of at least 3,840 × 2,160 pixels; and • **Prior consultation with BOT before using other biometric types**, such as iris or fingerprint recognition, or facial recognition for other purposes. Providers already using the technology would be required to complete the performance tests and a compliance assessment by internal audit or an independent external auditor, and report the results to BOT within 90 days from the day after the guideline is issued. Results obtained under the existing guideline could be reported if they are no more than one year old and consistent with the new requirements. Annual tests in later years would not need to be reported unless BOT requires it, and reporting under the existing biometric report form would cease from the day after issuance. Public consultation: (draft) guideline on the security of biometric technology of the facial recognition type for verifying or authenticating service users | BOT	Public consultation ended on 13 October 2026.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Thailand (4/4)

#	Issuing Authority	Title	Regulatory Update	Key Dates
4	SEC	**SEC Introduces Travel Rule for Digital-asset Transfers**	Thailand's Securities and Exchange Commission (SEC) announced the adoption of its digital-asset Travel Rule on 2 September 2026, following the issuance of Notification No. SorThor. 9/2569 on 25 August 2026. Effective from 27 February 2027, the rules require regulated digital-asset businesses to collect and exchange information about transfer originators and beneficiaries to strengthen transaction traceability and combat money laundering, terrorist financing and technology-related crime. The requirements cover transfers of all values, with additional information and wallet verification requirements for transactions exceeding THB 30,000. Operators must establish policies and procedures to assess risks involving customers, counterparties, other service providers, intermediaries and self-hosted wallets. Key requirements include: • **Transfer information:** Collect recipient identification information for every transfer. Transfers exceeding THB 30,000 also require the recipient's province or city, country and, for legal entities, registration number; • **Self-hosted wallets:** Verify ownership or control where a transfer exceeding THB 30,000 involves a self-hosted wallet; • **Information exchange:** Send originator and beneficiary information alongside the transfer instruction to the receiving operator; and • **Record retention:** Retain transfer information for at least five years in a form accessible to regulatory authorities. The rules apply specifically to digital-asset transfers and do not affect trading on an operator's platform, Thai baht transfers or Thai baht withdrawals. The implementation period gives operators time to develop information-sharing and transaction-verification systems, while additional checks may lengthen processing where information is incomplete or wallet verification is required. SEC Issues Travel Rules for Digital Assets Enhancing the prevention of money laundering and technological crimes in line with international standards | SEC	Effective 27 February 2027

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Vietnam



Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Vietnam (1/5)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	**Government**	**Government Issues Administrative Penalties for Violations in the Pilot Crypto-Asset Market**	On 16 July 2026, the State Council issued Decree No. 284/2026/ND-CP on administrative penalties for violations relating to crypto assets and the crypto-asset market under the pilot established by Resolution No. 05/2025/NQ-CP of 9 September 2025 (Resolution 05). The Decree applies to Vietnamese and foreign organisations and individuals, including crypto-asset issuers, service providers and pilot investors. It covers offering and issuance, market organisation, service-provider duties, trading, foreign investor remittances, unlawful handling of account data, obstruction of inspections, and anti-money laundering (AML), counter-terrorist financing (CFT) and counter-proliferation financing (CPF) duties. Sanctions are a warning or a fine, capped at VND 200 million for organisations and VND 100 million for individuals; the tiers are set for organisations, and individuals pay half. Additional sanctions are deprivation of the right to use the market-organising service licence for 1 to 3 months, suspension of offering and issuance for 1 to 12 months, of service provision for 1 to 6 months and of trading for 1 to 12 months, and confiscation. Remedial measures include correcting information, disgorging unlawful gains, removing websites and trading systems, and cancelling offerings with full refunds. Highlights of the fine tiers for organisations include: • **Offering and issuance:** VND 70–100 million for breaching foreign ownership rules on underlying assets; VND 100–150 million for inaccurate, incomplete or untimely information; VND 150–200 million for offering to ineligible persons, offering without meeting Resolution 05 conditions, or failing to publish or follow the prospectus; • **Market organisation:** VND 70–100 million for failing to announce the official service start date within 7 working days of licensing; VND 150–180 million for failing to file licence adjustments or operating outside the licence; VND 180–200 million for providing services or advertising without a market-organising licence; • **Service providers:** VND 30–50 million for failing to publish required procedures, audited financial statements or fee schedules; VND 50–70 million for failing to verify investor identity; VND 100–150 million for failing to segregate client funds and assets or to monitor trading; VND 150–200 million for failures on prospectus accuracy, information technology security and client-asset protection; and VND 50–70 million (under 15 days late) or VND 70–100 million (15 days or more late) for late information disclosure; • **Trading:** VND 30–50 million for domestic investors trading outside licensed service providers; VND 70–100 million for domestic investors trading assets offered to foreign investors; • **Foreign investor remittances:** VND 30–50 million for foreign investors breaching account opening, closing and use rules; VND 70–100 million for inauthentic dossiers or untruthful declarations; for authorised banks, VND 50–70 million for reporting dedicated-account activity under 15 days late, and VND 70–100 million for reporting 15 days or more late, failing to check and keep transaction documents, or failing to issue internal rules; • **Account data and inspections:** VND 150–200 million for unlawfully collecting, trading or disclosing crypto-asset account data; VND 50–150 million for obstructing inspections; and • **AML/CFT/CPF:** VND 80–200 million, including VND 100–120 million for customer due diligence and risk-assessment failures, VND 150–200 million for failing to report suspicious or required large-value transactions or to issue internal rules, and VND 170–200 million for failing to delay transactions or freeze accounts and assets where required. Penalising authority sits with office-holders of the State Securities Commission, SBV, the Ministry of Public Security and provincial People's Committees, with fining powers of up to VND 100 million, VND 160 million or VND 200 million for organisations depending on the office; SBV office-holders may penalise only violations relating to foreign investor remittances, account data, obstruction of inspections and AML/CFT/CPF duties. Decree No. 284/2026/NĐ-CP on administrative penalties for violations related to crypto assets and the crypto asset market | Government	Effective on 1 September 2026.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Vietnam (2/5)

#	Issuing Authority	Title	Regulatory Update	Key Dates
2	**SBV**	**SBV Proposes Amendments to Customer Due Diligence and Suspicious Transaction Reporting Rules for Anti-Money Laundering Reporting Entities**	On 17 August 2026, SBV published a draft circular amending Circular No. 27/2025/TT-NHNN of 15 September 2025, which guides the Law on Anti-Money Laundering (AML Law). The draft would apply to reporting entities under the AML Law. It would set customer due diligence (CDD) update frequencies by risk tier, realign suspicious transaction reporting with the draft amended Article 26 of the AML Law, and replace the seven suspicious transaction report forms. The accompanying comparison table states that several CDD provisions carry over Government Resolution No. 66.23/2026/NQ-CP of 24 July 2026. The update frequencies address a gap under criterion 10.7 of Financial Action Task Force (FATF) Recommendation 10, rated "partially met", and Organisation for Economic Co-operation and Development (OECD) commitments on beneficial ownership updates. Key proposals include: • **Customer risk classification** (low, medium or high) would be carried out immediately or within 10 working days of the customer being identified; • **CDD information** would be updated at least every 5 years for low-risk customers, every 2 years for medium-risk customers and every year for high-risk customers, with updates also triggered by a new risk or a known change in customer information, replacing wording that sets low-risk frequency as "reduced" and high-risk frequency as "increased" relative to medium-risk customers; • **Reduced measures for low-risk customers would not apply where money laundering, terrorist financing or proliferation financing is suspected**, or where the customer matches a high-risk scenario defined by the reporting entity, in which case enhanced CDD would be required; • The **beneficiary of a life insurance policy would become a factor in deciding on enhanced CDD**, including identifying and verifying the beneficial owner of a high-risk legal-person or legal-arrangement beneficiary at the time of payout; • The **internal-rules provisions** in Article 5 would be cut back to founder information for organisational customers, ongoing risk-based monitoring, and the timing of verification and review. The provisions on when CDD applies (including the VND 400 million single-day threshold for customers without an active account), verification, legal representatives and legal arrangements would be removed because, according to the explanation, they have moved to a draft decree amending Decree No. 19/2023/ND-CP; • Depending on their scale, scope and nature of operations**, reporting entities would be required to set up a dedicated unit, or designate a unit or person, responsible for AML at their head office** or, for reporting entities with a foreign parent, at their Vietnam office. They would register the details of the responsible person and unit with the Anti-Money Laundering Department and the relevant sector ministry, and the entities issuing a limited set of internal rules would extend from individuals and micro-enterprises to equivalent-sized trade and service organisations; • **Suspicious transaction reports** would be required where there are reasonable grounds to suspect that assets in a transaction are proceeds of crime or relate to terrorist or proliferation financing, replacing the current trigger of detecting a suspicious transaction related to money laundering, other money-laundering-related crime, terrorist financing or proliferation financing; and • Transaction type "C" in the Appendix II guidance on large-value transaction reports would drop cash transactions under economic contracts notarised, prepared or carried out by the reporting entity on a customer's behalf. Draft documents guiding the Law on Anti-Money Laundering | SBV	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Vietnam (3/5)

#	Issuing Authority	Title	Regulatory Update	Key Dates
3	SBV	**SBV Publishes Draft Decree Amending Customer Identification Triggers and Beneficial Owner Criteria Under the Anti-Money Laundering Implementing Decree**	On 17 August 2026, SBV published on its website a draft Government Decree amending Decree No. 19/2023/NĐ-CP of 28 April 2023, which details the Law on Anti-Money Laundering (AML), together with an explanation table. The explanation table cites gaps identified under Financial Action Task Force (FATF) Recommendations 10 (customer due diligence) and 15 (new technologies) and in the OECD Global Forum peer review on exchange of information on request for tax purposes, and states that the Article 7 amendments inherit the corresponding provisions of Government Resolution No. 66.23/2026/NQ-CP of 24 July 2026. Article 1 of the draft would amend Article 6 on customer identification. Key proposals include: • The daily threshold of VND 400 million for customers with no account, or none active for 6 continuous months, would remain, but would apply to one or several deposits, withdrawals or transfers, would exclude the crypto asset transactions covered by the new trigger, and would extend the existing exclusion for registered periodic payments to those made on a registered term or date; • A new trigger would require identification when a customer with no crypto asset account or wallet, or none active for 6 continuous months, conducts one or several crypto asset transactions worth USD 1,000 or more in a day; • Identification would also be triggered by incomplete transactions, including those a customer abandons when identification or a query on purpose is carried out; by signs under Articles 27 to 31 and 33a of the AML Law (currently Articles 27 to 31); and by changes to information on a legal arrangement; • Reporting entities would be allowed to refuse to open accounts, establish relationships, execute transactions or terminate relationships where a customer cannot be identified because the customer refuses to provide information or provides incomplete information, or where there is doubt about the accuracy of the identification information provided; • For low-risk customers, verification could be completed after products or services are provided, within 10 working days, under conditions set in the risk management process; and • Where money laundering is suspected and continuing identification would tip off the customer, reporting entities could stop identification and would consider filing a suspicious transaction report under Article 26 of the AML Law. Article 2 would replace Article 7 on beneficial owners. For organisations, the 25% test would apply to charter capital or total voting shares (currently charter capital), held directly, indirectly or combined, including by groups of persons related through personal relationships or contracts, with each ownership layer reviewed. Where no one meets that test or doubt exists, the beneficial owner would be the individual controlling the customer by other legal or de facto means; failing that, the senior manager with the greatest authority to act for the organisation, excluding state capital representatives (currently at least one legal representative). Separate rules would cover foreign-law funds, trusts and similar legal arrangements, listed companies whose beneficial owner information is published and accessible to the reporting entity, and life insurance. The draft leaves its effective date blank, within 2026. Draft documents guiding the Law on Anti-Money Laundering | SBV	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Vietnam (4/5)

#	Issuing Authority	Title	Regulatory Update	Key Dates
4	**National Assembly**	**National Assembly Enacts Law No. 23/2026/QH16 on Financial and AML Reforms**	On 24 August 2026, Law No. 23/2026/QH16 was officially passed by the National Assembly. The omnibus statute formally amends and supplements the Law on the State Bank of Vietnam No. 46/2010/QH12, the Law on Anti-Money Laundering No. 14/2022/QH15, and the Law on Credit Institutions No. 32/2024/QH15. Key Amendments under Law No. 23/2026/QH16 are: • **Foreign exchange management:** Reinforces restrictions on using foreign currencies for transactions, pricing, advertising, and contracts in Vietnam, except where legally permitted. • **Enhanced KYC requirements:** Expands customer information requirements, particularly for beneficial owners, trusts, and similar legal arrangements. • Life insurance beneficiaries: Requires beneficiary information to be collected upon designation and verified before insurance payouts. • **New products and technologies:** Requires money-laundering risk assessments before launching new or technology-enabled products and services. • **Suspicious transaction reporting:** Strengthens reporting obligations and expands indicators used to identify potentially suspicious transactions. • **Crypto-asset activities:** Brings crypto-asset services explicitly within the AML framework and introduces dedicated suspicious transaction indicators. • **Governance and supervision:** Enhances record-keeping obligations and clarifies AML responsibilities among reporting entities and competent authorities. • **Institutional financial regimes:** Shifts the authority to regulate the State Bank of Vietnam's financial framework from the Prime Minister to the Government. • **Business identity alignment:** Standardizes organization identification terminology (such as "business location") to align directly with the Enterprise Law 2020. Law No. 23/2026/QH16 of the National Assembly: Law on Amending and Supplementing a Number of Articles of the Law on the State Bank of Vietnam, the Law on Anti-Money Laundering, and the Law on Credit Institutions | National Assembly	Effective on 1 December 2026

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Vietnam (5/5)

#	Issuing Authority	Title	Regulatory Update	Key Dates
5	SBV	**SBV Proposes Procedures for Risk-Based Supervision of Anti-Money Laundering Activities in the Banking Sector**	On 21 September 2026, SBV published the dossier for a draft circular, dated 11 September 2026, that would regulate the sequence and procedures for the SBV to supervise anti-money laundering (AML) activities of reporting entities under the Law on Anti-Money Laundering (AML Law) that fall under its state management of money and banking operations. The SBV's explanatory note states that the draft is based on Article 48(3) of the AML Law and responds to the 2019 mutual evaluation by the Asia/Pacific Group on Money Laundering and Vietnam's placement on the Financial Action Task Force grey list in June 2023, citing the absence of a supervisory legal framework and of remote supervision. It also follows Government Resolution No. 71/NQ-CP of 15 May 2024 and SBV Decision No. 2853/QD-NHNN of 21 July 2025, which sets a completion date of December 2026. Under the draft, the supervising unit, which the draft identifies as the Anti-Money Laundering Department, would follow three steps: collecting and processing data, carrying out compliance and/or risk-based supervision, and preparing a supervision report proposing handling measures. Compliance supervision would cover reporting duties under Articles 15, 25, 26, 34, 36 and 37 of the AML Law, internal rules under Article 24, and directions of competent authorities. Risk-based supervision would score and classify supervised entities as low, medium or high risk using a methodology approved by the Governor, drawing on structural, inherent (customer, product, delivery channel and geographic) and control indicators. Annex 01 would require supervised entities to report: • Organisational, customer, product, delivery channel and geographic data by 15 October each year; • Examination and inspection conclusions and the status of follow-up recommendations by 15 September each year; and • Statistics on suspicious transaction, large-value transaction and electronic fund transfer reports, crime-related customers and transactions, and enforcement cases by 15 July and 15 January each year. Supervised entities would be required to respond to written explanation requests within the deadline set in the request and to attend meetings on at least 3 working days' written notice. Handling measures would include recommendations, warnings, administrative penalties and proposals for inspection. High-risk entities would face enhanced measures such as additional controls, more resources and technology, more frequent internal control and remote-supervision reporting, and remediation plans, while low-risk entities could face less frequent inspection and contact without relief from AML obligations. The supervising unit would complete an annual supervision report by 31 January of the following year. Draft Circular dossier on monitoring anti-money laundering activities | SBV	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

ASIA PACIFIC CENTRE FOR REGULATORY STRATEGY (ACRS)

ACRS Co-leads



Nai Seng Wong
Partner, SEA
ACRS Chair
SEA Regulatory Strategy Lead



Shinya Kobayashi
Partner, Japan
JP Insurance Sector Leader



Sean Moore
Partner, Australia
AU SR&T FS Industry Lead



Lakshmi Narasimhan
Partner, India
India SR&T



Xu Du
Director, China
China SR&T

ACRS Core-team



Nicola Sergeant
Managing Director
Operations Lead
JP SR&T



Edwin Goh
Manager
Coordinator
SEA SR&T



Nusaybah Maszlee
Consultant
SEA SR&T

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Acknowledgements

Australia

Tony Zhi-Wei Tang
Associate Director
Deloitte Australia



Eric Kanikevich
Senior Consultant
Deloitte Australia



China Mainland

Cheryl Fan Jia
Manager
Deloitte China



Hong Kong SAR

Adelide Yeung
Partner
Deloitte China



Gianfran Liu
Partner
Deloitte China



Indonesia

Robertus Indrakrishna
Partner
Deloitte Indonesia



David Christian Hidayat
Director
Deloitte Indonesia



India

Satya Mahapatra
Partner
Deloitte India



Japan

Shoya Kusuda
Senior Consultant
Deloitte Japan



Malaysia

Prakash Arikrishnan
Partner
Deloitte Malaysia



Wai Theng Ha
Senior Manager
Deloitte Malaysia



Philippines

Herbert Rollom
Director
Deloitte Philippines



Anna Avila
Manager
Deloitte Philippines



New Zealand

Catherine Law
Partner
Deloitte New Zealand



Singapore

Samuel Yue Xuan Ang
Consultant
Deloitte Singapore



Taiwan (China)

Kelly Liu
Partner
Deloitte Taiwan



Chien Wang
Manager
Deloitte Taiwan



Thailand

Narumol Jirapanich
Partner
Deloitte Thailand



Boonsom Jarusiritarangkul
Partner
Deloitte Thailand



Vietnam

Tho Nguyen
Partner
Deloitte Vietnam



Quoc Anh Luu
Senior Manager
Deloitte Vietnam



Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Appendix

Other Q3 2026 Regulatory Updates

Australia (1/1)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	**AUSTRAC**	**AUSTRAC Releases 2026 Intelligence Suite on Money Laundering, Terrorism Financing and Proliferation Financing**	On 30 June 2026, AUSTRAC released its annual 2026 intelligence suite of four threat assessments covering money laundering, terrorism financing, proliferation financing and terrorism financing risks in the non-profit organisation sector. AUSTRAC Releases 2026 Intelligence Suite on Money Laundering, Terrorism Financing and Proliferation Financing | AUSTRAC	-
2	**AUSTRAC**	**AUSTRAC Launches Redesigned Threshold Transaction Report and Suspicious Matter Report Forms in AUSTRAC Online**	On 30 June 2026, AUSTRAC announced the launch, effective 1 July 2026, of redesigned threshold transaction report and suspicious matter report submission forms in AUSTRAC Online, which change the submission workflow but leave reporting obligations under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 unchanged. AUSTRAC Launches Redesigned Threshold Transaction Report and Suspicious Matter Report Forms in AUSTRAC Online | AUSTRAC	Effective on 1 July 2026.
3	**AFCA**	**AFCA Commences as Authorised External Dispute Resolution Scheme for SPF Scam Complaints From 1 July 2026**	Effective 1 July 2026, AFCA was formally authorised as the external dispute resolution scheme for scam-related complaints under the Scams Prevention Framework (SPF), granting it the legislative power to begin building the scheme and rules. Detailed compliance obligations will be set out in sector-specific codes. While authorisation commenced in July 2026, the overall framework will officially go live and AFCA will begin receiving and resolving escalated consumer scam complaints on 31 March 2027. AFCA Commences as Authorised External Dispute Resolution Scheme for SPF Scam Complaints From 1 July 2026 | AFCA	Sector-specific codes to be finalised before 1 September 2026.
4	**AUSTRAC**	**AUSTRAC Travel Rule Takes Effect for Virtual Asset Transfers**	Effective 1 July 2026, the Travel Rule covers eligible domestic and cross-border transfers with no minimum transfer amount. Institutions must check wallets and collect, verify and share prescribed information as applicable. Transfers to self-hosted wallets are exempt from onward messaging. Reporting begins for transfers involving unverified self-hosted wallets on 31 March 2029. AML/CTF transitional rules 2026 | AUSTRAC	Effective on 1 July 2026.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Hong Kong SAR (1/1)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	**SFC**	**SFC Circulates FATF High-Risk Jurisdiction Statements and June Plenary Outcomes to Intermediaries**	On 14 July 2026, SFC issued anti-money laundering and counter-financing of terrorism circular SFO/IS/025/2026 to licensed corporations, SFC-licensed virtual asset service providers and associated entities, relaying the FATF statements of 19 June 2026 on high-risk jurisdictions and the outcomes of the FATF Plenary of 17 to 19 June 2026. SFC Circulates FATF High-Risk Jurisdiction Statements and June Plenary Outcomes to Intermediaries | SFC	FATF public consultation on the Recommendation 16 guidance closed on 21 August 2026; and FATF to consider countermeasures against Myanmar if no further progress is made by October 2026.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

India (1/1)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	**RBI**	**RBI Consolidates Fraud Risk Management and Supervisory Returns Requirements into Entity-Specific Master Directions**	On 31 July 2026, RBI issued Fraud Risk Management Directions and Supervisory Returns Directions as part of its 64 Consolidated Supervisory Directions, carrying forward existing Department of Supervision instructions without substantive change. Reserve Bank of India issues Consolidated Supervisory Directions | RBI Reserve Bank of India (Commercial Banks – Fraud Risk Management) Directions, 2026 | RBI Reserve Bank of India (Commercial Banks – Supervisory Returns) Directions, 2026 | RBI	-

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Indonesia (1/1)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	OJK	**OJK Issues AML, CFT and Counter-Proliferation Financing Guidelines for Trustees**	On 7 July 2026, OJK issued Regulation of the Member of the Board of Commissioners (PADK) No. 4 of 2026, effective on issuance, setting guidelines under OJK Regulation (POJK) No. 8 of 2023 for the implementation of anti-money laundering, counter-terrorism financing and counter-proliferation financing programmes by trustees (wali amanat), covering due diligence, monitoring, record-keeping and reporting, and standardising the format of their implementation reports. OJK Issues AML, CFT and Counter-Proliferation Financing Guidelines for Trustees | OJK	AML/CFT questionnaire provisions effective from the 2027 reporting period.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Vietnam (1/1)

#	Issuing Authority	Title	Regulatory Update	Key Dates
1	**SBV**	**SBV Consults on Draft Circular Setting Transfer and Retention Rules for Customer Account and Anti-Money Laundering Records**	On 16 July 2026, SBV opened a public consultation, with a comment period of 3 days from publication, on a draft circular amending Circular No. 04/2025/TT-NHNN that would set a 10-year retention period for customer payment-account transaction records and require dissolving or bankrupt credit institutions and foreign bank branches to transfer payment-account and anti-money laundering (AML) customer identification records to SBV's archive. Seeking comments on the draft Circular amending and supplementing a number of articles of Circular No. 04/2025/TT-NHNN dated 15 May 2025 of SBV on retention periods for records and documents in the banking sector | SBV	-
2	**SBV**	**SBV Proposes Government Resolution on Special Mechanisms to Amend Beneficial Ownership and Customer Due Diligence Rules**	On 20 July 2026, SBV sent a draft Government Resolution on special mechanisms to remove difficulties in anti-money laundering (AML) law to the Ministry of Justice for appraisal and posted it for wide consultation, proposing a new definition of beneficial owner, a 25% charter capital or voting share threshold for identifying beneficial owners and tighter customer risk classification and update requirements ahead of Vietnam's in-depth review request to the Organisation for Economic Co-operation and Development (OECD) Global Forum. Draft Resolution dossier: Government Resolution promulgating specific mechanisms and policies to remove difficulties in anti-money laundering law to meet the urgent requirements of international commitments on exchange of information on request for tax purposes | SBV	Global Forum in-depth review request due on 24 July 2026.

Introduction
Summary
Australia
China Mainland
Hong Kong SAR
India
Indonesia
Japan
Malaysia
New Zealand
Philippines
Singapore
Taiwan (China)
Thailand
Vietnam
Contacts
Appendix

Deloitte.

The Deloitte Centre for Regulatory Strategy is a source of critical insights and advice, designed to assist the world's largest financial institutions manage the strategic and aggregate impact of regional and international regulatory policy. With regional hubs in Asia Pacific, the Americas and EMEA, the Centre combines the strength of Deloitte's network of experienced risk, regulatory, and industry professionals — including a deep roster of former regulators, industry specialists, and business advisers — with a rich understanding of the impact of regulations on business models and strategy.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organisation"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the "Deloitte organisation") serves four out of five Fortune Global 500® companies. Learn how Deloitte's approximately 415,000 people make an impact that matters at www.deloitte.com.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Bengaluru, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Mumbai, New Delhi, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

This communication contains general information only, and none of DTTL, or the Deloitte organisation is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

Liability limited by a scheme approved under Professional Standards Legislation.

Member of Deloitte Asia Pacific Limited and the Deloitte organisation.

© 2026 Deloitte Touche Tohmatsu
Designed by CoRe Creative Services. RITM2672151