



Identomat

COMPLIANCE GUIDE

Crypto & Virtual Assets Compliance in Singapore

COUNTRY **Singapore**

INDUSTRY **Crypto & Virtual Assets**

LAST UPDATED **28 October 2026**

KEY REGULATORS **Monetary Authority of Singapore · Suspicious Transaction Reporting Office**

Key takeaways

- Running a crypto exchange, broker, custody or transfer service for customers in Singapore requires a licence from the Monetary Authority of Singapore (MAS). A Singapore business that serves only customers abroad needs a separate licence that MAS says it will generally not grant.
- Every customer must be identified and verified before the account is opened. Short delays are tolerated only under controls, and simplified checks are not allowed once a customer's transactions exceed S\$20,000 in a year.
- Fully online onboarding is allowed, but it must be at least as strong as meeting the customer in person, include checks against impersonation, and be assessed by an external auditor or independent consultant the first time a firm onboards remotely.
- Crypto transfers above S\$1,500 must carry verified sender identity data to the receiving provider (the "Travel Rule"). Transfers to or from personal wallets need extra risk measures, such as making the customer prove control of the wallet.
- Retail customers get extra protection: a risk awareness check before access, no sign-up incentives, no leverage and no payment by locally issued credit card. From 1 January 2027, platforms must also collect each user's tax residence for crypto tax reporting. New stablecoin legislation has been consulted on but is not yet law (as of October 2026).

Singapore is open to crypto businesses, but only through licensing. Services involving DPTs, the legal term for cryptocurrencies such as bitcoin, are regulated activities under the Payment Services Act 2019, and the anti-money laundering rules for licensees sit in a binding MAS Notice backed by criminal penalties.

MAS is the single regulator for licensing, conduct and anti-money laundering supervision. The Suspicious Transaction Reporting Office of the Singapore Police Force receives suspicious transaction reports, and the Personal Data Protection Commission oversees the handling of customer data.

The biggest obstacle for a new entrant is the licence itself: local incorporation or a local branch, minimum capital, resident directors, a penetration-tested platform and a working compliance programme are all assessed before MAS grants it, and MAS has revoked a licence for false information supplied during the process.

CONTENTS

- 1 Who regulates this sector
- 2 Licensing and authorisation
- 3 AML, KYC and customer due diligence
- 4 Identity verification and onboarding
- 5 Digital channels: what's different
- 6 Data protection and biometrics
- 7 Sector-specific obligations
- 8 Risk indicators and red flags
- 9 Enforcement and penalties
- 10 Recent changes and what to watch
- 11 What this means for identity verification
 - Sources

1 Who regulates this sector

Authority	Remit for crypto businesses	Level	Official site
Monetary Authority of Singapore (MAS)	Licensing under the Payment Services Act 2019 and the Financial Services and Markets Act 2022; AML/CFT Notice PSN02; consumer protection guidelines; supervision and enforcement	National	mas.gov.sg
Suspicious Transaction Reporting Office (STRO), Singapore Police Force	Financial intelligence unit; receives suspicious transaction reports through the SONAR platform; publishes red flag indicators for DPT providers	National	police.gov.sg
Inland Revenue Authority of Singapore (IRAS)	Crypto-Asset Reporting Framework registration and returns from 2027	National	iras.gov.sg
Personal Data Protection Commission (PDPC)	Personal Data Protection Act 2012, including guidance on collecting national identification numbers	National	pdpc.gov.sg

Tokens that are capital markets products, such as tokenised securities, fall under the Securities and Futures Act 2001 rather than the Payment Services Act. MAS classifies tokens by economic substance, and an exchange that lists such tokens will likely need approval as a market operator ([MAS Guide on the Tokenisation of Capital Markets Products, 14 November 2025](#), paragraph 2.1 and case study 12). The Inland Revenue Authority of Singapore (IRAS) administers crypto tax reporting (section 7).

A "digital payment token service" is a payment service under the [Payment Services Act 2019](#) (PS Act), which defines a DPT as a digital unit of value, not denominated in or pegged to any currency, intended as a medium of exchange (section 2). Since 4 April 2024 the regulated scope also covers DPT custody and the facilitation of DPT transmission or exchange even where the provider never holds the customer's money or tokens **In force** ([MAS media release, 2 April 2024](#)).

Which licence

Licence	When it applies	Base capital	Other key conditions
Standard Payment Institution (SPI)	Up to S\$3 million monthly transactions for one payment service, or S\$6 million for two or more	S\$100,000	Singapore company or Singapore branch; permanent place of business; resident director requirement
Major Payment Institution (MPI)	Above the SPI thresholds	S\$250,000	As SPI, plus security of S\$100,000 or S\$200,000 (cash deposit with MAS or bank guarantee) before starting business

Sources: [MAS, Licensing for Payment Service Providers](#); [MAS Guidelines PS-G01](#) (last revised 8 October 2025), which summarise the thresholds in [section 6\(5\) of the PS Act](#). DPT applicants must also file a legal opinion and a recent external auditor's assessment of their AML/CFT and consumer protection controls; a technology and cybersecurity assessment follows in-principle approval, and online services need a remediated penetration test before licensing (PS-G01 3.1.8, 4.1). Licensees must meet the Technology Risk Management Notice FSM-N13 (PS-G01 5.5).

Carrying on a payment service business without a licence is an offence under [section 5\(3\) of the PS Act](#): individuals face up to S\$125,000, three years' imprisonment or both (plus S\$12,500 a day if continuing); entities up to S\$250,000 plus S\$25,000 a day.

Serving only overseas customers

From 30 June 2025, a person in Singapore providing DPT or tokenised capital markets services solely to customers outside Singapore needs a digital token service provider (DTSP) licence under the Financial Services and Markets Act 2022 **In force**. MAS has

stated that it has set the bar high and will generally not issue such a licence; unlicensed providers had to cease, with no transition period ([MAS, 6 June 2025](#)). Services relating only to utility or governance tokens are outside the regime.

3 AML, KYC and customer due diligence

Licensed DPT service providers are obliged entities under [MAS Notice PSN02](#), issued under section 16 of the Financial Services and Markets Act 2022, in force from 4 April 2024 and last amended with effect from 1 July 2025. The Notice is legally binding; the accompanying [Guidelines to Notice PSN02](#) (last revised 1 July 2025) set supervisory expectations, and MAS states that the degree of observance may affect its risk assessment of the firm (Guidelines paragraph 1-3).

When CDD applies

On establishing business relations, on any transaction for a non-account holder, on any value transfer for a non-account holder, on suspicion of money laundering or terrorism financing, and on doubts about earlier information (Notice 6.3). Anonymous accounts are prohibited (6.1).

Data to collect

For individuals: full name and aliases, unique identification number, residential address, date of birth and nationality (6.6).

Beneficial owners

Firms must ask whether beneficial owners exist and identify and verify them in a cascade: ownership, then control, then executive authority (6.13 to 6.14B). The Guidelines cite more than 25% ownership as an example (6-8-2).

Simplified and enhanced CDD

Simplified CDD is barred where a customer's transactions exceed S\$20,000 cumulatively in any one year, and for FATF high-risk countries (7.4). Politically exposed persons trigger senior management approval and source of wealth and funds checks (8.3).

Screening, monitoring and reporting

Customers, connected parties, beneficial owners and every originator and beneficiary of a value transfer must be screened against MAS and other Singapore authority lists (Notice 6.49 to 6.51); the Guidelines expect transaction screening in real time, before execution (6-15-10). Terrorist designations by the Inter-Ministry Committee on Terrorist Designation freeze funds and prohibit dealings with immediate effect ([Ministry of Home Affairs](#)). A positive sanctions hit requires freezing without delay and a suspicious transaction report

(STR) no later than one business day after suspicion is established (Guidelines 6-15-2). MAS expects distributed ledger analytics proportionate to the business (Guidelines 6-11-12).

STRs, including attempted transactions, must be filed promptly with STRO regardless of amount (Notice 16.2). The underlying duty is section 45 of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992, and failure to file may be an offence; reports are filed electronically through SONAR ([Singapore Police Force](#)). Cash payouts of S\$20,000 or more are banned (10.2). CDD and transaction records must be kept for at least five years (14.3).

4

Identity verification and onboarding

Identity must be verified "using reliable, independent source data, documents or information" (Notice 6.9). The Guidelines name government-issued identity cards and passports as the best documents because they are hardest to obtain illicitly or falsify digitally, and expect an identity document with a clear photograph for individuals; residential address may be evidenced by identity card, recent utility or phone bill, bank statement or government correspondence (6-3-1, 6-6-1, 6-6-2). Firms should also collect occupation, employer, income range and contact details (6-3-2, 6-4-2).

Timing

Verification must be completed before business relations begin or before any transaction for a non-account holder (Notice 6.42). Deferral is allowed only where it is essential to normal business and the risk is managed (6.43). The Guidelines set the outer limits: verification within 30 business days, after which the account is suspended, and termination at 120 business days (6-14-2).

Reliance and outsourcing

A firm may rely on certain regulated third parties for CDD but remains responsible (Notice 11.5). Holders of a payment services licence, and foreign payment or DPT providers holding only an equivalent licence, are not eligible third parties (Notice 11.1; Guidelines 11-4). Outsourcing to an identity verification vendor is different: the vendor applies the firm's own policies (Guidelines 11-3).

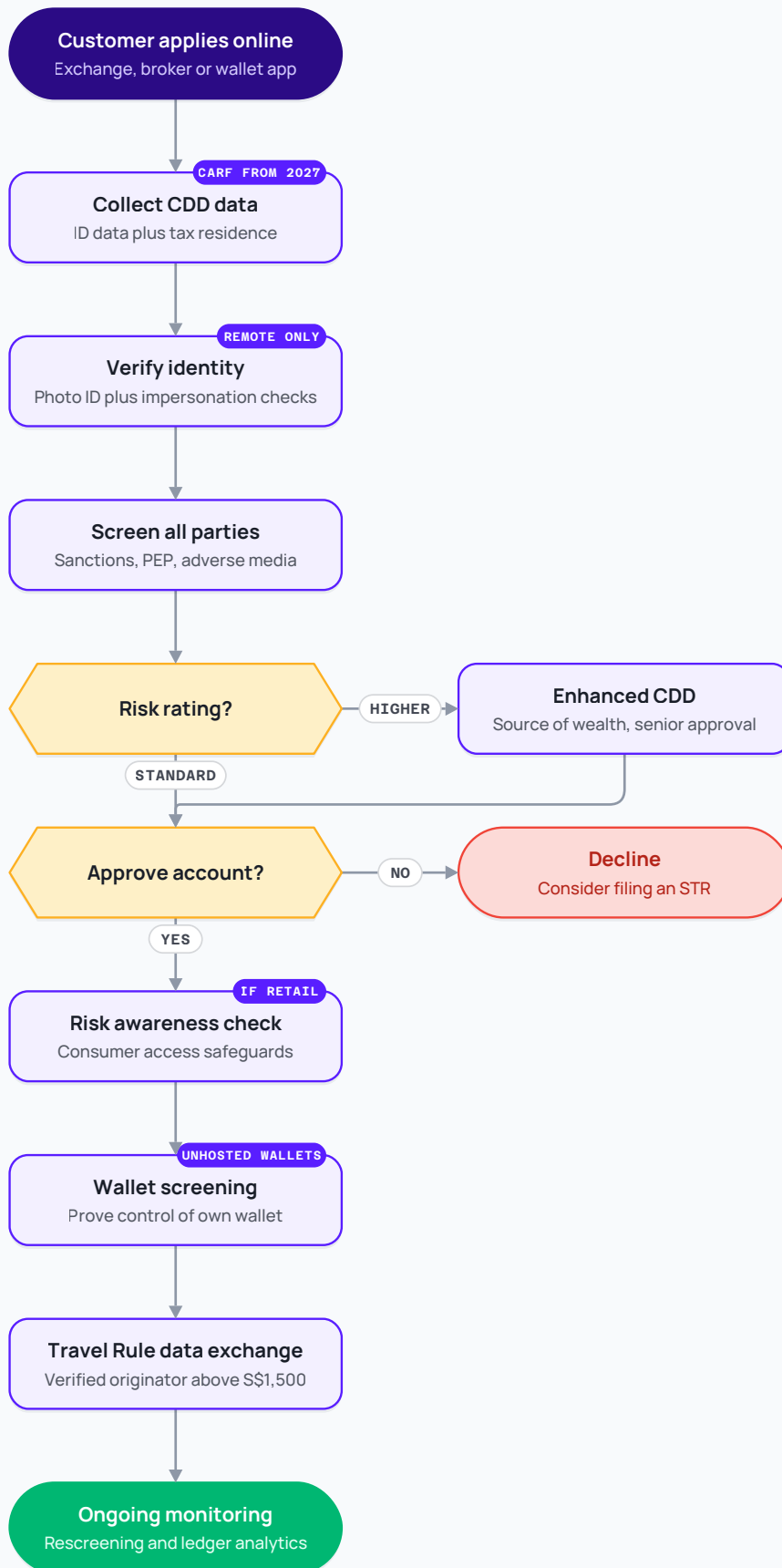


Figure 1. Remote onboarding of a retail customer by a licensed DPT service provider in Singapore.

5 Digital channels: what's different

Bottom line: remote onboarding is permitted and the core CDD rules are channel-neutral, but non-face-to-face business carries its own written policies, anti-impersonation checks and a mandatory independent assessment reported to MAS.

Requirement	In person	Online / remote	Difference
Onboarding permitted	Yes	Yes, with CDD at least as robust as in person (6.36)	Same
Specific risk policies	General CDD policies	Written policies for non-face-to-face risks (6.34, 6.35)	Differs
Independent assessment	Not required	External auditor or consultant at first remote contact; report to MAS within one year (6.37, 6.38)	Differs
Identity evidence	Original photo ID sighted	Photo ID plus additional anti-impersonation checks (Guidelines 6-12-3)	Differs
Device and location data	Not applicable	Device identifiers, IP addresses and geolocation listed as possible checks	Differs
Verification timing	Before business relations; deferral limits apply	Same rule (6.42 to 6.44)	Same
Travel Rule data	S\$1,500 tier	S\$1,500 tier (13.4 to 13.8)	Same
Record retention	At least 5 years	At least 5 years, electronic copies allowed (14.3, 14.4)	Same

The independent assessment

When a provider conducts its first non-face-to-face business contact, it must appoint, at its own expense, an external auditor or independent qualified consultant to assess its non-face-to-face policies, including any technology used to manage impersonation risk, and submit the report to MAS within one year (Notice 6.37, 6.38). A substantial change, such as a new technology solution, triggers a fresh assessment (6.39).

Accepted anti-impersonation methods

MAS gives non-exhaustive examples (Guidelines 6-12-3): independently verifiable phone contact, address confirmation, an initial deposit from the customer's account with a bank in Singapore, proof of control of the DPT wallet making the first deposit, device identifiers and IP addresses with time stamps and geolocation, real-time video conferencing comparable to face-to-face contact, secure digital signatures, and biometric technologies such as facial recognition, which "should be linked incontrovertibly to the customer".

Location signals

The Guidelines treat customers' use of IP anonymisers as a risk factor (4-6), and STRO lists access through a virtual private network or Tor as a red flag. Notice PSN02 does not prescribe geo-blocking of particular jurisdictions; the obligation is to assess and mitigate country risk, and customers from countries subject to a FATF call for countermeasures must be treated as higher risk (8.6).

Pending: the [Proposed, comments closed 16 Oct 2026](#) stablecoin amendments to the PS Act would add a licensed stablecoin issuer category but would not change the onboarding rules above.

6 Data protection and biometrics

The Personal Data Protection Act 2012 governs customer data generally. Notice PSN02 lets a provider collect, use and disclose personal data of customers, representatives, connected parties and beneficial owners without consent to comply with the Notice, and limits access and correction rights to core identification data (Notice 15.2 to 15.4). The PDPC's advisory guidelines restrict collecting NRIC (national identity card) numbers to cases required by law or where identity must be verified to a high degree of fidelity, which covers AML verification; the PDPC advises against using NRIC numbers to authenticate identity ([PDPC, updated 14 December 2024](#)).

MAS prescribes no biometric standard; biometrics are one accepted anti-impersonation technique, tested in the independent assessment. CDD evidence, including images and liveness results, falls under the five-year minimum retention in Notice 14.3.

Travel Rule

At or below S\$1,500, the ordering provider must send both parties' names and account numbers (or a unique transaction reference). Above S\$1,500 it must also verify the originator and add an address, identification number, or date and place of birth (Notice 13.4, 13.6). Data must travel immediately and securely; if it cannot, the transfer must not be executed (13.9, 13.11).

Self-hosted wallets

The Travel Rule applies only between financial institutions. Transfers to or from an entity that is not a regulated financial institution, which includes a customer's own unhosted wallet, require enhanced risk mitigation (Notice 6.27). For the customer's own wallet, the Guidelines suggest requiring proof of control by sending an amount specified by the provider (13-7).

Custody and retail safeguards

Since 4 October 2024, DPT providers must segregate customer assets and hold them on trust **In force** ([MAS, 2 April 2024](#)). From 19 June 2025, [MAS Guidelines PS-G03](#) (revised 19 September 2024) expect providers to give retail customers a Risk Awareness Assessment and refuse DPT services to those who fail it, offer no incentives for sign-ups, referrals or trading, provide no credit, leverage or DPT derivatives, and refuse payment by credit or charge cards issued in Singapore (PS-G03 1.2.1, 4.2 to 4.4) **In force**.

Tax reporting (CARF)

The [Income Tax \(International Tax Compliance Agreements\) \(Crypto-Asset Reporting Framework\) Regulations 2026](#) **Adopted, effective 1 Jan 2027** require Singaporean reporting crypto-asset service providers to obtain a valid self-certification of each user's tax residence on or before establishing the relationship, collect self-certifications from existing users by 31 December 2027 (no transactions for them from 1 January 2028 without one), register with IRAS by 31 March 2028 and file an annual return by 31 May (regulations 7, 11 and 12).

Scam account orders

The [Scams \(Countermeasures\) and Other Matters Act 2026](#) (Act 21 of 2026) **Adopted, commencement date not yet set** will let the Police order providers of DPT accounts to disable accounts for up to 30 days, restrict services to identified persons for up to three

years and disclose account information; non-compliance by a firm carries a fine of up to S\$1 million.

Stablecoins

Under the proposed MAS Single-Currency Stablecoin framework, only licensed issuers of stablecoins pegged to the Singapore dollar or a G10 currency could call their tokens "MAS-regulated stablecoins"; other stablecoins would be treated as DPTs and carry the same consumer safeguards [Proposed, comments closed 16 Oct 2026](#). The consultation also proposes prohibiting interest on MAS-regulated stablecoins.

8

Risk indicators and red flags

STRO RED FLAG INDICATORS FOR DPT SERVICE PROVIDERS (SELECTION)

- **Anonymised access:** logging in through a virtual private network or Tor.
- **Throwaway contact details:** registering with an encrypted, anonymous or temporary email service.
- **Shifting identifiers:** frequent changes of address, IP address, linked bank accounts or wallet addresses.
- **Tainted sources:** deposits from or withdrawals to addresses linked to darknet markets, mixers or ransomware.
- **Pass-through activity:** assets withdrawn immediately after deposit without a plausible business reason.
- **Structuring:** many small transactions in a short period that add up to a substantial total.
- **Funnel accounts:** many unrelated senders, often from different countries, paying one local account.
- **Kiosk funding:** frequent or large receipts from virtual asset kiosks.

Sources: [STRO, Red Flag Indicators for DPT Service Providers](#); the same indicators appear in Appendix B of the Guidelines to Notice PSN02 (revised 1 July 2025).

9 Enforcement and penalties

Breach of an AML/CFT Notice is a criminal offence under section 16(4) of the Financial Services and Markets Act 2022: a fine of up to S\$1 million for each offence and, for a continuing offence, a further S\$100,000 for every day or part of a day it continues after conviction ([FSMA section 16, current version](#); [MAS, Anti-Money Laundering](#)). MAS may compound offences rather than prosecute: on 27 June 2025 it imposed composition penalties of S\$110,000 to S\$280,000 (S\$960,000 in total) on five remittance institutions for breaches of the parallel Notice PSN01, including screening failures and missing originator data ([MAS enforcement action](#)).

Licence revocation is the other main tool. MAS revoked the major payment institution licence of Bsquared Technology Pte Ltd, a DPT provider licensed on 1 January 2025, with effect from 14 May 2026 for weak risk management and conflict of interest controls, outsourcing failures and materially false or misleading information given to MAS ([MAS, 20 May 2026](#)).

10 Recent changes and what to watch

- **6 October 2026** Passed, commencement not yet set [Financial Services and Markets \(Amendment\) Bill](#) passed: section 16 powers extend to proliferation financing; penalties unchanged.
- **9 September 2026** Adopted, commencement date not yet set Scams (Countermeasures) Act passed (gazetted 29 September), covering DPT accounts.
- **1 September 2026** Proposed, comments closed 16 Oct 2026 MAS consultation on stablecoin amendments to the PS Act; no bill yet.
- **11 August 2026** Adopted, effective 1 Jan 2027 CARF Regulations gazetted. Onboarding needs a tax residence self-certification step.
- **20 May 2026** Effective 14 May 2026 Bsquared Technology's DPT licence revoked.
- **1 July 2025** In force PSN02 amendments; existing customers reviewed on a risk basis (6.48A).
- **30 June 2025** In force DTSP regime for firms serving only overseas customers.

What this means for identity verification

- **Verify before the first trade.** No funding before verification, or limits and a 30 business day clock where deferral is justified.
- **Layer impersonation checks.** Combine photo ID with MAS-listed controls such as face match, video, a Singapore bank deposit or device signals.
- **Plan for the audit.** Document the remote flow and its performance; changing vendors may trigger a new assessment.
- **Treat the NRIC number as data, not a password.** Never use it to authenticate returning users.
- **Add tax residence.** Capture a CARF self-certification at onboarding from 2027 alongside CDD data.
- **Extend identity to wallets.** Exchange Travel Rule data, screen counterparties in real time and require proof of control for self-hosted wallets.
- **Re-verify on triggers.** Refresh CDD for higher-risk customers periodically and for all customers on trigger events; keep evidence for at least five years.

How Identomat helps

Identomat runs identity verification, screening and monitoring for regulated businesses on one platform, with workflows you configure for each market. For the requirements in this guide, that means:

- Remote KYC onboarding with ID document capture and verification (including NFC), face match and biometric liveness to address impersonation risk in non-face-to-face onboarding.
- Video KYC for customers or cases where real-time video contact is the chosen anti-impersonation control.
- AML screening of customers, connected parties and beneficial owners against sanctions, PEP and adverse-media lists, with ongoing monitoring for periodic rescreening.
- KYB and beneficial owner verification for corporate customers, with KYC questionnaires for occupation, source of funds and source of wealth.
- A no-code workflow builder with an audit trail of each check, to evidence the onboarding design to an independent assessor and to MAS.

Request a meeting

DISCLAIMER

This article is intended for informational purposes only and does not constitute legal advice. It is a compilation of information from various sources and reflects the information available as of the last updated date indicated above. Laws, regulations, and regulatory guidance may change, so readers should consult qualified legal professionals for advice specific to their circumstances.

Sources

- **Payment Services Act 2019**, Singapore Statutes Online, section 2 (definitions), sso.agc.gov.sg/Act/PSA2019
- **MAS Notice PSN02, Prevention of Money Laundering and Countering the Financing of Terrorism, Digital Payment Token Service**, 2 April 2024, last revised 30 June 2025 (effective 1 July 2025), mas.gov.sg; amendment document [PDF](#)

- **Guidelines to MAS Notice PSN02**, 2 April 2024, last revised 1 July 2025, [mas.gov.sg](https://www.mas.gov.sg); [PDF](#), paragraphs 1-3, 4-6, 6-3 to 6-15, 7, 8, 11, 13-7
- **MAS Guidelines on Licensing for Payment Service Providers (PS-G01)**, 18 December 2019, last revised 8 October 2025, paragraphs 2.3, 3.1, 4.1, 5.5 and Appendix 6, [mas.gov.sg](https://www.mas.gov.sg)
- **MAS Guidelines on the Provision of Consumer Protection Safeguards by DPT Service Providers (PS-G03)**, 2 April 2024, last revised 19 September 2024, paragraphs 1.2.1 and 4.2 to 4.4, [mas.gov.sg](https://www.mas.gov.sg)
- **MAS Guide on the Tokenisation of Capital Markets Products**, 14 November 2025, paragraphs 1.5, 2.1 and case study 12, [mas.gov.sg](https://www.mas.gov.sg)
- **Financial Services and Markets Act 2022**, section 16, current version as at 28 October 2026, sso.agc.gov.sg; as enacted, Government Gazette Acts Supplement, 13 May 2022, egazette.gov.sg ([PDF](#))
- **Income Tax (International Tax Compliance Agreements) (Crypto-Asset Reporting Framework) Regulations 2026** (S 551/2026), gazetted 11 August 2026, in operation 1 January 2027, regulations 1, 7, 11 and 12, egazette.gov.sg ([PDF](#))
- **Scams (Countermeasures) and Other Matters Act 2026** (Act 21 of 2026), passed 9 September 2026, assented 24 September 2026, published in the Acts Supplement 29 September 2026, section 7 (new Part 2A of the Protection from Scams Act 2025, sections 6A to 6F), sso.agc.gov.sg
- **Financial Services and Markets (Amendment) Bill** (Bill No. 19/2026), read the first time 8 September 2026, passed 6 October 2026, clause 5, parliament.gov.sg ([PDF](#)); status from [Parliament, Bills Introduced](#)
- **Payment Services Act 2019**, sections 5 and 6(5), current version as at 28 October 2026, sso.agc.gov.sg
- **Ministry of Home Affairs, Countering the financing of terrorism** (Inter-Ministry Committee on Terrorist Designation), updated 30 January 2026, mha.gov.sg
- **MAS, Licensing for Payment Service Providers**, last updated 2 September 2024, [mas.gov.sg](https://www.mas.gov.sg)
- **MAS media release, MAS Expands Scope of Regulated Payment Services**, 2 April 2024, [mas.gov.sg](https://www.mas.gov.sg)
- **MAS media release, MAS Clarifies Regulatory Regime for Digital Token Service Providers**, 6 June 2025, [mas.gov.sg](https://www.mas.gov.sg)
- **MAS media release, MAS Consults on Legislative Amendments to Implement Stablecoin Regulatory Framework**, 1 September 2026, [mas.gov.sg](https://www.mas.gov.sg)
- **MAS media release, MAS Revokes the Major Payment Institution Licence of Bsquared Technology Pte Ltd**, 20 May 2026, [mas.gov.sg](https://www.mas.gov.sg)
- **MAS enforcement action, MAS Imposes Composition Penalties against Five Major Payment Institutions**, 27 June 2025, [mas.gov.sg](https://www.mas.gov.sg)
- **MAS, Anti-Money Laundering** (penalties under the Financial Services and Markets Act 2022), last updated 23 October 2026, [mas.gov.sg](https://www.mas.gov.sg)
- **Singapore Police Force, Suspicious Transaction Reporting** (CDSA section 45; SONAR), police.gov.sg
- **STRO, Red Flag Indicators for Digital Payment Token Service Providers**, police.gov.sg ([PDF](#))

- PDPC, **Advisory Guidelines on the PDPA for NRIC and other National Identification Numbers**, 31 August 2018, page updated 14 December 2024, pdpc.gov.sg