Identomat

COMPLIANCE GUIDE

Telecom & Mobile Services Compliance in Australia

COUNTRY Australia

INDUSTRY Telecom & Mobile Services

LAST UPDATED 2 November 2026

KEY REGULATORS Australian Communications and Media Authority · Office of the Australian Information Commissioner · Australian Competition and Consumer Commission

Key takeaways

- A prepaid mobile service, including one sold online or as an eSIM, cannot be switched on until the customer's identity has been checked using one of the methods the telecoms regulator lists. Apart from a few narrow exceptions, there is no grace period.
- Online sign-ups can be verified against government databases, through a government-accredited Digital ID provider (allowed since 16 December 2025), or with a transaction on the customer's own bank or credit account. Identity documents and document numbers generally may not be recorded and kept.
- Before a SIM swap, a number transfer to another provider, or a change to account details, the telco must confirm the person asking is the real account holder, usually with a one-time code or secure link sent to the customer; SIM swaps and account changes also need knowledge checks.
- Telecoms providers are not covered by Australia's anti-money laundering law, but anti-scam duties are growing: telcos are a designated sector under the new Scams Prevention Framework, with its core obligations applying from 31 March 2027.
- Penalties rose on 27 October 2026: breaching the identity rules can now cost a company up to about $11 million per breach, or more if linked to turnover, and a new provider registration scheme must start by 26 October 2027.

Australia is open to new mobile providers, including mobile virtual network operators (MVNOs) and online-only brands. There is no licence for a carriage service provider (CSP) today, but the identity rules a provider must apply are detailed, prescriptive and actively enforced.

The Australian Communications and Media Authority (ACMA) writes and enforces the identity rules. The Office of the Australian Information Commissioner (OAIC) oversees how identity data and biometrics are handled, and the Australian Competition and Consumer Commission (ACCC) is the general regulator of the new scams framework.

The main compliance build for a new entrant is two separate identity controls set out in detail in the rules: a fixed list of verification methods at activation, and strict authentication before every SIM swap, port or account change, with records that prove each step.

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

The identity rules covered in this guide are Commonwealth (federal) laws and instruments.

Regulator	Remit	Level	Official site
Australian Communications and Media Authority (ACMA)	Makes and enforces service provider determinations and industry standards (prepaid ID checks, customer identity authentication, pre-porting verification); registers industry codes; sector regulator for telecommunications under the Scams Prevention Framework	Federal	acma.gov.au
Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts	Telecommunications policy and legislation	Federal	infrastructure.gov.au
Office of the Australian Information Commissioner (OAIC)	Privacy Act 1988, including biometric data used for verification	Federal	oaic.gov.au

Attorney-General's Department	Administers the Identity Verification Services Act 2023 and the government Document Verification Service used for online document checks	Federal	ag.gov.au
Australian Competition and Consumer Commission (ACCC)	General regulator of the Scams Prevention Framework (all provisions except sector codes)	Federal	accc.gov.au

The Telecommunications Industry Ombudsman handles consumer complaints, and the Communications Access Co-ordinator gives the ACMA its views on whether alternative prepaid identity arrangements meet law enforcement needs.

2 Licensing and authorisation

Carriers need a carrier licence under Part 3 of the Telecommunications Act 1997. Retail providers, including MVNOs that resell another carrier's network, are carriage service providers and currently need no licence, but must comply with every service provider determination, industry standard and registered industry code that applies to them (Telecommunications Act 1997 ss 101 and 128, Compilation No. 117, and s 121 as amended on 27 October 2026).

Carriage service provider registration `Adopted, commences by 26 Oct 2027`

The Telecommunications Amendment (Enhancing Consumer Safeguards) Act 2026 (Act No. 99, 2026, assented 26 October 2026) inserts a new Division 3A into the Telecommunications Act. Once Schedule 1 commences (on a date fixed by Proclamation, or otherwise on 26 October 2027), a registrable CSP must not supply or offer a listed carriage service to the public unless it is registered with the ACMA (new s 96A). Carriers and wholesale providers must not supply listed services to an unregistered registrable CSP (s 96B), subject to limited exceptions.

3 Identity framework (AML rules do not apply)

Supplying phone, SMS or internet services is not a designated service under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Compilation No. 63, 1 October 2026, s 6), so a telco is not an AML/CTF reporting entity for its

telecommunications business. A telco that provides a designated service listed in s 6 is a reporting entity in respect of that service.

Customer identity in telecommunications is instead governed by three ACMA instruments made under the Telecommunications Act:

Prepaid Determination

Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2017, Compilation No. 1 (16 December 2025). Identity checks before a prepaid mobile service is activated.

CIA Determination

Telecommunications Service Provider (Customer Identity Authentication) Determination 2022, in force since 30 June 2022. Authentication before high-risk customer transactions on phone and internet services (account-managed and integrated business customers are excluded, s 4).

Pre-Porting Standard

Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020, in force since 30 April 2020. Verification before a mobile number is ported to a new provider.

The Prepaid Determination serves law enforcement while limiting data collection to the minimum (s 2.1); the other two instruments protect customers from fraud and account takeover. These instruments impose no beneficial ownership, transaction monitoring or suspicious matter reporting duty; a customer acting for a business gives the business name and address instead of a residential address (s 4.3).

Using or disclosing customer information outside the statutory exceptions is an offence punishable by up to 2 years' imprisonment (Telecommunications Act s 276).

4 Identity verification and onboarding

Prepaid activation

A CSP must not activate a prepaid mobile service until it has collected the required information and verified the customer (Prepaid Determination ss 2.3 and 4.2). "Activate" means enabling any use beyond communications with the provider and calls to an

emergency call service (s 1.5). For a service activator the CSP must collect name, date of birth and residential address (or, if acting for an entity, the entity's name and business address) (s 4.3), then verify using one of nine approved methods in Schedule 1:

Schedule 1 method	What it requires
Government online verification service	Document number, issuer and any required dates matched against the issuing agency's records
Existing post-paid account	Account details plus proof of being the account holder, such as a valid password
White-listed email service	Confirmation of an active ".edu.au" or ".gov.au" email address
Real-time financial transaction	Transaction on the customer's bank or credit card account returning a transaction code; no financial disadvantage to the customer
Time-delayed financial transaction	Account transfer; one service only, temporarily activated; deactivated within one day if not confirmed within two business days
Existing eligible prepaid account (with or without direct debit)	An account the provider previously verified; without direct debit, the service must be no more than 24 months old and the customer must end up with fewer than 5 services activated this way
Visual identity document check	1 category A document or 2 different category B documents; 2 category A, or 1 category A and 2 category B, if the customer will have 5 or more active prepaid services
Government-accredited Digital ID service `In force since 16 Dec 2025`	Customer consent and verification by an accredited entity, or by an identity service provider working through one, under the Digital ID Act 2024

Category A documents include a passport, an Australian licence or permit, a tertiary student card, a birth certificate and a government benefit statement; category B documents include a debit or credit card, a Medicare card and a post-paid phone bill or rates notice under 12 months old (s 1.8). A purchaser who pays by debit or credit card, and will hold fewer than 5 services, needs no document check (s 4.4). Alternatively, a CSP may follow an ACMA-approved compliance plan (Part 5). Narrow exceptions allow activation at the moment a real-time payment confirms a direct debit account (s 4.2(2)) and Part 3

exempts services for people displaced by emergencies or family violence (30 days unless the ACMA approves longer).

Authentication after onboarding

Before the first high-risk transaction, such as a SIM swap, change of account details, adding an authorised representative or a large one-off charge, a CSP must confirm the requester is the customer (CIA Determination s 8). Where the customer starts the interaction, the CSP needs two knowledge checks (account security information or personal details) plus one of: proof of direct access to the service or listed number, a one-time code or secure link carrying prescribed warning text, biometrics, a category A photo document compared with the person's face in person or over a live audio-visual link, or a cryptographic key (s 9). If those fail, a fraud-trained staff member must use documents, two government documents checked online, or a government-accredited digital identity service, and notify the customer (s 10).

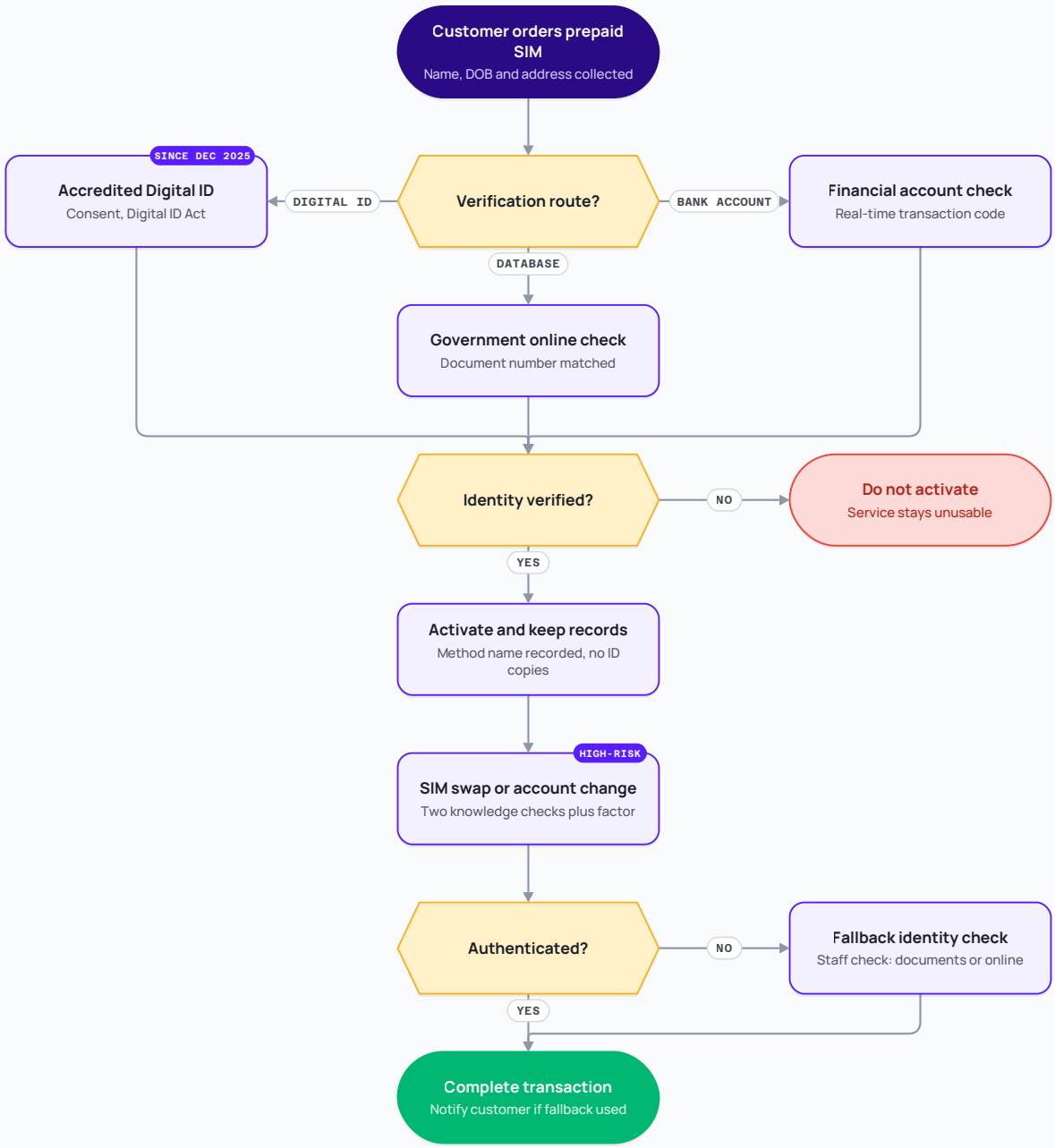


Figure 1. Online prepaid SIM or eSIM activation and later SIM-swap authentication in Australia.

Number porting

Before porting a mobile number in, the gaining provider must confirm the requester is the rights of use holder, by confirming access to a device using the number, a one-time code sent by SMS to that number, or biometrics (Pre-Porting Standard s 8(2)). If none of these works (the standard gives a lost phone as an example), it may use category A and B documents or two government documents checked online (s 8(3) and (4)). The port must not proceed until one of these processes is complete (s 8(5)).

5 Digital channels: what's different

Bottom line: the activation rule is the same in a shop and online (no activation before verification). Every activation must use a Schedule 1 method or an ACMA-approved compliance plan, and Schedule 1 does not list document-and-selfie capture as a method in its own right.

Requirement	In person / retail	Online / remote	Difference
Verification before activation	Required	Required	Same
Approved verification methods	Any Schedule 1 method or an approved compliance plan	Same list; Schedule 1 methods are not limited by channel	Same
Copies of ID documents	Must not be copied or kept	Must not be copied or kept; document number held only until verification completes	Same
Authentication for SIM swap	In-store call to the number, or photo ID face comparison	One-time code or secure link with warning text, biometrics, or face comparison by live video	Same
Port-out protection	Call to the number in store	SMS one-time code to the number	Same
Record retention	Prepaid records while service active; authentication records at least one year	Same periods	Same

Remote prepaid activation methods

For the visual identity document check, item 8 requires the customer to "show" the documents; the 2017 explanatory statement describes them as "sighted". Neither the Determination nor ACMA guidance states whether documents may be shown over a video call, and the ACMA had not addressed the point as of October 2026. The CIA Determination, by comparison, expressly allows a face-to-photo check "in person or by live audio-visual link" (Schedule 1, clause 4). A method outside Schedule 1 requires an ACMA-

approved compliance plan (s 2.3): the ACMA found 18,388 contraventions by Telstra (November 2024 to February 2025) for using an accredited Digital ID exchange before Schedule 1 listed it.

Data minimisation applies online too

A provider must not record and keep the identifying number of a government document, or a category A or B document, nor copy such documents (s 6.4(1) and (4)). Exceptions apply where a law requires or authorises the recording, and where the number is held only to help a customer complete a government online check and destroyed immediately after verification.

Account security in app and web channels

Every one-time code or secure link must warn that a high-risk interaction has started and say what to do if the customer did not start it; if the customer reports it, the provider must stop or reverse the transaction (CIA Determination s 9(3) and (5)). Customers at risk of fraud must get extra protections, such as pausing high-risk transactions (s 13).

6 Data protection and biometrics

The Privacy Act 1988 and the Australian Privacy Principles apply alongside the telecommunications rules; industry codes and standards do not override them (Telecommunications Act s 116A). From 27 October 2026 the ACMA must consult the Information Commissioner before enforcing a code breach that relates to a privacy matter (new Telecommunications Act s 121A).

Both the CIA Determination and the Pre-Porting Standard allow biometric data, defined as measurable biological or behavioural characteristics such as face, fingerprints or voice. The OAIC's guide on facial recognition technology (29 July 2026) treats biometric templates and facial images used for automated verification as sensitive information, generally needing valid consent, and recommends a privacy impact assessment. From 10 December 2026, APP entities' privacy policies must describe certain automated decisions that could significantly affect individuals.

Government document checks run under the Identity Verification Services Act 2023, whose participation agreements require the individual's express consent (s 7).

Retention is set by purpose: prepaid activation records for as long as the service is active (Prepaid Determination s 6.1), authentication records for at least one year (CIA Determination s 16). Separately, carriers and internet service providers operating

infrastructure in Australia must keep subscriber identification information until 2 years after the account closes (Telecommunications (Interception and Access) Act 1979 ss 187A, 187AA and 187C).

7 Sector-specific obligations

Scams Prevention Framework Partly in force

The Scams Prevention Framework Act 2025 inserted Part IVF into the Competition and Consumer Act 2010. Voice call and message services supplied over a listed carriage service were designated a regulated sector by an instrument made on 22 May 2026, with the ACMA as sector regulator (Competition and Consumer (Scams Prevention Framework–Regulated Sectors) Designation 2026, ss 13 and 14). Until 31 March 2027 only the sector code provisions and the external dispute resolution provisions (membership from 1 September 2026) apply to telcos (s 102). From 31 March 2027 the governance, prevent, detect, report, disrupt and respond principles apply in full. The ACCC is the framework's general regulator (s 58EB). Breaching the prevent, detect, disrupt or respond principles can cost a company the greater of 159,745 penalty units, three times the benefit, or 30% of adjusted turnover (s 58FK).

Registered industry codes now binding

From 27 October 2026, every participant in a section of the industry covered by a registered code must comply with it (new s 121); previously the ACMA had to direct compliance first. Registered codes include the Reducing Scam Calls and Scam SMs code (C661:2022), the Mobile Number Portability code (C570:2024) and the Telecommunications Consumer Protections Code (C628:2019).

Verifying businesses that send SMS under a sender ID

Under the Telecommunications (SMS Sender ID Register) Industry Standard 2025, a certified provider registering a sender ID for a customer must first confirm the requester's identity using an identity verification service, confirm they are an authorised representative, confirm the entity is officially recognised, and match the sender ID to an official register (ss 11 and 12, in force since 30 November 2025).

8 Risk indicators and red flags

MOBILE NUMBER FRAUD INDICATORS DRAWN FROM ACMA RULES AND INVESTIGATIONS

- **Unsolicited one-time codes**: a customer reports codes they did not request; in the Telstra case, the ACMA found protections were not applied after such reports.
- **Call-backs to unlisted numbers**: staff contact a number not listed on the account to authenticate the caller.
- **Duplicate accounts**: a fraudster creates a new account and passes authentication using its own details.
- **Single-document identity checks**: fallback checks completed with one government document where two are required.
- **System workarounds in porting**: system weaknesses that let scammers bypass parts of pre-port verification (Exetel).
- **High prepaid volumes**: one person activating 5 or more prepaid services, which triggers stronger document requirements.

9 Enforcement and penalties

Breaching a service provider determination contravenes the civil penalty provision in Telecommunications Act s 101; breaching an industry standard contravenes s 128. Penalties apply per contravention (s 570(1)).

Contravention (body corporate)	Conduct before 27 Oct 2026	Conduct wholly on or after 27 Oct 2026
Service provider determination (Prepaid, CIA)	Up to $10 million each	Greatest of 30,300 penalty units (about $11.03 million at $364), 3 times the benefit, or 30% of adjusted turnover
Industry standard (Pre-Porting Standard)	Up to $250,000 each	Same as above
Registered industry code	Enforceable only after an ACMA direction	Same as above

Infringement notices	Amounts set by determination	Capped at 20% of the court maximum

The ACMA reports more than $5 million in penalties paid by telcos under its mobile number fraud crackdown. Recent actions:

- **Telstra, September 2026**: the ACMA found 15 unauthorised SIM swaps without the required authentication and 13 failures to protect at-risk customers in 2025. Telstra paid $277,200 under an infringement notice covering 14 of those contraventions (26 June to 30 October 2025), and the ACMA accepted court-enforceable undertakings; customers reported losses of at least $39,500.
- **Exetel, 27 August 2025**: $694,860 for 73 breaches of the Pre-Porting Standard in June and July 2024, after scammers bypassed parts of its verification; reported losses of at least $412,000.

10 Recent changes and what to watch

- **27 October 2026**: higher penalties, mandatory registered codes and stronger infringement notices `In force`. Breaches by conduct wholly on or after this date are subject to the new turnover-linked maximum.
- **26 October 2026**: CSP registration scheme enacted `Adopted, commences by 26 Oct 2027`. Registrable CSPs will need to register, and carriers and wholesale providers must not supply listed services to unregistered ones (s 96B).
- **29 September 2026**: draft Telecommunications (Consumer Protections) Industry Standard 2026 released `Proposed, comments close 10 Nov 2026`. It would replace the consumer code and require an external credit check before contracts above a debt limit.
- **1 September 2026**: the scams dispute resolution scheme membership provision (s 58BZG) began to apply to telcos `Partly in force`; full scams principles apply from 31 March 2027.
- **16 December 2025**: accredited Digital ID added as a prepaid verification method `In force`. The ACMA plans a wider review; the Prepaid Determination is due to sunset on 1 October 2027 unless remade.
- **9 December 2024**: ACMA proposal to vary the CIA Determination `Proposed, under review since Feb 2025`. It would add passkeys, make accredited Digital ID a primary option and move biometrics to a last resort, or remove them.

11 What this means for identity verification

- **Design to a fixed list.** Each prepaid activation must map to one Schedule 1 method (or an approved compliance plan), and the method's exact name must be recorded.
- **Records without document copies.** Prepaid records must show compliance and the method name (s 6.1, Sch 1), while identity documents and document numbers may not be recorded and kept, subject to the s 6.4 exceptions.
- **Document and selfie journeys.** Schedule 1 lists accredited Digital ID services (with customer consent) and the visual document check, but not document-and-selfie capture as a separate method. Whether a video call satisfies the visual check is not addressed by the Determination or the ACMA; an approved compliance plan covers any method outside Schedule 1.
- **SIM swap and port checks.** SIM swaps and other high-risk transactions need knowledge checks plus a listed factor, codes carrying the prescribed warning, and a reversal path (CIA Determination ss 9 and 10); ports need one listed verification process before proceeding (Pre-Porting Standard s 8).
- **Biometrics are sensitive information.** The OAIC guide points to consent (or a narrow exception) and a privacy impact assessment; automated-decision disclosures apply from 10 December 2026. The pending CIA variation would demote biometrics for SIM-swap authentication.
- **Keep audit trails for at least one year** for authentication, and for the life of the service for prepaid activation.

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:

- Remote identity verification for prepaid SIM and eSIM activation, with ID document capture, face match and biometric liveness, and configuration that avoids storing document images or numbers.
- Biometric re-verification and face match before SIM swaps, number ports and account changes, where the authentication rules permit biometric factors.
- Phone and email verification for possession checks, and configurable workflows that route failed checks to a staff fallback path.
- A no-code workflow builder and audit trail for each check, supporting record-keeping duties, with cloud, on-premises or hybrid deployment.

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

- **Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2017**, Compilation No. 1, 16 December 2025 (F2026C00020), ss 1.5, 1.8, 2.1 to 2.4, 4.2 to 4.5, Parts 3, 5 and 6, Schedule 1, Federal Register of Legislation, legislation.gov.au
- **Explanatory Statement to the Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2017**, registered 7 April 2017, sections 1.8 and Schedule 1 item 8, legislation.gov.au
- **Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Amendment Determination 2025 (No. 1)** and Explanatory Statement, registered 15 December 2025 (F2025L01545), legislation.gov.au

- **Telecommunications Service Provider (Customer Identity Authentication) Determination 2022** (F2022L00548), ss 4 to 16 and Schedule 1, legislation.gov.au
- **Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020** (F2020L00179), s 8, legislation.gov.au
- **Telecommunications Act 1997**, Compilation No. 117, 4 June 2026 (C2026C00224), ss 101, 116A, 121, 128, 276, 570, legislation.gov.au
- **Telecommunications Amendment (Enhancing Consumer Safeguards) Act 2026** (Act No. 99, 2026), Schedules 1 to 4, legislation.gov.au
- **Scams Prevention Framework Act 2025** (C2025A00015), ss 58EB and 58FK, legislation.gov.au
- **Competition and Consumer (Scams Prevention Framework–Regulated Sectors) Designation 2026** (F2026L00627), ss 13, 14 and 102, legislation.gov.au
- **Anti-Money Laundering and Counter-Terrorism Financing Act 2006**, Compilation No. 63, 1 October 2026, s 6, legislation.gov.au
- **Identity Verification Services Act 2023**, Compilation No. 1, 11 December 2024, s 7, legislation.gov.au
- **Telecommunications (Interception and Access) Act 1979**, Compilation No. 134, 27 August 2026 (C2026C00372), ss 187A, 187AA, 187C, legislation.gov.au
- **Telecommunications (SMS Sender ID Register) Industry Standard 2025** (F2025L01235), ss 2 and 12, legislation.gov.au
- **Administrative Arrangements Order**, 13 May 2025, Compilation No. 1, 1 July 2025 (C2025Q00005), Part 2, legislation.gov.au
- **ACMA, Telstra investigation report ACMA2025/126 (prepaid identity checks)**, July 2025, acma.gov.au
- **ACMA, "Proposal to vary the Telecommunications Service Provider (Customer Identity Authentication) Determination 2022"**, consultation 9 December 2024 to 14 February 2025, and consultation paper (5 December 2024), acma.gov.au
- **ACMA, "Proposal to make the Telecommunications (Consumer Protections) Industry Standard"**, consultation 29 September to 10 November 2026, and consultation draft, acma.gov.au
- **ACMA, "Proposal to amend the Prepaid Determination"**, consultation paper, September 2025, acma.gov.au
- **Attorney-General's Department, "Identity verification services"**, ag.gov.au
- **Crimes (Amount of a Penalty Unit) Instrument 2026** (F2026N00424), s 5, legislation.gov.au
- **ACMA, "ACMA strengthens consumer protections with Digital ID verification"**, December 2025, acma.gov.au
- **ACMA, "Telstra pays $277K after consumer fraud losses"**, MR 27/2026, 3 September 2026, acma.gov.au
- **ACMA, Telstra Limited investigation report**, 4 June 2026, and infringement notice, 26 June 2026, acma.gov.au
- **ACMA, "Exetel penalised $694K for anti-scam breaches"**, 27 August 2025, acma.gov.au

- ACMA, "Stronger penalty options to lift telco consumer protections", 15 October 2026, acma.gov.au
- ACMA, "Have your say on stronger protections for telco consumers", 29 September 2026, acma.gov.au
- ACMA, Register of telco industry codes and standards, acma.gov.au
- Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts, "New telecommunications laws boost consumer protections", 16 October 2026, infrastructure.gov.au
- OAIC, "Facial recognition technology: a guide to assessing the privacy risks", 29 July 2026, oaic.gov.au