



Identomat

COMPLIANCE GUIDE

Telecom & Mobile Services Compliance in Singapore

COUNTRY **Singapore**

INDUSTRY **Telecom & Mobile Services**

LAST UPDATED **28 October 2026**

KEY REGULATORS **Infocomm Media Development Authority · Singapore Police Force · Personal Data Protection Commission**

Key takeaways

- Anyone selling mobile, internet or other telecom services in Singapore needs a licence from the Infocomm Media Development Authority (IMDA). A virtual mobile operator renting another carrier's network needs an individual services-based licence.
- Telecom companies are not covered by Singapore's anti-money laundering (AML) rules. Their identity duties come from licence conditions instead: check an official identity document before activating a SIM card, keep a copy and keep the customer record for at least 12 months.
- Signing up customers online requires Singpass, the national digital identity. Prepaid customers must be at least 15, and each person may hold at most 3 prepaid and 10 postpaid SIM cards across all operators.
- Since 1 January 2025 it is a crime for an operator, a retailer or their staff to register a SIM card with someone else's details, or with false details, when they know or have reason to believe it will be misused.
- Mobile operators carry anti-scam duties of their own: blocking text messages from unregistered senders and filtering malicious links. An operator that fails these duties can be expected to repay a customer's phishing losses. A new law passed in September 2026 will also let the Police order operators to disable lines or refuse service to named people, from a date still to be set.

Singapore is open to new telecom entrants, including fully digital mobile brands, but entry is licensed and identity rules are strict. IMDA licenses and supervises operators, while the Ministry of Home Affairs and the Singapore Police Force enforce the criminal offences that target misuse of SIM cards.

The biggest practical obstacle for a new entrant is the anti-scam regime. Registration limits are counted per person across every operator, people dealt with as scam mules can be barred from new lines, and both online and in-store channels must produce a verified, auditable record of who holds each number.

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

Telecommunications is regulated nationally. IMDA licenses operators under the Telecommunications Act 1999 and sets subscriber registration rules through licence conditions and directions. Several other authorities shape how operators identify customers.

Authority	Remit for telecom identity	Level	Official site
Infocomm Media Development Authority (IMDA)	Licensing, SIM registration conditions, SIM limits, anti-scam directions to operators	National	imda.gov.sg
Ministry of Digital Development and Information (MDDI)	Policy ministry for IMDA; anti-scam policy for calls and messages	National	mddi.gov.sg
Singapore Police Force (SPF) and Ministry of Home Affairs (MHA)	SIM card misuse offences, facility restrictions on scam mules, suspicious transaction reports	National	police.gov.sg
Monetary Authority of Singapore (MAS)	Co-owner with IMDA of the Shared Responsibility Framework for phishing losses	National	mas.gov.sg
Personal Data Protection Commission (PDPC)	Personal data rules, including collection of identity card numbers	National	pdpc.gov.sg
Cyber Security Agency of Singapore (CSA)	Cybersecurity guidance, including the advisory against authenticating people by identity card number	National	csa.gov.sg

IMDA's guidelines state that under the Telecommunications Act 1999 any person operating and providing telecommunication systems and services in Singapore must be licensed.

IMDA uses two tiers. A facilities-based operations licence covers anyone deploying its own network, including mobile base stations. A services-based operations licence covers operators that lease network elements from a licensed facilities-based operator or resell its services.

Services-based licences

Services-based licences come in two categories. Individual licences are required for, among others, mobile virtual network operation, IP telephony, machine-to-machine services and prepaid services. Class licences cover lighter services such as some internet-based voice and data services and require only registration. Under IMDA's Guidelines for Submission of Application for Services-Based Operations Licence (version 5b, 20 June 2022):

- there is no foreign equity limit, but the licensee must be a company incorporated, or a foreign company registered, under the Companies Act 1967;
- individual licences run for five years and are renewable; IMDA aims to award them within 14 working days of a complete application;
- the annual fee is S\$4,000 on the first S\$50 million of annual gross turnover, 0.5% on turnover between S\$50 million and S\$100 million, and 0.8% above that;
- individual licensees that collect deposits or issue prepaid cards need paid-up capital of at least S\$100,000, and class licensees may not collect deposits or use prepaid cards at all.

Facilities-based licences

Facilities-based licences are individually negotiated. A licence IMDA issued in February 2023 illustrates the terms: a 15-year period, an annual fee of at least S\$80,000 rising to 0.8% and then 1% of turnover above S\$50 million and S\$100 million, a performance bond, and the same subscriber and retailer registration conditions as the services-based template where mobile virtual network services are licensed. There is no separate digital telecom licence: an operator that sells only through an app needs the licence matching its service.

Identity framework (AML rules do not apply)

Telecom operators are not designated financial institutions and are not subject to an AML notice of the kind MAS issues to banks and payment firms. There is no customer due diligence regime in the financial sense, no risk rating requirement and no beneficial ownership check imposed by AML law on operators.

Identity obligations come instead from three sources:

Licence conditions

IMDA's services-based licence template (version 10, 1 December 2025) requires operators to verify identity documents, keep a register of subscribers and a register of retailers, and limit sales per person.

Criminal offences

Part 6A of the Miscellaneous Offences (Public Order and Nuisance) Act 1906 punishes subscribers, middlemen, retailers and licensees involved in SIM cards used for crime.

Anti-scam framework

IMDA directions under section 31 of the Telecommunications Act 1999, the Shared Responsibility Framework and the facility restriction framework for scam mules.

For a mobile virtual network operator, the licence requires a register of prepaid subscribers with name, address, identity number, contact details, service period and service identifiers such as the International Mobile Subscriber Identity (IMSI) and mobile number. A parallel register applies to postpaid subscribers, who must be registered before activation. Both registers are open to inspection by authorised government agencies and must be kept for at least 12 months after the service ends.

Identity verification and onboarding

Accepted documents

Before recording a prepaid subscriber bought in Singapore, a mobile virtual network operator must see the customer's identity card issued under the National Registration Act 1965 (or a uniformed services card), a passport, or one of nine listed passes, including the S Pass, Employment Pass, Dependant's Pass and Student's Pass, and must make and keep a photocopy. Postpaid customers must produce an identity card, passport or Employment

Pass, again with a copy kept. IMDA has also stopped the use of foreign passports to register postpaid SIM cards.

Age and quantity limits

Prepaid service may not be provided to anyone under 15. Each person may register at most 3 prepaid SIM cards across all operators, a limit in place since April 2014. From 28 February 2026, each person may register at most 10 postpaid SIM cards across all operators, replacing the April 2024 limit of 10 per operator. Corporate plans and data-only SIM cards that cannot call or send text messages are outside the postpaid limit. If a prepaid sale breaches the age rule or the limit, the licence requires the operator to terminate the service, where applicable within 14 days of the sale.

Retailers and record security

Prepaid service may be sold only through authorised retailers, and the operator must keep a register of every retailer and the numbers allocated to it. Electronic systems used to keep the registers, including retailers' systems, must comply with the ISO/IEC 27002 information security controls standard or an equivalent, and every access to a register must be logged with the user's name, user ID, employer and time.

Existing customers and vulnerable consumers

IMDA has issued Guidelines for Subscriber Verification Process to make operators' checks on account-specific requests more robust against identity theft, and expects operators to tighten processes against unauthorised and fraudulent access to accounts. Its Advisory Guidelines on the Protection of Vulnerable Consumers ask frontline staff to identify vulnerable consumers at face-to-face sign-up and handle suspected exploitation.

Restricted persons

Under the facility restriction framework, operational since October 2025, people warned, prosecuted or convicted for mule offences, and some under investigation, can be barred from subscribing to new mobile lines; from 1 July 2026 they can also be barred from using Singpass to register for mobile lines and other high-risk services. Onboarding flows need a step that honours these restrictions.

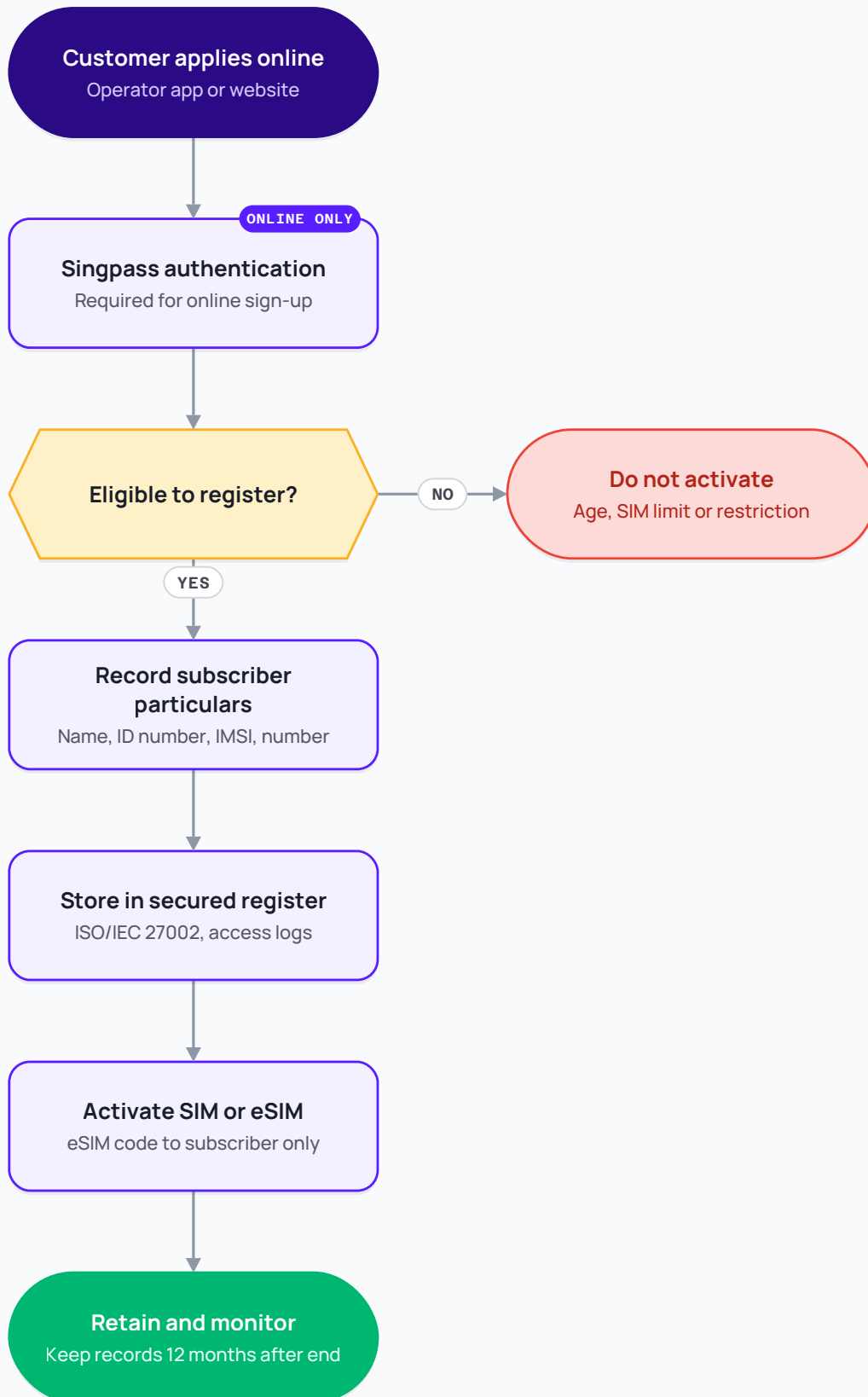


Figure 1. Online SIM or eSIM activation by a Singapore mobile operator.

Bottom line: the registration rules are largely channel-neutral, but online sign-up must run through Singpass, which in practice replaces the in-store document check and photocopy with a government-backed digital identity.

Requirement	In person / retail	Online / remote	Difference
How identity is established	Original document shown, photocopy kept	Singpass required for online registration	Differs
Foreign passport for postpaid	Not accepted	Not accepted	Same
SIM limits per person	3 prepaid, 10 postpaid across operators	3 prepaid, 10 postpaid across operators	Same
Minimum age (prepaid)	15	15	Same
Record retention	12 months after service ends	12 months after service ends	Same
Physical SIM and eSIM	Both are SIM cards in law	Handing over an eSIM code counts as providing the SIM	Same
Who can be liable for fraudulent registration	Retailer and its employees	Licensee and its employees	Same
Sales outside Singapore (overseas, in-flight)	Not applicable	Best-efforts check of locally recognised documents; records forwarded within 7 working days	Differs

Singpass as the online gate

IMDA's January 2026 announcement lists the requirement to use Singpass for online registration among the safeguards already in place, alongside government-issued identity documents and the bar on foreign passports for postpaid lines. The licence text itself describes document production and photocopying, so an online journey should be

designed to produce an equivalent auditable record of the verified identity. Since 1 July 2026, people under the facility restriction framework can be blocked from using Singpass to register mobile lines.

eSIM is treated as a SIM card

Part 6A defines a SIM card as prepaid or postpaid, physical or digital, issued with a Singapore number. Giving someone the code or link to download an eSIM counts as providing the SIM card.

6 Data protection and biometrics

The Personal Data Protection Act 2012 governs all collection of customer data. PDPC's Advisory Guidelines on NRIC and other national identification numbers generally bar organisations from collecting identity card numbers or copies of identity cards unless the law requires it or identity must be verified to a high degree of fidelity. PDPC's own illustration of the legal requirement is a mobile line: an operator may record or scan the customer's identity card because its licence conditions require a register of subscribers. Organisations must still protect that data properly. Separately, section 30 of the Telecommunications Act 1999 lets IMDA issue codes of practice on operators' collection, use and disclosure of subscriber information without consent.

Collecting a card number is not the same as using it to authenticate. In a joint advisory of 26 June 2025, last updated 7 May 2026, PDPC and CSA advise organisations against using identity card numbers for authentication. This matters for customer service flows, SIM replacement and number transfer requests, where knowing a customer's card number is not proof that the caller is that customer.

The SIM misuse offences define personal information broadly to include biometric data, signatures, authentication codes and passwords, so registering a SIM card with someone else's facial image or credentials falls within the offences.

7 Sector-specific obligations

SIM card misuse offences

Part 6A of the Miscellaneous Offences (Public Order and Nuisance) Act 1906, inserted by the Law Enforcement and Other Matters Act 2024, took effect on 1 January 2025. It creates offences for subscribers who hand over SIM cards or let their particulars be used, for

anyone who buys, sells, receives or possesses SIM cards registered to others or unregistered cards for crime, and, in section 39G, for a retailer or telecommunication licensee that registers a SIM card knowing or having reason to believe the person did not authorise it or that the information is false, where the card is meant for or used in crime. Employees acting in the course of employment are covered. Holding more than 10 such cards triggers a presumption of criminal intent. MHA noted that before these offences, operators could already be in breach of regulatory obligations if they or their retailers facilitated fraudulent registrations.

Anti-scam duties under the Shared Responsibility Framework

The MAS Guidelines on Shared Responsibility Framework, effective 16 December 2024, apply to mobile network operators providing cellular service. Their telecom duties are a subset of IMDA directions under section 31 of the Telecommunications Act 1999: deliver sender ID text messages only from authorised aggregators, block sender ID messages from any other source, and filter all text messages against a designated database of malicious links. Losses from covered phishing scams fall first on the bank or payment firm; the operator is expected to repay the customer if the financial institution met all its duties and the loss arose from the operator's breach. Claims must be investigated within 21 business days, or 45 for complex cases.

8

Risk indicators and red flags

SIM MISUSE AND IDENTITY ABUSE INDICATORS

- **Bulk applications:** one identity applying for many postpaid lines across retailers, the pattern IMDA cites for the 2026 limit.
- **Lines registered for others:** a subscriber who cannot say who uses the line or why.
- **Paid hand-overs:** offers of cash or credits in exchange for registering SIM cards.
- **Retailer pre-registration:** extra SIM cards registered with genuine customers' details without their knowledge.
- **Corporate line clusters:** rising numbers of scam lines registered by companies.
- **Repeat offenders:** applicants already dealt with for mule offences, who may be under a line prohibition.
- **Mismatched sign-up:** Singpass identity that does not match the delivery or payment details.

Enforcement and penalties

Under section 10 of the Telecommunications Act 1999, IMDA may issue a compliance order or impose a financial penalty of up to the higher of 10% of the annual turnover of the licensed business or S\$1 million for breach of a licence condition, code of practice or direction, and may suspend, cancel or shorten the licence. Failing to comply with a section 10 order is an offence carrying a fine of up to S\$100,000, three years' imprisonment, or both. In January 2024, IMDA imposed a S\$50,000 financial penalty on StarHub Mobile for failing to implement enhanced signalling controls required by an IMDA direction by the deadline, taking into account partial early implementation and its later efforts.

The SIM misuse offences carry criminal penalties that scale with the offender and repetition:

- individuals: a fine of up to S\$10,000, imprisonment of up to three years, or both;
- repeat offences by middlemen and by retailers or licensees under section 39G: up to S\$20,000, five years, or both;
- companies and other entities: up to S\$20,000, rising to S\$40,000 for repeat offences under sections 39D to 39G;
- from 30 December 2025, discretionary caning of up to 12 strokes for scam mules who provide SIM cards used for scams.

Corporate officers who consented to or connived in an offence, or failed to take reasonable steps to stop it, can be liable for the same offence. In March 2025, the Police raided three mobile phone shops and investigated ten people, including retailer staff suspected of using legitimate customers' details to pre-register additional prepaid SIM cards, under section 39G and other laws. The Police disrupted more than 47,500 scam-related mobile lines across all operators in the first half of 2026 and have said they will continue to act against errant retailers.

Recent changes and what to watch

- **9 September 2026** Passed, commencement date not yet set The Scams (Countermeasures) and Other Matters Bill lets the Police order telecom operators to disclose account information, disable lines for up to 30 days and restrict services to named persons for up to three years. Operators should prepare processes to receive and act on these orders.
- **1 July 2026** In force Facility restriction framework extended to block restricted persons from using Singpass to register mobile lines and other high-risk services.

- **28 February 2026** **In force** Postpaid limit of 10 SIM cards per person across all operators; onboarding must check the cross-operator count.
- **30 December 2025** **In force** Discretionary caning for scam mules who provide SIM cards, raising the stakes of subscriber hand-overs.
- **October 2025** **In force** Facility restriction framework: people dealt with as scam mules can be barred from new mobile lines.
- **1 January 2025** **In force** SIM misuse offences in Part 6A, including criminal liability for retailers and licensees.
- **16 December 2024** **In force** Shared Responsibility Framework, making operators liable for some phishing losses when they breach SMS duties.

11 What this means for identity verification

- **Document types:** in-store checks must accept the identity card, uniformed services cards, passports and the listed work and study passes for prepaid; postpaid is limited to the identity card, passport or Employment Pass, and foreign passports are refused.
- **Remote method:** online sign-up runs through Singpass; keep an auditable record of the verified identity that matches the register fields.
- **Eligibility checks:** confirm age 15 or over for prepaid, the 3 prepaid and 10 postpaid cross-operator limits, and any mobile line prohibition before activation.
- **eSIM delivery:** send activation codes only to the verified subscriber, since passing a code is providing a SIM card.
- **Retention and security:** keep registers at least 12 months after service ends, log every access and meet ISO/IEC 27002 or an equivalent.
- **Re-verification triggers:** SIM replacement, number transfer and changes of particulars should rely on stronger authentication than knowledge of an identity card number.

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 SIM and eSIM onboarding with ID document capture and verification, including NFC reading of passports.
- Face match and biometric liveness detection so the person activating a line is the document holder.
- Age verification to enforce the minimum age for prepaid service.
- Configurable no-code workflows with an audit trail of every check for subscriber register and inspection needs.
- Phone and email verification for re-authentication before SIM replacement or changes to particulars.

[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

- **Services-Based Operations (Individual) Licence template**, IMDA, version 10, 1 December 2025, conditions 17, 32 and Schedule B Annex 8, [imda.gov.sg](https://www.imda.gov.sg)
- **Guidelines for Submission of Application for Services-Based Operations Licence**, IMDA, version 5b, 20 June 2022, sections 1 to 4, [imda.gov.sg](https://www.imda.gov.sg)
- **Tightening of limit on number of postpaid SIM cards**, IMDA press release, 23 January 2026, [imda.gov.sg](https://www.imda.gov.sg)
- **Anti-scam efforts by MDDI**, Ministry of Digital Development and Information, last updated 18 August 2026, [mddi.gov.sg](https://www.mddi.gov.sg)

- **Response to Parliamentary Question on use of local SIM cards for scams**, MDDI, 8 April 2026, mddi.gov.sg
- **Law Enforcement and Other Matters Act 2024**, section 3 (inserting Part 6A, sections 39A to 39I, and sections 40A and 40B into the Miscellaneous Offences (Public Order and Nuisance) Act 1906), Singapore Statutes Online, sso.agc.gov.sg
- **Commencement of the Law Enforcement and Other Matters Act on 1 January 2025**, MHA press release, 30 December 2024, mha.gov.sg
- **Commencement of the Criminal Law (Miscellaneous Amendments) Act 2025**, MHA press release, 19 December 2025, mha.gov.sg
- **Guidelines on Shared Responsibility Framework**, MAS and IMDA, issued 24 October 2024, effective 16 December 2024, sections 1, 5, 6 and 7, mas.gov.sg
- **Restricting Access to Facilities for Scam Mules**, joint release by SPF, MAS, IMDA and GovTech, 17 September 2025, police.gov.sg
- **10 Persons Under Investigation for Fraudulent Registration of Prepaid SIM Cards**, SPF news release, 20 March 2025, police.gov.sg
- **Enforcement decision: StarHub Mobile Pte Ltd, contravention of Direction on Enhanced Signalling Controls**, IMDA, 24 January 2024, imda.gov.sg
- **PDPC Issues NRIC Advisory Guidelines (with factsheet)**, PDPC media release, 31 August 2018, Annex A, pdpc.gov.sg
- **Joint Advisory Against Using NRIC Numbers for Authentication**, PDPC and CSA, 26 June 2025, last updated 7 May 2026, csa.gov.sg
- **Telecommunications Act 1999 (2020 Revised Edition)**, sections 10, 30, 31 and 32, Singapore Statutes Online, sso.agc.gov.sg
- **Licence to Provide Facilities-Based Operations granted to Telekom Malaysia (S) Pte. Ltd.**, IMDA, issued 22 February 2023, conditions 1, 2, 6, 39 and Schedule C, imda.gov.sg
- **Codes of Practice and Guidelines: Infocomm (Guidelines for Subscriber Verification Process; Advisory Guidelines on the Protection of Vulnerable Consumers)**, IMDA, last updated 25 May 2026, imda.gov.sg
- **Mid-Year Scam and Cybercrime Brief 2026**, SPF, pages 11 to 14, police.gov.sg
- **First Reading of the Scams (Countermeasures) and Other Matters Bill**, MHA press release, 4 August 2026, mha.gov.sg
- **Second Reading of the Scams (Countermeasures) and Other Matters Bill**, wrap-up speech, MHA, 9 September 2026, mha.gov.sg
- **20th ASEAN Ministerial Meeting on Transnational Crimes: Singapore's Country Statement**, MHA, 20 October 2026, mha.gov.sg