



Identomat

COMPLIANCE GUIDE

Fintech & Digital Payments Compliance in Singapore

COUNTRY **Singapore**

INDUSTRY **Fintech & Digital Payments**

LAST UPDATED **28 October 2026**

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

Key takeaways

- Any business offering e-wallets, money transfers, remittance, e-money or money-changing in Singapore needs a licence from the MAS, the single financial regulator. Smaller firms take a standard licence; firms above S\$3 million a month in transactions (S\$6 million across two or more services) need a major licence.
- Fully online onboarding is allowed, but remote identity checks must be at least as strong as checks done in person, and the firm must add checks against impersonation, such as biometric face matching, live video or a certified digital signature.
- The first time a firm onboards a customer remotely, it must hire an external auditor or independent consultant to test its remote onboarding controls and send the report to MAS within one year. This requirement has no in-person equivalent.
- Identity must be verified before the account opens. Verification can be briefly deferred, but MAS guidance caps the delay at 30 business days, after which the account should be suspended.
- E-wallet providers can let customers hold up to S\$20,000 and send up to S\$100,000 a year, but only after putting MAS-specified anti-scam controls in place. A new anti-scam law, passed but not yet in force, will let police order payment firms to refuse service to suspected scam mules for up to three years and to freeze accounts for up to 30 days.

Singapore is open to fintech and digital payment businesses, including online-only models, but every regulated payment activity requires a licence under the Payment Services Act 2019. An applicant must be a Singapore-incorporated company or a Singapore branch of a foreign corporation, with a permanent place of business in Singapore and at least one executive director who meets MAS's residency rules.

MAS licenses and supervises payment firms and sets their anti-money laundering rules in Notice PSN01. Suspicious transactions are reported to the Suspicious Transaction Reporting Office of the Singapore Police Force.

The biggest obstacle for a new entrant is usually not the licence itself but the evidence MAS expects behind it: compliance arrangements, a penetration-tested online platform before launch, and, for remote onboarding, an independent assessment of the controls used to stop impersonation.

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 payment firms	Level	Official site
Monetary Authority of Singapore (MAS)	Licensing under the Payment Services Act 2019; AML/CFT Notices PSN01 and PSN02; conduct, technology risk 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	National	police.gov.sg
Inter-Ministry Committee on Terrorist Designation (with the Ministry of Home Affairs)	Designates terrorists under the Terrorism (Suppression of Financing) Act 2002	National	mha.gov.sg
Personal Data Protection Commission (PDPC)	Personal data rules, including the handling of NRIC numbers	National	pdpc.gov.sg
Ministry of Law, AML/CFT Division	Publishes national risk assessments and Singapore's FATF evaluation materials	National	acd.mlaw.gov.sg

MAS is a single integrated regulator, so a payment firm adding banking, insurance or digital payment token activity deals with the same authority under different instruments.

Section 5(1) of the Payment Services Act 2019 (PS Act) prohibits carrying on a business of providing any type of payment service in Singapore without a licence, unless the provider is exempt under section 13 (banks, merchant banks, finance companies and card issuers are). The Act covers seven services: account issuance (including e-wallets), domestic money transfer (including payment gateways), cross-border money transfer, merchant acquisition, e-money issuance, digital payment token services and money-changing.

Licence	Who needs it	Base capital	Other entry conditions
Money-changing licence	Firms that only buy and sell foreign currency notes	See MAS licensing guidelines	Ownership and nationality rules by entity type; AML/CFT experience
Standard payment institution	Firms within the section 6(5) thresholds: monthly transactions averaging S\$3 million for one service or S\$6 million for two or more, and average daily e-money of S\$5 million	S\$100,000	Company or foreign corporation; permanent place of business or registered office in Singapore; an executive director who is a citizen or permanent resident, or in a prescribed class
Major payment institution	Firms above any of those thresholds; application to change licence within the prescribed period after crossing one	S\$250,000	As above, plus security of S\$100,000 (monthly transactions averaging up to S\$6 million for any one service) or S\$200,000, as a cash deposit with MAS or a bank guarantee

MAS's licensing guidelines (PS-G01) add that base capital should cover six to twelve months of operating expenses. One condition applies only to digital businesses: an applicant that will provide online financial services must penetration-test the platform, remediate every high-risk finding and have the remediation independently validated before the licence is granted (it need not be done before applying).

Licensees file returns (Notice PSN04), meet cyber hygiene rules (FSM-N14), follow conduct rules (PSN07), report material suspicious activities and frauds to MAS within five working days (Notice PSN03) and appoint an auditor every year. They may not grant credit facilities to individuals, and e-money issuers may not lend customer money (section 20). Money-changing and cross-border transfer may be offered only at the permanent place of business unless MAS approves another location (section 14(5)).

MAS Notice PSN01 (dated 2 April 2024, last revised 30 June 2025) is a legally binding notice issued under section 16 of the Financial Services and Markets Act 2022. It applies to licensees providing account issuance, domestic money transfer, cross-border money transfer or money-changing services, and to exempt providers (such as banks) offering a combined wallet product. Merchant acquisition is not regulated for AML/CFT purposes because MAS assesses it as low risk (PS Act FAQ 32).

When due diligence is triggered

Customer due diligence (CDD) is required when a firm opens a business relationship, on any cross-border wire transfer or cross-border money transfer for a non-account customer, on any other transaction above S\$5,000 for a non-account customer, on suspicion of money laundering or terrorism financing, and when earlier information is in doubt (paragraph 7.3).

Exempted products

A wallet that allows no cash withdrawal, no cash refunds above S\$100 without photo ID, and holds no more than S\$1,000 is outside the CDD, screening, reliance and wire transfer paragraphs of PSN01 (paragraphs 2.1 and 3.3).

Simplified CDD

Permitted where risk is assessed as low and documented, but never once a customer's transactions exceed S\$20,000 cumulatively in a year, or where FATF countermeasure jurisdictions or suspicion are involved (paragraph 8).

Enhanced CDD

For politically exposed persons and other higher-risk customers: senior management approval, source of wealth and source of funds, and enhanced monitoring (paragraph 9).

Beneficial ownership, screening and monitoring

Firms must ask whether a beneficial owner exists, identify the natural persons who ultimately own or control a corporate customer, and take reasonable steps to verify them (paragraphs 7.13 to 7.14B). Customers, persons acting for them, connected parties and beneficial owners must be screened against money laundering and terrorism financing sources and lists from MAS and other Singapore authorities, at onboarding, periodically

and whenever the lists change; wire transfer originators and beneficiaries are screened too (paragraphs 7.51 to 7.54). MAS asks every person in Singapore to screen clients against the United Nations sanctions lists it publishes. Ongoing monitoring of the relationship cannot be outsourced through reliance (paragraph 12.3).

Reporting, wire transfers and records

Section 45 of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992 requires anyone who knows or has reasonable grounds to suspect that property is connected to crime to file a suspicious transaction report (STR) with STRO, filed electronically through SONAR. PSN01 requires reports promptly and regardless of amount, including attempted transactions (paragraph 18.2). Cash payouts of S\$20,000 or more are prohibited for most services (paragraph 11.2). For cross-border wire transfers above S\$1,500 the ordering firm must verify the originator and send an address, identification number or date and place of birth; at or below S\$1,500 names and account numbers suffice (paragraphs 15.4 and 15.6). CDD and transaction records are kept for at least five years (paragraph 16.3).

4 Identity verification and onboarding

For an individual, PSN01 requires full name and aliases, a unique identification number (identity card, birth certificate or passport number), residential address, date of birth and nationality (paragraph 7.6). Identity must be verified “using reliable, independent source data, documents or information” (paragraph 7.9). The Notice is technology-neutral: it does not prescribe documents, and neither the Notice nor its Guidelines name Singpass or Myinfo as a verification source.

Verification must be complete before the business relationship starts (paragraph 7.43). A firm may defer it where this is essential to normal business and the risk is managed (paragraph 7.44); the Guidelines to PSN01 say deferred verification should not exceed 30 business days, after which the relationship should be suspended, and suggest transaction limits in the meantime (paragraph 7-14-2).

Reliance on another regulated financial institution’s CDD is allowed if it is supervised to FATF standards, but the firm must obtain the CDD information immediately and remains responsible (paragraphs 12.2 to 12.5). For corporate customers, PSN01 allows date of birth and nationality in place of a connected party’s identification number where risk is not high and the number cannot be obtained (paragraph 7.8A).

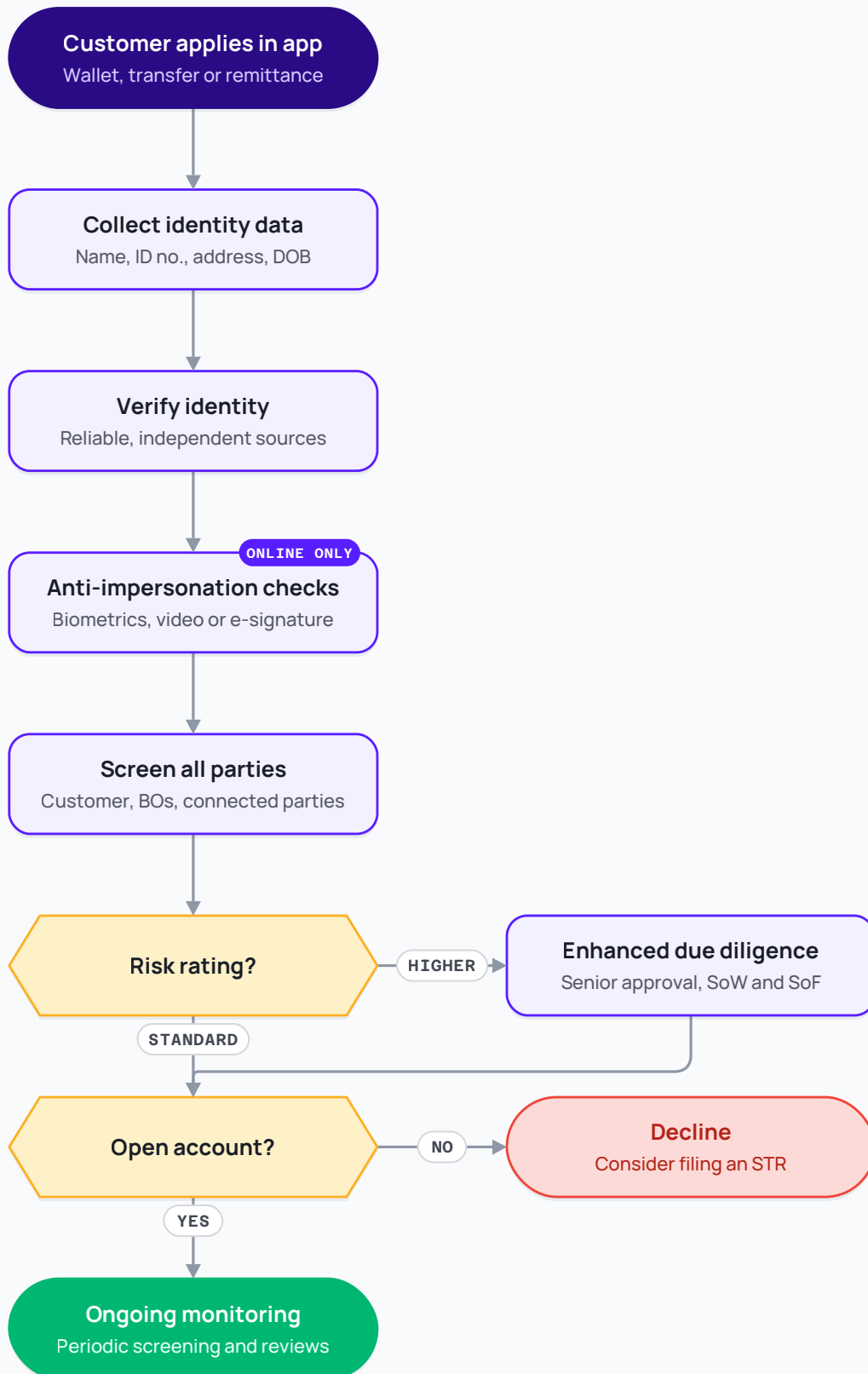


Figure 1. Remote customer onboarding for a Singapore payment institution under MAS Notice PSN01.

Bottom line: remote onboarding is permitted on the same data and timing rules as in person, but MAS expects extra anti-impersonation checks and an independent assessment of the remote onboarding controls, reported to MAS within a year of the first remote customer.

Requirement	In person	Online / remote	Difference
Licence prerequisites	Standard licence conditions	Penetration test, remediation and independent validation before licence	Differs
Remote onboarding permitted	Yes	Yes, with written policies for non-face-to-face risks	Differs
Strength of CDD	PSN01 paragraph 7 measures	At least as robust as face-to-face	Same
Identity data collected	Name, ID number, address, date of birth, nationality	Same five elements	Same
Impersonation controls	Physical presence	Additional checks expected, such as biometrics, live video, digital signature	Differs
Independent assessment	None	External auditor or consultant; report to MAS within one year	Differs
Verification timing	Before relationship; deferral up to 30 business days	Same	Same
E-wallet account security	Not applicable	Anti-scam controls before higher caps; phishing loss-sharing duties	Differs

Anti-impersonation checks

PSN01 requires policies addressing the specific risks of non-face-to-face business and CDD at least as robust as in person (paragraphs 7.34 to 7.36). The Guidelines explain that internet and phone applications may pose greater risk because of easy unauthorised access, multiple fictitious applications, no physical documents and fast transactions (paragraph 7-12-1). They list additional checks a firm may use, including real-time video comparable to face-to-face contact, a document signed with credentials from a certified Certificate Authority under the Electronic Transactions Act 2010, and biometric technology such as facial recognition that is linked incontrovertibly to the customer (paragraph 7-12-3). These are examples in MAS Guidelines, which are not legally binding in the way Notices are: breaching them is not an offence, but MAS expects their spirit to be observed and takes observance into account in its risk assessment of the firm.

The independent assessment

After its first non-face-to-face business contact, a firm must appoint, at its own cost, an external auditor or independent qualified consultant to assess its remote onboarding policies, including any technology used against impersonation, and submit the report to MAS within one year (paragraphs 7.37 and 7.38). A substantial change, such as adopting a different technology solution, triggers a fresh assessment (paragraph 7.39; Guidelines paragraph 7-12-6).

Serving Singapore users from abroad

An unlicensed provider, whether in Singapore or elsewhere, may not offer payment services to the public in Singapore or advertise such an offer, and a person in Singapore may not do so on behalf of an unlicensed overseas provider (PS Act section 9). An app or website marketed to Singapore users therefore needs a licence, and a Singapore place of business, before launch.

E-wallet security

Major payment institutions issuing personal e-wallets that go above the former S\$5,000 holding and S\$30,000 annual outflow limits must first implement MAS's anti-scam measures, including a 12-hour cooling-off period after login on a new device, alerts for high-risk activity and a self-service kill switch (MAS Circular MAS/PD/2024/10/04, 25 October 2024). The same firms are responsible financial institutions under the Guidelines on Shared Responsibility Framework, applicable since 16 December 2024.

6 Data protection and biometrics

The Personal Data Protection Act 2012 (PDPA) is the general regime, and other written law prevails where it is inconsistent (section 4(6)). PSN01 uses that room: payment firms may collect, use and disclose the personal data of customers, beneficial owners, connected parties and representatives without consent where needed to comply with the Notice (paragraph 17.4), and need not give access to or correction of that data beyond the core identity fields (paragraphs 17.2 and 17.3).

The PDPC's Advisory Guidelines on NRIC and other national identification numbers allow organisations to collect NRIC numbers or copies of the NRIC without consent where the law requires it, expect a higher level of security for them, and say physical NRICs should not be retained unless the law requires it (paragraphs 2.4, 3.2 and 4.1). Biometric and video evidence captured during onboarding forms part of CDD records, kept for at least five years after the relationship ends, electronically if admissible in a Singapore court (PSN01 paragraphs 16.3 and 16.4).

The NRIC number is an identifier, not proof of identity. A joint PDPC and Cyber Security Agency advisory (issued June 2025, updated May 2026) tells organisations to stop using full or partial NRIC numbers to authenticate people and warns that someone who can state an NRIC number is not necessarily its holder. Login and step-up authentication should rely on something the user owns or is, such as a token or a biometric.

7 Sector-specific obligations

Rule	What it requires	Source
E-wallet holding cap	Personal e-wallets issued by a major payment institution may hold up to S\$20,000 at any time, aggregated across a user's wallets; wallets of S\$1,000 or less without a shared identifier may be excluded	PS Act s 24; PS Regulations reg 18 (amended 15 Dec 2023)
E-wallet outflow cap	Up to S\$100,000 a year, excluding transfers to the user's own or designated personal bank account	PS Act s 24; PS Regulations reg 18
No cash-out in Singapore dollars	E-money may not be withdrawn and exchanged for Singapore notes and coins for Singapore residents, except when the account is closed	PS Act s 19

Safeguarding	Major payment institutions offering money transfer or merchant acquisition safeguard customer money by the next business day; e-money issuers from receipt; by bank undertaking, bank guarantee or trust account	PS Act s 23
Security deposit	MAS can use the security to pay customer claims if the licence lapses or is revoked; an auditor's closure certificate is due within 45 days	PS Act s 22

Cross-border remittance and agents

A customer without an account must go through CDD before any cross-border money transfer, whatever the amount (PSN01 paragraph 7.3©). Agents used in Singapore must themselves be licensed or exempt (PS Act section 18), and AML frameworks must oversee local and overseas agents (PS-G01). Agents assisting with cross-border transfers need a written, senior-management-approved arrangement and coverage by the firm's AML programme (PSN01 paragraph 14).

Unauthorised transactions and phishing losses

For e-wallets able to hold more than S\$1,000, issued to individuals or sole proprietors, the E-Payments User Protection Guidelines require real-time outgoing transaction alerts and make the provider bear losses caused by its own action or omission (paragraphs 4.10 and 5.4). Under the Shared Responsibility Framework, the same providers carry duties to mitigate phishing scams and are expected to compensate victims where they breach them, including real-time surveillance for rapid draining of balances, which MAS has described for banks as holding such transfers for at least 24 hours (written reply, 3 February 2026).

PAYMENT AND REMITTANCE TYPOLOGIES (MAS, STRO, FATF)

- **Cross-border remittance:** Singapore rates money remittance, including unlicensed remittance and cross-border online payments, the highest terrorism financing risk.
- **Multiple fictitious applications:** repeated remote sign-ups at low cost, flagged in the Guidelines to PSN01.
- **Mule accounts:** accounts sold to scammers to move funds by internet banking, PayNow and cards.
- **Repeat mules:** individuals already linked to mule offences applying for new facilities.
- **Structuring:** linked transactions split to stay under the S\$5,000 or S\$20,000 thresholds.
- **New-device takeover:** login from a new device followed by payee or limit changes.
- **Licence misuse:** a third party operating a remittance business under a licensee's name.
- **Deepfakes:** synthetic video or voice used to impersonate customers, flagged by MAS in September 2025.

Breach	Maximum penalty	Source
Breach of Notice PSN01	Fine of S\$1 million per offence; may be compounded	FSMA s 16(4), s 177(1)
Unlicensed payment business, or holding out as licensed	Individuals: S\$125,000 or 3 years' imprisonment or both; others: S\$250,000; plus S\$12,500 or S\$25,000 a day for continuing offences	PS Act ss 5(3), 8(2)
Soliciting the Singapore public without a licence	As for unlicensed business	PS Act s 9

Breach of e-wallet caps or safeguarding	S\$250,000, plus S\$25,000 a day for continuing offences	PS Act ss 23, 24(4)
Ignoring a police service limitation or account disabling order (once in force)	Companies: S\$1 million, plus S\$100,000 a day; individuals: S\$20,000 or 12 months' imprisonment or both	Protection from Scams Act 2025 s 6F, inserted by Act 21 of 2026
False or misleading information, or contraventions	Licence revocation or suspension	PS Act s 11(2)

On 27 June 2025 MAS imposed composition penalties totalling S\$960,000 on five major payment institutions providing cross-border money transfer, ranging from S\$110,000 to S\$280,000, for failures including not obtaining residential addresses, not asking about beneficial owners, not verifying identity using reliable independent sources, not screening customers and omitting originator or beneficiary information from wire transfers. On 14 October 2026 MAS announced it had revoked the major payment institution licence of Sir Money Changer Pte. Ltd. with effect from 15 September 2026, for letting a third party run a remittance business under its name and giving MAS false information. On 9 July 2026 a licensed money-changer, its director and its compliance manager were charged in court for breaching MAS directions on complaints handling; officers can be prosecuted personally. Singapore's 2026 FATF evaluation still judges penalties for unlicensed activity not dissuasive.

10 Recent changes and what to watch

• 16 October 2026: FIDReC membership for payment firms

Proposed, comments close 30 Nov 2026 All standard and major payment institutions would have to join the Financial Industry Disputes Resolution Centre.

• 14 October 2026: licence revocation for licence misuse **In force** Licensees must keep control of every business operated under their name.

• 6 October 2026: Financial Services and Markets (Amendment) Bill 2026 passed

Passed 6 Oct 2026, not yet in force Makes proliferation financing an explicit part of MAS supervision from a date to be notified in the Gazette.

• 29 September 2026: Scams (Countermeasures) and Other Matters Act 2026

Adopted, not in force as at 23 Oct 2026 Police will be able to order payment firms to refuse or restrict services to an identified person for up to three years, disable payment

accounts for up to 30 days and disclose account information; this puts the scam-mule restrictions in place since October 2025 on a statutory footing.

- **1 September 2026: stablecoin amendments to the PS Act**

Proposed, consultation closed 16 Oct 2026 Only licensed issuers could call single-currency stablecoins “MAS-regulated”; others would be treated as digital payment tokens.

- **May 2026: FATF-APG Mutual Evaluation of Singapore** **Published** It rates remittance as the highest terrorism financing risk and cross-border payment firms as medium-high money laundering risk.

- **1 July 2025: PSN01 amendments** **In force** Proliferation financing written into the Notice, and date of birth, nationality and business address allowed in place of a beneficial owner’s ID number or residential address in lower-risk cases.

11 What this means for identity verification

Onboarding must capture name, identification number, residential address, date of birth and nationality, verified against a source the firm can defend as reliable and independent; because no source is mandated, the choice should be documented in the risk assessment.

Remote flows need a demonstrable anti-impersonation layer, such as facial recognition, live video or a certified digital signature, which an independent assessor will examine within a year of launch and after any substantial technology change.

Screening must cover beneficial owners and connected parties and rerun when lists change. Biometric and video evidence is kept for five years after the relationship ends, and authentication should never rely on NRIC numbers.

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 that captures the five identity data points MAS Notice PSN01 requires, with ID document capture and verification including NFC.
- Biometric liveness and face match to address impersonation risk in non-face-to-face onboarding.
- AML screening of customers, beneficial owners and connected parties against sanctions, PEP and watchlists, at onboarding and on an ongoing basis.
- KYB and beneficial owner verification for business customers and merchants.
- No-code workflow builder with an audit trail of each check, to support record keeping and independent assessments.

[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** (2020 Revised Edition, informal consolidation in force from 9 March 2025), sections 5, 6, 8, 9, 11, 13, 14, 18 to 20 and 22 to 24, Singapore Statutes Online, sso.agc.gov.sg
- **Payment Services (Amendment No. 2) Regulations 2023** (S 827/2023), amending regulation 18 of the Payment Services Regulations 2019 from 15 December 2023, sso.agc.gov.sg
- **Personal Data Protection Act 2012**, section 4(6), sso.agc.gov.sg
- **Scams (Countermeasures) and Other Matters Act 2026** (Act 21 of 2026), passed 9 September 2026, assented 24 September 2026, uncommenced as at 23 October 2026, inserting Part 2A (sections 6A to 6N) into the Protection from Scams Act 2025, sso.agc.gov.sg

- **First reading of the Scams (Countermeasures) and Other Matters Bill**, Ministry of Home Affairs, 4 August 2026, mha.gov.sg
- **Bills Introduced**, Parliament of Singapore (dates passed for Bills 16/2026 and 19/2026), parliament.gov.sg
- **Financial Services and Markets (Amendment) Bill**, Bill No. 19/2026, read the first time 8 September 2026, sso.agc.gov.sg
- **Guidelines on Licensing for Payment Service Providers (PS-G01)**, last revised 26 August 2024, paragraphs 3.1.5 to 3.1.8, mas.gov.sg
- **MAS Notice PSN03, Reporting of Suspicious Activities and Incidents of Fraud**, 5 December 2019, paragraphs 4 to 8, mas.gov.sg
- **MAS Supervisory Approach and Regulatory Instruments**, MAS, mas.gov.sg
- **E-Payments User Protection Guidelines**, effective 16 December 2024, paragraphs 2, 4.10 and 5.4, mas.gov.sg
- **Licensing for Payment Service Providers**, MAS, mas.gov.sg
- **Types of Payment Services**, MAS, mas.gov.sg
- **Ongoing Requirements for Payment Service Providers**, MAS, mas.gov.sg
- **MAS Notice PSN01, Prevention of Money Laundering and Countering the Financing of Terrorism, Specified Payment Services**, 2 April 2024, last revised 30 June 2025, paragraphs 2 to 18, mas.gov.sg
- **Guidelines to MAS Notice PSN01**, last revised 1 July 2025, paragraphs 7-12 and 7-14, mas.gov.sg
- **FAQs on the Payment Services Act 2019**, revised 19 April 2024, questions 32, 36, 38, 51 and 52, mas.gov.sg
- **Circular MAS/PD/2024/10/04, Anti-scam measures by Major Payment Institutions that issue personal payment accounts containing e-money**, 25 October 2024, mas.gov.sg
- **Guidelines on Shared Responsibility Framework**, MAS, paragraph 1.1 and definitions, mas.gov.sg
- **MAS and IMDA announce implementation of Shared Responsibility Framework from 16 December 2024**, media release, 24 October 2024, mas.gov.sg
- **Written reply to Parliamentary Questions on the Shared Responsibility Framework and real-time fraud detection**, 3 February 2026, mas.gov.sg
- **MAS Imposes Composition Penalties against Five Major Payment Institutions**, 27 June 2025, mas.gov.sg
- **Samlit Moneychanger Pte. Ltd., its Director and Compliance Manager to be Charged for Offences Under the Financial Services and Markets Act 2022**, 9 July 2026, mas.gov.sg
- **MAS Revokes the Major Payment Institution License of Sir Money Changer Pte Ltd**, 14 October 2026, mas.gov.sg
- **Consultation on Expanding FIDReC Membership to Payment Service Providers**, P017-2026, 16 October 2026, mas.gov.sg

- **MAS Consults on Legislative Amendments to Implement Stablecoin Regulatory Framework**, media release, 1 September 2026, [mas.gov.sg](https://www.mas.gov.sg)
- **Financial Services and Markets (Amendment) Bill 2026, Second Reading Speech**, 6 October 2026, [mas.gov.sg](https://www.mas.gov.sg)
- **MAS/TCRS/2025/06, Cyber Risks Associated with Deepfakes**, 18 September 2025, [mas.gov.sg](https://www.mas.gov.sg)
- **Joint press release by SPF, MAS, IMDA and GovTech on restricting access to facilities for scam mules**, 17 September 2025, [mas.gov.sg](https://www.mas.gov.sg)
- **Targeted Financial Sanctions: Lists of Designated Individuals and Entities**, MAS, [mas.gov.sg](https://www.mas.gov.sg)
- **Suspicious Transaction Reporting (CDSA section 45; TSOFA sections 8 and 10)**, Singapore Police Force, [police.gov.sg](https://www.police.gov.sg)
- **Countering the financing of terrorism**, Ministry of Home Affairs, updated 30 January 2026, [mha.gov.sg](https://www.mha.gov.sg)
- **Advisory Guidelines on the PDPA for NRIC and other National Identification Numbers**, PDPC, issued 31 August 2018 (cover note December 2024), paragraphs 2.4, 3.1, 3.2 and 4.1, [pdpc.gov.sg](https://www.pdpc.gov.sg)
- **Joint Advisory against using NRIC Numbers for Authentication**, PDPC and CSA, issued June 2025, updated May 2026, [csa.gov.sg](https://www.csa.gov.sg)
- **Mutual Evaluation of Singapore**, FATF-APG, May 2026, chapter 1 (paragraph 66), chapter 3 (paragraph 216) and Recommendation 14, via Ministry of Law AML/CFT/CPF resources, acd.mlaw.gov.sg