Identomat

COMPLIANCE GUIDE

# Banking & Digital Banking Compliance in Singapore

COUNTRY Singapore

INDUSTRY Banking & Digital Banking

LAST UPDATED 28 October 2026

KEY REGULATORS Monetary Authority of Singapore · Suspicious Transaction Reporting Office

## Key takeaways

- Taking deposits or lending as a bank in Singapore needs a licence from the MAS, the single regulator for all banks. MAS is not currently granting new digital-only bank licences, so most new entrants operate as a wholesale bank, a merchant bank or a partner of an existing bank.
- Every bank must identify each customer, check that identity against reliable, independent sources and finish the check before the account is opened. A bank may delay the check only in limited cases where the risk is managed.
- Opening an account through an app or website is allowed. The checks must be at least as strong as in a branch, and the bank must add steps to stop impersonation, such as an initial deposit from the customer's account at another Singapore bank.
- Online banking carries extra anti-scam duties: a cooling-off period of at least 12 hours after a new digital security token is set up, real-time alerts, a self-service "kill switch" and real-time fraud monitoring. A bank that breaches these duties is expected to cover the customer's phishing losses.
- Penalties are criminal fines of up to S$1 million per breach of the anti-money laundering rules. In July 2025 MAS fined six banks and three other firms S$27.45 million in total over one money laundering case.

---

Singapore is open to banking businesses, including digital ones, but entry is tightly controlled. The Monetary Authority of Singapore licenses full banks, wholesale banks and merchant banks, writes the binding anti-money laundering rules (MAS Notice 626) and supervises them. Suspicious transaction reports go to the Suspicious Transaction Reporting Office of the Singapore Police Force.

The biggest obstacle for a new entrant is the licence itself. The four digital bank licences awarded in 2020 are fully allocated and MAS is not taking new applications, so a retail digital proposition generally needs an existing licensed bank behind it. Once licensed, the main operational burden is customer due diligence that holds up under MAS examination, especially on source of wealth and transaction monitoring.

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 banks | Level | Official site |
|---|---|---|---|
| Monetary Authority of Singapore (MAS) | Bank licensing and supervision; AML/CFT Notices and Guidelines; targeted financial sanctions; outsourcing, technology risk and anti-scam rules | National | mas.gov.sg |
| Suspicious Transaction Reporting Office (STRO), Singapore Police Force | Financial intelligence unit; receives suspicious transaction reports through SONAR | National | police.gov.sg |
| Ministry of Home Affairs (MHA) | Protection from Scams Act 2025; Police restriction orders to banks | National | mha.gov.sg |
| Singapore Deposit Insurance Corporation (SDIC) | Deposit Insurance Scheme for member banks and finance companies | National | sdic.org.sg |
| Personal Data Protection Commission (PDPC) | Personal Data Protection Act 2012, including rules on NRIC numbers | National | pdpc.gov.sg |
| Accounting and Corporate Regulatory Authority (ACRA) | Registers of registrable controllers (beneficial ownership) of companies and LLPs | National | acra.gov.sg |

## 2 Licensing and authorisation

Under section 4 of the Banking Act 1970, banking business (receiving money on current or deposit account, paying and collecting cheques, and making advances to customers) may be carried on in Singapore only by a company holding a bank licence from MAS. Using the word "bank" also needs a licence or MAS consent (section 5).

| Authorisation | What it allows | Capital entry test |
|---|---|---|
| Full bank | Universal banking, including deposit taking, lending and other MAS-regulated business | Locally incorporated: paid-up capital and capital funds of at least S$1,500 million; branch: head office capital funds of at least S$200 million equivalent (Banking Act s 9) |
| Wholesale bank | Full bank activities except Singapore dollar retail banking | Banking Act s 9 applies to all bank licences |
| Digital full bank or digital wholesale bank | Full or wholesale bank licence with the same scope and rules; two of each issued in 2020; MAS is not granting new licences | As for full and wholesale banks once fully functioning; under MAS's 2019 framework a digital full bank started in a restricted phase with S$15 million paid-up capital and a S$50 million aggregate deposit cap |
| Merchant bank | Activities set by Banking Act s 55V | Merchant bank licence |
| Finance company | Deposit taking and lending to individuals and companies | Licensed under the Finance Companies Act |

Wholesale and merchant bank applicants need home-supervisor consent and a sound group track record; the fee is S$20,000 and processing typically takes three to four months.

Carrying on banking business without a licence is an offence under section 4(2): up to S$125,000 or three years' imprisonment, or both, for an individual, and up to S$250,000 for any other person, with daily fines of S$12,500 or S$25,000 for continuing offences.

## 3 AML, KYC and customer due diligence

Every bank in Singapore is subject to MAS Notice 626 on Prevention of Money Laundering and Countering the Financing of Terrorism, issued under section 16 of the Financial Services and Markets Act 2022. The current Notice is dated 28 March 2024, in force from 1 April 2024 and last revised on 30 June 2025, with the latest amendments effective from 1 July 2025. The Notice is binding; the Guidelines to Notice 626 set out MAS's supervisory expectations.

### When customer due diligence is required

A bank must perform CDD when it:

- establishes business relations with any customer;
- undertakes a transaction above S$20,000 for a customer without an account;
- effects or receives a domestic wire transfer, or a cross-border wire transfer above S$1,500, for a customer without an account;
- undertakes any digital token transaction or value transfer for a customer without an account;
- suspects money laundering or terrorism financing, or doubts information obtained earlier.

### Beneficial owners

For legal persons a bank must identify the natural persons who ultimately own the customer, then those who control it, then those with executive authority, applying each step only if the previous one does not identify anyone (paragraph 6.14; Guidelines 6-8-1). The Guidelines give more than 25% ownership as an example threshold, and a person below it who controls the customer is still a beneficial owner. The bank must take reasonable steps to verify each beneficial owner. Since 1 July 2025, for lower-risk customers, date of birth, nationality and business address may replace an unobtainable identification number or home address (paragraph 6.14C). Listed companies on the Singapore Exchange and certain regulated institutions are exempt from the beneficial ownership inquiry (paragraph 6.16). Companies and limited liability partnerships must also keep registers of registrable controllers and file them with ACRA's central register, but a bank's own identification duty is not replaced by that filing.

### Enhanced and simplified measures

For politically exposed persons, their family members and close associates, the bank must obtain senior management approval, establish source of wealth and source of funds, and

apply enhanced monitoring (paragraph 8.3). Customers from jurisdictions subject to FATF countermeasures are automatically higher risk (paragraph 8.6).

### Monitoring, screening and reporting

Banks must monitor relationships on an ongoing basis and keep CDD data up to date (paragraphs 6.19 to 6.24). Customers, their representatives, connected parties and beneficial owners must be screened against relevant sources and official lists at onboarding, periodically, and whenever the lists or the people change (paragraphs 6.39 to 6.42). MAS publishes the lists of individuals and entities designated under targeted financial sanctions and expects screening against United Nations lists before doing business. Suspicious transactions, including attempted ones, must be reported to STRO promptly and regardless of amount (paragraph 14.2). The statutory reporting duty is in section 45 of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992, and reports are filed electronically through SONAR. SONAR cash transaction reports apply to precious stones and metals dealers, not banks.

### Records

CDD records, account files and analysis must be kept for at least five years after the relationship ends, and transaction records for at least five years after completion (paragraph 12.3). Records may be kept in electronic form provided they are admissible as evidence in a Singapore court (paragraph 12.4).

## 4 Identity verification and onboarding

For an individual, the bank must obtain full name and any aliases, a unique identification number (such as an identity card, birth certificate or passport number), residential address, date of birth and nationality (paragraph 6.6). It must then verify identity "using reliable, independent source data, documents or information" (paragraph 6.9). The rule is technology-neutral: the Notice does not list approved methods, name a digital identity scheme or set a liveness standard.

The Guidelines describe what MAS treats as good evidence. The best documents are those most difficult to obtain illicitly or counterfeit, such as government-issued identity cards and passports (Guidelines 6-3-1). Identity documents should carry a clear photograph, and address may be verified from an identity card, a recent bill, a bank statement or government correspondence (6-6-1, 6-6-2). Documents must be legible, which MAS stresses matters most without face-to-face contact (6-6-8).

### Timing

Verification of the customer, any person acting for it and its beneficial owners must be completed before business relations are established (paragraph 6.32). Deferral is allowed only where it is essential to normal business and the risks are managed (paragraphs 6.33 and 6.34). If CDD cannot be completed, the bank must not open or continue the relationship and must consider filing a suspicious transaction report (paragraphs 6.35 and 14.3).

### Reliance and outsourcing

A bank may rely on CDD performed by another financial institution supervised to FATF standards, but may never rely on a third party for ongoing monitoring, must immediately obtain the CDD information, and remains responsible (paragraphs 9.2 to 9.5). Using an identity verification vendor is outsourcing, not reliance: the vendor works under the bank's own policies (Guidelines 9-1 to 9-3).

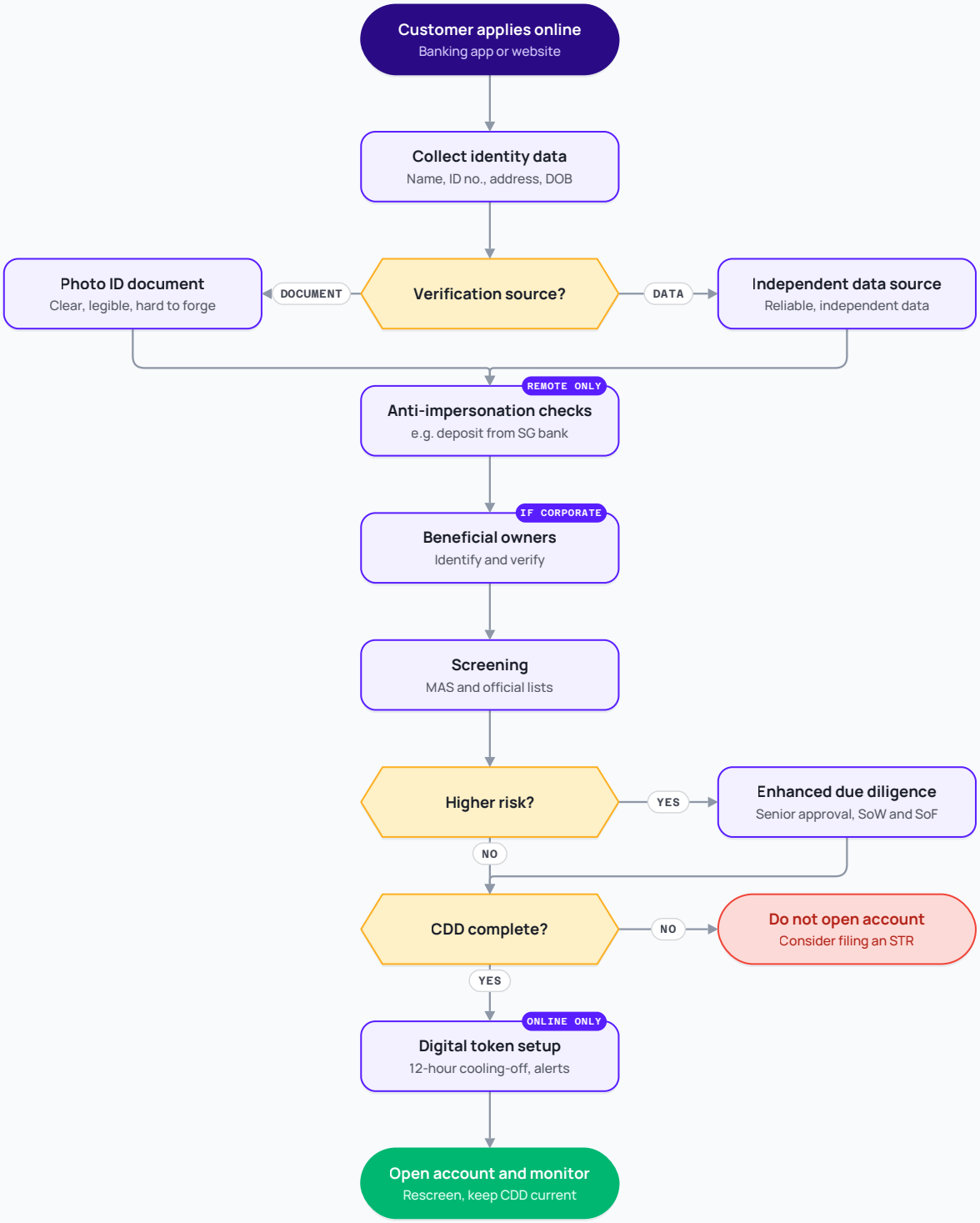



Figure 1. Remote account opening for an individual or corporate customer at a Singapore bank under MAS Notice 626.

## 5 Digital channels: what's different

**Bottom line:** the CDD rules are channel-neutral, but remote onboarding requires its own documented policies and extra anti-impersonation checks, and online banking adds scam-control duties (cooling-off, alerts, kill switch, fraud surveillance) that have no branch equivalent.

| Requirement | In person / branch | Online / remote | Difference |
|---|---|---|---|
| **Remote account opening** | Standard CDD | Permitted; specific non-face-to-face policies required (6.27, 6.28) | Differs |
| **Identity data collected** | Name, ID number, address, date of birth, nationality | Same five items (6.6) | Same |
| **Verification standard** | Reliable, independent source (6.9) | At least as robust as face to face (6.29) | Same |
| **Anti-impersonation checks** | Not specified | Additional checks expected (Guidelines 6-11-3) | Differs |
| **When verification is completed** | Before account opening (6.32) | Before account opening (6.32) | Same |
| **Screening** | Onboarding, periodic, list changes | Same (6.39, 6.40) | Same |
| **New digital token or device** | Not applicable | 12-hour cooling-off, real-time alerts (SRF 4.2.1, 4.2.2) | Differs |
| **Liability for phishing losses** | Not covered | Bank bears loss if it breached SRF duties | Differs |
| **Record keeping** | 5 years | 5 years; electronic records accepted if admissible (12.3, 12.4) | Same |

### Risk treatment of remote onboarding

Notice 626 does not classify remote onboarding as automatically higher risk. Instead, the Guidelines note that internet applications may pose greater risk because of easy unauthorised access, multiple fictitious applications at no cost, the absence of physical documents and the speed of electronic transactions, and say verification measures depend on the product and the customer's risk profile (Guidelines 6-11-1, 6-11-2). Where verification is done without face-to-face contact, for example electronically, the bank should add checks against impersonation. Examples include a call to an independently verifiable number, certified documents, or an initial deposit from the customer's account at another Singapore bank (Guidelines 6-11-3). New delivery channels and technologies must be risk-assessed before launch (paragraph 5).

### Digital token setup and Singpass Face Verification

The Guidelines on Shared Responsibility Framework (effective 16 December 2024) require a cooling-off period of at least 12 hours, during which high-risk activities cannot be performed, after a digital security token is activated on a device, plus real-time notifications of token activation, high-risk activities and outgoing transactions. In September 2024 MAS and the banking association announced that major retail banks would use Singpass Face Verification, a face scan checked against national records, in higher-risk scenarios before a digital token can be activated.

### Fraud surveillance and the kill switch

These duties apply to "protected accounts": payment accounts held by individuals or sole proprietors that can hold more than S$1,000 or are credit facilities. Banks must offer a reporting channel available at all times with a self-service feature to block mobile and online access. Since 16 June 2025 they must also run real-time fraud surveillance: where an account with a balance of S$50,000 or more loses more than half of it within 24 hours, the bank must block further payments to the scammer until it verifies with the customer, or notify the customer and hold the payments for at least 24 hours. If a bank breaches any of these duties in a covered phishing scam, it is expected to bear the full loss.

## 6 Data protection and biometrics

The Personal Data Protection Act 2012 (PDPA), administered by the PDPC, applies to the identity data, document images and face images a bank collects; other written law prevails where inconsistent (section 4(6)). For anti-money laundering purposes, Notice 626 lets a bank collect, use and disclose personal data, directly or through a third party, without

consent, and limits access and correction rights to core identification data (paragraphs 13.2 to 13.4). The PDPA still requires reasonable security arrangements (section 24), deletion once retention serves no legal or business purpose (section 25), which for CDD records means after the five-year minimum, and comparable protection for transfers abroad (section 26). The PDPC's biometric guide (May 2022), written for security applications, treats a face template held without identifying information as anonymised data but still expects safeguards where re-identification is possible; it reserves guidance on other commercial uses, including onboarding, for later.

Banking secrecy adds a stricter layer: customer information may be disclosed only as the Banking Act allows (section 47). Its Third Schedule permits disclosure solely to perform outsourced operational functions, subject to MAS's conditions, which is the route for sharing data with an identity verification provider.

Under the PDPC's Advisory Guidelines on NRIC numbers, organisations may collect NRIC numbers or copies of the NRIC only where the law requires it or identity must be verified to a high degree of fidelity; financial transactions are given as an example. A joint PDPC and Cyber Security Agency advisory of 26 June 2025 (updated 7 May 2026) tells organisations not to use NRIC numbers for authentication.

## 7 Sector-specific obligations

### Correspondent banking and wire transfers

A bank providing correspondent services to a foreign institution must assess the respondent, document responsibilities and obtain senior management approval, and must not deal with a shell financial institution (paragraphs 10.3 to 10.6). Wire transfer information requirements become fuller above S$1,500, and every originator and beneficiary must be screened (paragraphs 6.41 and 11).

### Outsourcing and technology

MAS Notice 658, effective 11 December 2024, governs outsourced relevant services at full and wholesale banks; its Annex A expressly lists name screening for AML/CFT or KYC purposes and due diligence on potential customers. Notices FSM-N05 and FSM-N06 (both effective 10 May 2024) require banks to notify MAS within one hour of a relevant IT incident, limit critical-system downtime to four hours a year, protect customer information, and use multi-factor authentication for administrative accounts and for systems that access customer information over the internet.

### Scam controls and information sharing

Under the Protection from Scams Act 2025, in force since 1 July 2025, the Police may direct banks to restrict a scam victim's transfers, withdrawals and credit facilities. An order lasts up to 30 days and may be extended up to five times; banks complying with reasonable care and in good faith are immune from liability (sections 4, 5 and 9). COSMIC, launched by MAS on 1 April 2024 with six major commercial banks, lets participants share information on customers showing multiple red flags.

### Deposit insurance

If a Deposit Insurance Scheme member bank or finance company fails, a depositor's insured deposits with that member are aggregated and insured up to S$100,000 by SDIC.

## 8 Risk indicators and red flags

**BANKING RED FLAGS (GUIDELINES TO MAS NOTICE 626, APPENDIX B, AND MAS ENFORCEMENT FINDINGS)**

- **Reluctant applicant**: minimal, false or hard-to-verify information at account opening.
- **Pass-through activity**: funds withdrawn immediately after deposit, or high velocity with low balances.
- **Dormant account revival**: a quiet account suddenly receiving or paying out large sums.
- **Income mismatch**: large deposits inconsistent with the customer's salary or business.
- **Third-party flows**: many unrelated payers, or third parties repaying the customer's loans.
- **Uncorroborated source of wealth**: discrepancies between stated wealth and independent sources, the main failing MAS found in the 2023 case.

## 9 Enforcement and penalties

MAS also uses composition penalties (sums paid to settle an offence without prosecution), reprimands and prohibition orders.

| Breach | Provision | Maximum penalty |
|---|---|---|
| Failing to comply with an MAS AML/CFT Notice, CDD or record-keeping duty | Financial Services and Markets Act 2022, s 16(4) | S$1 million per offence, plus S$100,000 a day for continuing offences after conviction |
| Failing to report knowledge or suspicion to STRO | CDSA s 45(3) | Individual: S$250,000 or 3 years, or both; others: S$500,000 |
| Money laundering | CDSA s 54(5), (7) | Individual: S$500,000 or 10 years, or both; others: S$1 million or twice the value of the benefits, whichever is higher |
| Disclosing customer information outside permitted cases | Banking Act 1970, s 47(6) | Individual: S$125,000 or 3 years, or both; others: S$250,000 |
| Intentional or negligent breach of data protection obligations | Personal Data Protection Act 2012, s 48J | 10% of Singapore turnover where it exceeds S$10 million; otherwise S$1 million |

On 4 July 2025 MAS imposed composition penalties totalling S$27.45 million on nine financial institutions linked to the August 2023 money laundering case. The six banks paid between S$1 million (LGT Bank) and S$5.8 million (Credit Suisse Singapore Branch); United Overseas Bank paid S$5.6 million. MAS found weak customer risk rating, source of wealth corroboration and alert review. In March 2026 MAS barred two former relationship managers convicted in the same case for 16 and 7 years. The 2026 FATF evaluation called MAS's financial sanctions insufficiently dissuasive.

## 10 Recent changes and what to watch

- **30 September 2026**: MAS consults on amendments to corporate governance regulations for banks, including board composition and approval of key appointments. `Proposed, comments close 9 Dec 2026`
- **6 May 2026**: FATF and the Asia/Pacific Group published Singapore's mutual evaluation, rating it Substantial for financial supervision and preventive measures and Moderate for beneficial ownership transparency. `Published`
- **6 March 2026**: MAS consulted on Guidelines on Third-Party Risk Management, including a register of third-party arrangements. `Proposed, consultation closed 20 Apr 2026` Notice 658 continues to apply meanwhile.

- **1 July 2025**: Amendments to MAS Notice 626 took effect, including proliferation financing in scope and alternatives to identification numbers and residential addresses for lower-risk beneficial owners. `In force` Update CDD data rules and documentation.
- **1 July 2025**: Protection from Scams Act 2025 commenced. `In force` Banks receiving restriction orders must restrict the named individual's facilities.
- **16 June 2025**: Real-time fraud surveillance duty under the Shared Responsibility Framework applies. `In force` Account-draining patterns must be blocked or held.
- **11 December 2024**: MAS Notice 658 on outsourced relevant services took effect. `In force` Identity verification vendors must be managed under it.

## 11 What this means for identity verification

- **Documents**: no method is prescribed, but government photo identity cards and passports are MAS's benchmark, captured legibly with tamper checks.
- **Remote onboarding**: add a documented anti-impersonation layer on top of document or data verification.
- **Timing**: do not issue a usable account before verification completes.
- **Re-verification**: doubts about earlier data, suspicion, list updates and changes of representatives or owners trigger new checks; higher-risk token setups may require face verification.
- **NRIC, retention and vendors**: collect the NRIC number for CDD, never use it to authenticate, keep evidence for at least five years, and treat identity providers as outsourcing.

IDENTOMAT

## 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:

- ID document capture and verification, including NFC chip reading, to check identity against reliable, independent sources before the account opens.
- Biometric liveness and face match as an added anti-impersonation layer for non-face-to-face onboarding.
- KYB and beneficial owner verification for corporate customers, with an audit trail for each step.
- AML screening against sanctions, PEP and adverse-media lists at onboarding, with ongoing monitoring and rescreening when lists change.
- A no-code workflow builder with cloud, on-premises or hybrid deployment to fit outsourcing and data-location requirements.

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

- **MAS Notice 626, Prevention of Money Laundering and Countering the Financing of Terrorism – Banks**, dated 28 March 2024, last revised 30 June 2025, paragraphs 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, mas.gov.sg
- **MAS Notice 626 amendment notes (June 2025)**, amendments effective 1 July 2025, mas.gov.sg
- **Guidelines to MAS Notice 626**, 28 March 2024, revision published 30 June 2025 and in effect from 1 July 2025, paragraphs 6-3, 6-6, 6-8, 6-11, 9-1 to 9-3, Appendix B, mas.gov.sg
- **MAS, Anti-Money Laundering** (penalties under the Financial Services and Markets Act 2022), mas.gov.sg

- **Banking Act 1970** (2020 Revised Edition, current version as at 28 October 2026), sections 2, 4, 5, 9, 47 and Third Schedule, Part 1 item 3, Singapore Statutes Online, sso.agc.gov.sg
- **Financial Services and Markets Act 2022**, section 16, sso.agc.gov.sg
- **Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992**, sections 45 and 54, sso.agc.gov.sg
- **Personal Data Protection Act 2012**, sections 4(6), 24, 25, 26 and 48J, sso.agc.gov.sg
- **Protection from Scams Act 2025**, sections 4, 5 and 9, sso.agc.gov.sg
- **MAS, Types of Deposit-Taking Institutions**, mas.gov.sg
- **MAS, Licensing and Authorisation for Banking Business**, mas.gov.sg
- **MAS, Digital Bank Licence**, mas.gov.sg
- **MAS, Guidelines on Shared Responsibility Framework**, issued 24 October 2024, effective 16 December 2024, sections 4 and 6, mas.gov.sg
- **MAS, Combatting Scams**, mas.gov.sg
- **MAS–ABS media release, Major retail banks to introduce Singpass Face Verification**, 18 September 2024, mas.gov.sg
- **MAS, COSMIC**, mas.gov.sg
- **MAS Notice 658, Management of Outsourced Relevant Services for Banks**, effective 11 December 2024, Annex A, mas.gov.sg
- **MAS Notice FSM-N05, Technology Risk Management**, issued 9 May 2024, effective 10 May 2024, paragraphs 5 to 9, mas.gov.sg
- **MAS Notice FSM-N06, Cyber Hygiene**, issued 9 May 2024, effective 10 May 2024, paragraph 4.6, mas.gov.sg
- **MAS, E-Payments User Protection Guidelines**, version effective 16 December 2024 (last revised 25 October 2024), definition of "protected account", mas.gov.sg
- **MAS, Operational Resilience** (Consultation Paper P004-2026 on Guidelines on Third-Party Risk Management, 6 March 2026), mas.gov.sg
- **MAS Consultation Paper P016-2026 on Amendments to Corporate Governance Regulations for Banks, Insurers and Designated Financial Holding Companies**, 30 September 2026, mas.gov.sg
- **MAS, Lists of Designated Individuals and Entities**, mas.gov.sg
- **MAS, Regulatory actions against 9 financial institutions for AML-related breaches**, 4 July 2025, mas.gov.sg
- **MAS, Key Enforcement Actions Taken by MAS in Q1 2026**, 1 April 2026, mas.gov.sg
- **MAS, Capital Asia Investments enforcement operation**, March 2026 (penalty provisions), mas.gov.sg
- **Singapore Police Force, Suspicious Transaction Reporting**, police.gov.sg
- **MHA, Commencement of the Protection From Scams Act**, 30 June 2025, mha.gov.sg

- **MHA, Singapore has a robust framework for combatting financial crime according to international body**, 6 May 2026, mha.gov.sg
- **FATF and APG, Mutual Evaluation Report of Singapore**, 2026, Key Recommended Actions and Chapter 3 (IO.3), published via Ministry of Law AML/CFT/CPF resources, acd.mlaw.gov.sg
- **Singapore Police Force, SONAR** (report types filed with STRO), police.gov.sg
- **SDIC, Deposit Insurance Scheme**, sdic.org.sg
- **PDPC media release, PDPC issues NRIC Advisory Guidelines**, 31 August 2018, with factsheet, pdpc.gov.sg
- **PDPC, Advisory Guidelines on the Personal Data Protection Act for NRIC and Other National Identification Numbers**, issued 31 August 2018 (cover note: remain valid pending update following MDDI's 13 December 2024 statement), Part II, pdpc.gov.sg
- **MAS, Eligibility Criteria and Requirements for Digital Banks**, 2019, section III, mas.gov.sg
- **PDPC, Guide on Responsible Use of Biometric Data in Security Applications**, 17 May 2022, Introduction and Part I, pdpc.gov.sg
- **CSA and PDPC, Joint Advisory Against Using NRIC Numbers for Authentication**, 26 June 2025, updated 7 May 2026, csa.gov.sg
- **ACRA, Register of Registrable Controllers**, updated 6 March 2026, acra.gov.sg