



Identomat

COMPLIANCE GUIDE

eCommerce & Marketplaces Compliance in Singapore

COUNTRY **Singapore**

INDUSTRY **eCommerce & Marketplaces**

LAST UPDATED **28 October 2026**

KEY REGULATORS **Singapore Police Force · Ministry of Home Affairs · Competition and Consumer Commission of Singapore**

Key takeaways

- Marketplaces and online shops in Singapore do not need a general licence to operate, and are not covered by the anti-money laundering (AML) customer due diligence rules that banks follow. The exceptions are specific goods, such as liquor and precious stones and metals.
 - The binding identity rule comes from anti-scam law. Platforms designated by the Police under the Online Criminal Harms Act must verify sellers and advertisers against government-issued records, and must meet strengthened requirements by 31 January 2027.
 - Every online marketplace is expected to check merchants against government records under the national e-commerce standard (TR 76), which is voluntary but is the benchmark the Government uses to rate platforms publicly.
 - Online sellers of liquor must take all reasonable steps to confirm buyers are 18 or older; this rule has applied to online and app sales since January 2024.
 - New penalties of up to S\$10 million per breach for designated platforms, and new offences for selling or lending marketplace accounts, were passed in September 2026 but are not yet in force.
-

The Singapore market is open to online marketplaces and e-retailers without a sector licence. What a platform must do about identity depends on its risk profile rather than a licence: the Singapore Police Force can designate high-risk e-commerce services and impose binding anti-scam codes, while every other platform is measured against a voluntary national standard and an annual public safety rating.

The principal authorities are the Ministry of Home Affairs and the Singapore Police Force (scams and online crime), the Competition and Consumer Commission of Singapore (consumer protection), the Inland Revenue Authority of Singapore (GST on marketplace sales) and the Personal Data Protection Commission (personal data, including national identity numbers).

The biggest obstacle for a new entrant is building seller verification that meets the Government's expectation of checks against government-issued records, while respecting strict limits on collecting national identity card (NRIC) numbers.

CONTENTS

- 1 Who regulates this sector
- 2 Licensing and authorisation
- 3 Identity framework (AML rules do not apply)
- 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 marketplaces and e-retailers	Level	Official site
Singapore Police Force, Online Criminal Harms Act Office	Competent Authority under the Online Criminal Harms Act 2023: designates online services, issues codes of practice and implementation directives	National	police.gov.sg
Ministry of Home Affairs (MHA)	Anti-scam policy, E-commerce Marketplace Transaction Safety Ratings, scam legislation	National	mha.gov.sg
Competition and Consumer Commission of Singapore (CCS)	Consumer Protection (Fair Trading) Act 2003, unfair practices, e-commerce guidance (TR 76)	National	ccs.gov.sg
Inland Revenue Authority of Singapore (IRAS)	GST registration and collection by overseas vendors and electronic marketplace operators	National	iras.gov.sg
Personal Data Protection Commission (PDPC)	Personal Data Protection Act 2012, NRIC number guidance	National	pdpc.gov.sg
Health Sciences Authority (HSA)	Health products sold online, including removal of illegal listings from e-commerce platforms	National	hsa.gov.sg

Online Safety Commission	Directions and identity disclosure for specified online harms under the Online Safety (Relief and Accountability) Act 2025	National	mlaw.gov.sg
Suspicious Transaction Reporting Office (STRO)	Singapore's financial intelligence unit; receives suspicious transaction reports from any business	National	police.gov.sg
Ministry of Law, AML/CFT Division	Registration and AML supervision of precious stones and precious metals dealers, including online dealers	National	acd.mlaw.gov.sg

2

Licensing and authorisation

No general licence is needed to run an online marketplace or shop. Obligations attach in three ways.

Designation under the Online Criminal Harms Act

The Online Criminal Harms Act 2023 lets the Competent Authority in the Singapore Police Force designate online services and apply codes of practice. Designation is risk-based: Carousell, Facebook Marketplace and Facebook Business Pages are designated under the Code of Practice for E-Commerce Services as the highest e-commerce scam risks. Designated providers may appeal to the Minister for Home Affairs against designation, against the application of a code or against a specific requirement.

Product licences that follow the goods online

Some goods carry a licence regardless of channel. Any person or business supplying liquor, including an online retailer or an e-commerce platform that allows users to sell liquor, must hold a liquor licence under section 4(1) of the Liquor Control (Supply and Consumption) Act 2015, according to the Singapore Police Force's guidance. Dealers in precious stones, precious metals and precious products must register with the Registrar of Regulated Dealers under the Precious Stones and Precious Metals (Prevention of Money Laundering, Terrorism Financing and Proliferation Financing) Act 2019; a foreign dealer must register if it carries on business in Singapore for more than 90 days in a calendar year, and must meet the transaction-based requirements either way (Ministry of Law guide for foreign dealers, July 2025).

Tax registration

Under the overseas vendor registration regime, overseas businesses with global turnover above S\$1 million that make more than S\$100,000 a year of business-to-consumer supplies of remote services or low-value goods to Singapore must register for GST under a simplified pay-only regime. An electronic marketplace operator may be treated as the supplier of low-value goods sold through its marketplace by local and overseas sellers, and must then charge GST on those sales. Low-value goods are goods valued at no more than S\$400, delivered to Singapore by air or post (IRAS, overseas businesses page).

3

Identity framework (AML rules do not apply)

Online marketplaces and e-retailers are not among the sectors subject to AML/CFT customer due diligence notices or directives in Singapore. The Suspicious Transaction Reporting Office's list of reporting industries with sector AML rules covers financial institutions, casinos, real estate, corporate service providers, pawnbrokers, moneylenders and precious stones and metals dealers, but not general e-commerce. Identity obligations for marketplaces instead come from anti-scam law and consumer protection guidance (section 4).

Suspicious transaction reporting applies to everyone

Anyone who, in the course of trade, profession, business or employment, knows or has reasonable grounds to suspect that property may be connected to criminal activity must file a suspicious transaction report with STRO through its SONAR platform (section 45 of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992). Failure to file may be an offence.

Terrorism financing information

Every person in Singapore must give the Police information about terrorist property and terrorism financing transactions under sections 8 and 10 of the Terrorism (Suppression of Financing) Act 2002; this can be done through a suspicious transaction report.

Online precious stones and metals dealers

Regulated dealers, including those selling online, must perform customer due diligence (CDD) and file a cash transaction report within 15 business days for cash or cash-equivalent transactions above S\$20,000, keep CDD records for five years, and must not proceed if CDD cannot be completed (Ministry of Law).

A marketplace that collects and pays out funds itself may be providing payment services under the Payment Services Act 2019, such as merchant acquisition or account issuance, which need a Monetary Authority of Singapore (MAS) licence and bring payment-sector AML rules into scope. On 23 September 2024 MAS directed Qoo10, a marketplace operating under a transitional exemption, to suspend its covered payment services after delays in paying merchants.

4

Identity verification and onboarding

Binding seller verification for designated platforms

The Code of Practice for E-Commerce Services (section 21(1)(b) of the Online Criminal Harms Act 2023), in operation from 17 August 2026, requires designated providers to:

- subject users who advertise or post about the sale of goods or services, or intend to, to verification against government-issued records (requirement B7);
- verify advertisers' identities against government-issued records, including business registration records and identification documents, before they may publish advertisements (B6);
- put in place reasonable verification measures against inauthentic, bot-controlled or compromised accounts, and run additional verification when suspicious activity is detected or reported by the Police or users (B1, B2);
- require login verification, require the account holder's consent before a login from a new or unrecognised device, and offer a "verified" account status backed by stronger checks (B3 to B5);
- offer users an optional payment protection mechanism that releases payment to the seller only after delivery is verified (C1).

Each requirement must be implemented within six months of the date in the provider's Code Application Notice. The Singapore Police Force has set 31 January 2027 as the compliance date for the designated platforms, and may grant full or partial waivers based on each service's assessed risk.

Calibrated application in practice

Under the 2024 code, MHA let designated services verify only selected sellers at first. In March 2025 it decided not to mandate verification of all Facebook Marketplace sellers after reported scams there fell by about 55%. In November 2025 MHA reported scammers using Singpass-verified Carousell accounts obtained by phishing, purchase or stolen Singpass credentials; Carousell committed to passkey and biometric logins and to blacklisting Singpass credentials linked to scam accounts. The 2026 code keeps the calibrated approach. MHA waived the payment protection requirement under the 2024 code; the 2026 code restates it as requirement C1.

The benchmark for every other platform

Technical Reference 76 (TR 76), the national guidelines for e-commerce transactions, was enhanced on 26 September 2025. It recommends verifying merchants against government records or internal business tools, enhanced verification or suspension when fraud is detected, keeping account and transaction records, and answering regulatory requests within 24 hours. TR 76 is voluntary, but MHA's annual E-commerce Marketplace Transaction Safety Ratings score major marketplaces on user authenticity, meaning whether sellers' identities are verified, preferably against government-issued documentation.

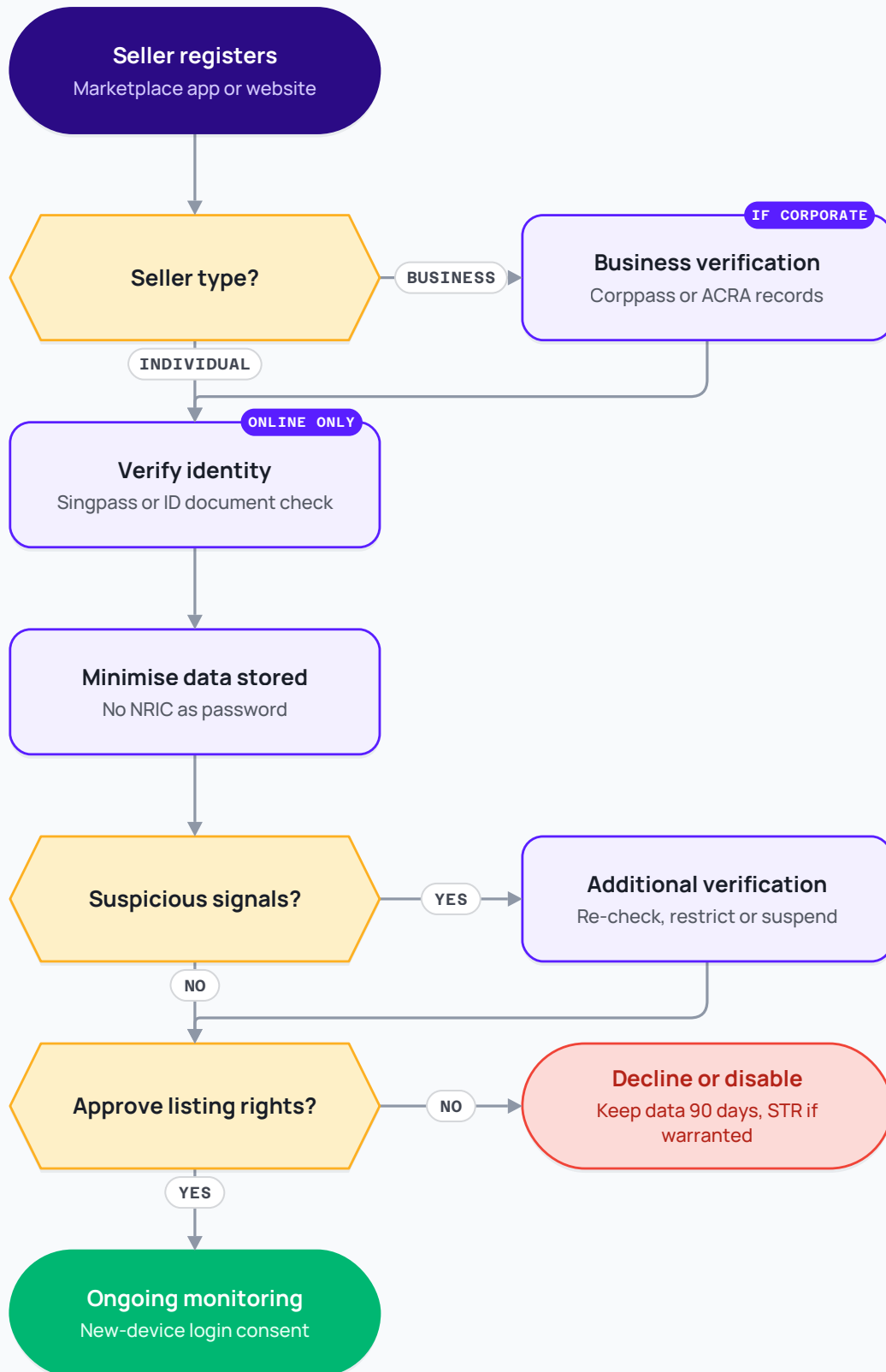


Figure 1. Seller onboarding on a marketplace designated under the Online Criminal Harms Act.

Age checks for restricted goods

Since 2 January 2024, regulation 11 of the Liquor Control (Supply and Consumption) (Liquor Licensing) Regulations 2015 prohibits licensees from supplying liquor to anyone under 18 online or through a telecommunication service. A licensee selling through a third-party platform must not do so if it knows, or ought reasonably to know, that the platform does not take all reasonable steps to ascertain that buyers are 18 or older and warn them of the offence and penalty. Police guidance gives examples of reasonable steps: a buyer declaration of age, a warning that buying under 18 is an offence, and information on the penalty.

5

Digital channels: what's different

Bottom line: Singapore imposes seller identity checks specifically on online platforms through anti-scam law; a physical shop has no equivalent duty to verify the people it trades with.

Requirement	In person / physical retail	Online / marketplace	Difference
Seller or advertiser verification	No general duty	Against government-issued records on designated platforms; recommended for all by TR 76	Differs
Account security	Not applicable	Login verification and consent for new-device logins on designated platforms	Differs
Liquor age check	No sale to under-18s at licensed premises	No sale to under-18s; platforms must take all reasonable steps and display warnings	Differs
Response to scam reports	No specific duty	Assess and act on user reports within 24 hours on designated platforms	Differs
Data retention for investigations	No specific duty	At least 90 days for accounts flagged by the Police on designated platforms	Differs

Suspicious transaction reporting	Required in the course of business	Required in the course of business	Same
Unfair practices (CPFTA)	Prohibited	Prohibited	Same
Precious stones and metals CDD	Cash or equivalent above S\$20,000	Cash or equivalent above S\$20,000	Same
NRIC collection limits	Apply	Apply	Same

Verification attaches to selling, not buying

The E-Commerce Code requires verification of users who advertise or post sales, not of every buyer.

Account security is now part of compliance

The enhanced code requires consent before a login from a new or unrecognised device and encourages multi-factor or biometric authentication.

Pending changes

The Scams (Countermeasures) and Other Matters Act 2026

Adopted, effective date not yet set will criminalise supplying or buying accounts on designated online services for unlawful purposes and let the Police order account disabling and disclosure.

6 Data protection and biometrics

The Personal Data Protection Act 2012 governs the collection of seller and buyer identity data. Two pieces of PDPC guidance shape onboarding design.

NRIC numbers and copies. Under the PDPC's Advisory Guidelines on NRIC and other national identification numbers, applied from 1 September 2019, organisations may collect, use or disclose NRIC numbers or copies of the NRIC only where required by law or where necessary to establish or verify identity to a high degree of fidelity, with notification and consent. The same treatment extends to birth certificate, foreign identification and work permit numbers, and physical identity documents may be retained only where the law

requires. Collecting a copy of the NRIC means collecting all the personal data on it, and passport numbers should be treated similarly. A partial number limited to the last three digits and checksum is not treated as a full NRIC number. The PDPC does not treat sighting an ID card, without keeping it or recording data, as collection; its own example is checking a buyer's date of birth for an age-restricted purchase.

No NRIC-based authentication. 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, because the numbers must be assumed to be known to others. The advisory lists biometrics among the options for authentication when chosen on a risk basis.

Facial images and other biometric data captured during verification are personal data, so PDPA consent, purpose, protection and retention obligations apply. Designated platforms must nonetheless keep data on accounts flagged by the Police for at least 90 days.

7 Sector-specific obligations

Anti-scam controls beyond verification

Designated e-commerce services must proactively act against scams and compromised, inauthentic or bot-controlled accounts; remove impersonation content; review advertisements before publication, including for URL cloaking; and refuse advertisements for financial services or products unless the advertiser is licensed by the Monetary Authority of Singapore or another Singapore authority, or authorised by a licensed entity. They must provide a fast-track channel for law enforcement and submit an annual implementation report to the Competent Authority.

Consumer protection and fair dealing with merchants

The Consumer Protection (Fair Trading) Act 2003, administered by CCS, protects consumers against unfair practices, whether they transact online or offline (Ministry of Trade and Industry, March 2024). The enhanced TR 76 adds guidance on accurate listings, fake reviews, misleading interfaces such as subscription traps, and fair treatment of merchants.

Health products listed online

The Health Sciences Authority (HSA) states that it is illegal to sell prescription medicines, unregistered or professional-use medical devices, and adulterated health products on

local e-commerce platforms, and that contact lenses may not be sold online. HSA removed 2,358 illegal listings in 2025, most on Shopee, Lazada and TikTok.

Disclosure of user identity for online harms

Since 29 June 2026, the Online Safety Commission can require platforms to provide the identity information of end-users who committed specified online harms, such as their name or contact details, and victims may apply for disclosure for purposes such as bringing a court claim. The first phase covers intimate image abuse, image-based child abuse, doxxing, online harassment and online stalking. Platforms must also take reasonable measures to address specified harms on notice.

8 Risk indicators and red flags

E-COMMERCE SCAM AND IDENTITY-ABUSE INDICATORS (MHA AND SINGAPORE POLICE FORCE)

- **Unverified seller accounts:** MHA notes scammers are more likely to list goods from accounts not verified by the platform.
- **Off-platform payment requests:** sellers steering buyers to PayNow or bank transfers instead of the platform's secured payment option.
- **Moving the conversation:** buyers or sellers asking to continue on WhatsApp or Telegram, a feature of the Carousell fake-buyer phishing variant reported from July 2026.
- **Fake invoices and payment links:** PDFs resembling platform invoices with QR codes leading to cloned platform and bank sites.
- **Misused verified accounts:** Singpass-verified accounts taken over by phishing, bought from users, or verified with stolen Singpass credentials.
- **Impersonation:** listings, pages or advertisements using the likeness of public figures, brands or verified businesses.
- **Cloaked advertisement URLs:** destination links hidden or changed during an advertisement's lifecycle.
- **Unlicensed financial offers:** advertisements for investment products from advertisers not licensed in Singapore.

9 Enforcement and penalties

Regime	Penalty structure	Basis
Online Criminal Harms Act codes (current)	Non-compliance leads to a Rectification Notice; failing to comply with it without reasonable excuse is an offence under section 51(3), fine up to S\$1 million plus up to S\$100,000 per day for a continuing offence	Per notice, after conviction
Online Criminal Harms Act codes (passed, not yet in force)	Administrative penalty up to S\$10 million per instance of non-compliance, or a Rectification Notice or Compliance Order; failing to comply is an offence with a fine up to S\$10 million plus S\$300,000 per day	Per instance
Supplying or receiving designated online accounts for crime, new sections 39GA and 39GB of the Miscellaneous Offences Act (passed, not yet in force)	Individuals up to S\$10,000 and/or 3 years (repeat: S\$20,000 and/or 5 years); others up to S\$20,000 (repeat: S\$40,000); up to 12 strokes of the cane where the individual knew the account would be used for a scam	Per offence
Liquor supplied online to under-18s	Fine up to S\$10,000 for breach of regulation 11	Per breach
Personal Data Protection Act, section 48J	Financial penalty up to S\$1 million or 10% of annual Singapore turnover (where turnover exceeds S\$10 million), whichever is higher	Per intentional or negligent contravention
Health Products Act (illegal health products sold online)	Adulterated or counterfeit products: up to S\$100,000 and/or 3 years; HSA cites up to S\$50,000 and/or 2 years for other illegal import, manufacture or supply	Per offence, on conviction

The Online Criminal Harms Act's directive power was first used against Meta on 24 September 2025 (facial recognition against impersonation scams on Facebook) and extended on 27 January 2026. The Singapore Police Force has assessed that designated services complied with the 2024 codes. The PDPC fined Carousell S\$58,000 in December 2023 after an API flaw exposed non-public user data later offered for sale (about 2.6 million records), citing inadequate pre-launch testing and documentation.

Recent changes and what to watch

- **9 September 2026:** Parliament passed the Scams (Countermeasures) and Other Matters Bill **Adopted, effective date not yet set**. Once the Minister notifies commencement, platforms face penalties of up to S\$10 million per breach; earlier breaches stay under the old regime.
- **17 August 2026:** Enhanced Code of Practice for E-Commerce Services issued **Partly in force**. The code operates from 17 August 2026, but designated platforms have until 31 January 2027 to implement new-device login consent and advertisement safeguards.
- **29 June 2026:** Online Safety Commission began operations **In force**. Platforms can be required to disclose the identity of users who commit specified online harms.
- **27 January 2026:** Second Implementation Directive to Meta **In force**. Shows the Government's readiness to mandate biometric controls on specific platforms.
- **21 November 2025:** MHA concluded Carousell's verification pilot **In force**. Verified-account takeover and resale is now the key risk regulators expect platforms to control.
- **26 September 2025:** Enhanced TR 76 published **In force**. Voluntary, but sets the merchant verification benchmark used to rate marketplaces.
- **10 March 2025:** MHA decided not to require verification of all Facebook Marketplace sellers **Optional relief**. Verification of selected sellers remains acceptable while scam numbers stay down.

What this means for identity verification

Verify sellers against government-issued records: Singpass and Corppass for local individuals and businesses, ACRA records for companies, and document verification with forgery detection for overseas sellers. Let Police notifications, user reports or internal detection trigger re-verification, suspension or restriction.

Keep the data footprint small. Collect NRIC numbers or images only where a high degree of identity fidelity is genuinely needed, never use them as passwords or authenticators, and avoid storing identity documents unless the law requires it. For age-restricted goods such as liquor, an age check that does not retain document data fits PDPC guidance.

Treat account security as part of identity: consent for new-device logins, passkey or biometric login options, and re-verification when account details change, so a verified account cannot simply be taken over or sold. Plan retention so that data on accounts flagged by the Police is kept for at least 90 days.

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:

- Seller onboarding with ID document capture and verification, face match and biometric liveness for sellers who cannot use Singpass.
- KYB and beneficial owner verification for corporate merchants before they list or advertise.
- Age verification for age-restricted goods such as liquor, configurable to minimise stored identity data.
- Ongoing monitoring and re-verification triggered by suspicious activity, with an audit trail for each check.
- No-code workflow builder to apply risk-based verification to selected or all sellers as requirements change.

[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

- **Code of Practice for e-Commerce Services (with effect from 17 August 2026)**, issued under section 21(1)(b) of the Online Criminal Harms Act 2023, Singapore Police Force, [police.gov.sg](https://www.police.gov.sg)
- **Codes of Practice and designated online services**, Singapore Police Force, [police.gov.sg](https://www.police.gov.sg)
- **Issuance of Codes of Practice under the Online Criminal Harms Act**, Singapore Police Force news release, 18 August 2026, [police.gov.sg](https://www.police.gov.sg)
- **Assessment of Carousell's and Meta's Enhanced Verification Measures under the E-commerce Code**, MHA, 10 March 2025, [mha.gov.sg](https://www.mha.gov.sg)

- **Second Reading of the Scams (Countermeasures) and Other Matters Bill**, opening speech, MHA, 8 September 2026, mha.gov.sg
- **Scams (Countermeasures) and Other Matters Act 2026 (No. 21 of 2026)**, sections 16 (new sections 39GA to 39GC of the Miscellaneous Offences (Public Order and Nuisance) Act 1906), 21, 23, 27 and 33, published in the Acts Supplement on 29 September 2026, sso.agc.gov.sg
- **Issuance of Implementation Directive to Meta under the Online Criminal Harms Act**, MHA, September 2025, mha.gov.sg; second directive, 29 January 2026, mha.gov.sg
- **E-commerce Marketplace Transaction Safety Ratings 2025**, MHA press release, mha.gov.sg
- **Enhanced E-commerce Guidelines to Safeguard Consumer Trust and Foster Competitive E-commerce Market (TR 76)**, joint media release, 26 September 2025, ccs.gov.sg
- **Consumer Protection (Fair Trading) Act 2003**, Singapore Statutes Online, sso.agc.gov.sg
- **Overseas businesses: GST and the digital economy**, IRAS, iras.gov.sg
- **New Requirements to Regulate Supply of Liquor Online or through Telecommunication Services**, Singapore Police Force, 18 November 2023, police.gov.sg
- **FAQ on the Liquor Control (Supply and Consumption) (Liquor Licensing) Regulations**, Singapore Police Force, police.gov.sg
- **Suspicious Transaction Reporting**, section 45 CDSA and sections 8 and 10 TSOFA, Singapore Police Force, police.gov.sg
- **Transaction-Based Requirements for regulated dealers**, Ministry of Law AML/CFT Division (updated 23 October 2026), acd.mlaw.gov.sg
- **PDPC Issues NRIC Advisory Guidelines**, media release and factsheet, 31 August 2018, pdpc.gov.sg
- **Joint Advisory against using NRIC Numbers for Authentication**, PDPC and CSA, issued June 2025, updated May 2026, csa.gov.sg
- **Online Safety Commission and Online Safety (Relief and Accountability) Act 2025 to start on 29 June 2026**, MinLaw and MDDI, 14 May 2026, mlaw.gov.sg
- **Police Advisory on Phishing Scams Involving Fake Buyers on Online Marketplace**, Singapore Police Force, 23 October 2026, police.gov.sg
- **Enhanced Verification Measures by Carousell under the E-Commerce Code**, MHA, 21 November 2025, mha.gov.sg
- **Advisory Guidelines on the PDPA for NRIC and other National Identification Numbers** (issued 31 August 2018; cover note confirms they remain valid pending update), PDPC, pdpc.gov.sg
- **Advisory Guidelines on Enforcement of the Data Protection Provisions** (revised 1 October 2022), paragraph 27.1, PDPC, pdpc.gov.sg
- **Carousell Pte. Ltd. [2023] SGPDP 13**, PDPC decision, 28 December 2023, pdpc.gov.sg
- **HSA Removes over 1,200 Online Listings of Illegal Health Products**, HSA, 26 June 2025, hsa.gov.sg; **HSA Seized Over 1 Million Illegal Health Products and Removed More Than 2,300 Online Listings in 2025**, HSA, 24 March 2026, hsa.gov.sg

- **MAS Directs Qoo10 Pte Ltd to Suspend Provision of Covered Payment Services in Singapore**, MAS media release, 23 September 2024, [mas.gov.sg](https://www.mas.gov.sg)
- **Guide for Foreign Dealers of Precious Stones, Precious Metals and Precious Products**, Ministry of Law (updated 2 July 2025), acd.mlaw.gov.sg
- **How to identify adulterated, counterfeit and substandard health products**, HSA, 9 April 2026, hsa.gov.sg
- **Written reply to PQ on consumer protection for e-commerce marketplace**, Ministry of Trade and Industry (now METI), 1 March 2024, meti.gov.sg