Identomat

COMPLIANCE GUIDE

Banking & Digital Banking Compliance in Australia

COUNTRY Australia

INDUSTRY Banking & Digital Banking

LAST UPDATED 2 November 2026

KEY REGULATORS Australian Prudential Regulation Authority · Australian Transaction Reports and Analysis Centre · Australian Securities and Investments Commission

Key takeaways

- Only a company licensed by the Australian Prudential Regulation Authority (APRA) as an authorised deposit-taking institution (ADI) may carry on banking business, and any other financial business needs APRA's consent to call itself a "bank" or "neobank". APRA is ending its restricted "starter" licence and moving to formal licensing criteria, expected to be final in late 2026.
- Every bank must enrol with AUSTRAC, the anti-money laundering regulator, and must establish who each customer is before providing services, with narrow exceptions. Since 31 March 2026 the law sets outcomes rather than a fixed checklist of documents.
- Fully online account opening is allowed. AUSTRAC's guidance accepts a video call, or biometric face matching against photo ID from an identity verification provider, to confirm the applicant is the person on the document.
- An account may be opened and deposits accepted before checks are finished, but no money may leave the account until they are complete.
- From 31 March 2027 banks face most duties under the new scams law (the Scams Prevention Framework), with penalties for the highest-tier breaches that can reach 30% of turnover.

Australia is open to digital banks, but entry runs through a single prudential gate. APRA grants the banking authority, AUSTRAC supervises anti-money laundering and counter-terrorism financing (AML/CTF) compliance, and the Australian Securities and Investments Commission (ASIC) regulates conduct and, from 2026, scams prevention for the banking sector.

The biggest obstacle for a new entrant is the APRA licence itself, and its rules are being rewritten: under APRA's May 2026 proposal, every applicant would have 12 months to meet one set of criteria. Once licensed, a bank's onboarding must meet the reformed AML/CTF customer due diligence rules that took effect on 31 March 2026, with a transitional option to keep pre-reform procedures until 31 March 2029.

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

Banking is regulated nationally.

Regulator	Remit for banks	Level	Official site
APRA	Grants ADI authority under the Banking Act 1959; prudential standards (capital, operational risk, information security); restricted words; Financial Claims Scheme	Commonwealth	apra.gov.au
AUSTRAC	AML/CTF regulator and financial intelligence unit; enrolment, CDD, suspicious matter and threshold reporting	Commonwealth	austrac.gov.au
ASIC	Conduct regulator; consumer credit licensing (banks are credit licensees); Scams Prevention Framework sector regulator for banking	Commonwealth	asic.gov.au
ACCC	Scams Prevention Framework general regulator; Digital ID Regulator	Commonwealth	accc.gov.au
OAIC	Privacy Act 1988, including biometric data used in onboarding	Commonwealth	oaic.gov.au

Australian Sanctions Office (DFAT)	Consolidated List; asset freezing and permits	Commonwealth	dfat.gov.au
Department of Home Affairs	AML/CTF policy and amending legislation	Commonwealth	homeaffairs.gov.au
Attorney-General's Department	Identity Verification Services, including the Document Verification Service (DVS)	Commonwealth	idmatch.gov.au

2 Licensing and authorisation

A body corporate that carries on banking business in Australia without being the Reserve Bank or an ADI commits an indictable offence (200 penalty units, with each day a separate offence) under Banking Act 1959 s 8 (Compilation No. 69, 31 March 2026). Authority is sought from APRA in writing under s 9, and APRA may set criteria by legislative instrument. Using "bank", "banker", "banking" or a similar word in a financial business without APRA's consent is a separate offence under s 66; APRA lists "neobank", "banc" and "banq" among the restricted words.

A licensing framework in transition `Proposed, final late 2026`

APRA's current guidelines (August 2021) offer a full ADI licence or a restricted ADI licence for up to two years, and require an attestation of a board-approved AML/CTF programme and AUSTRAC enrolment. On 13 May 2026 APRA released draft formal licensing criteria in a legislative instrument and announced it is discontinuing the restricted pathway. Applicants would have 12 months to meet the criteria, APRA aims to decide within 90 days of a substantially complete application, and all decisions, including refusals, would be published. Final criteria are expected in late 2026.

Overseas banks serving retail clients need a local subsidiary. Deposits at locally incorporated ADIs are protected under the Financial Claims Scheme up to $250,000 per account holder per ADI; foreign-currency deposits are excluded.

3 AML, KYC and customer due diligence

Opening an account by an ADI is a designated service under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act) s 6, table 1, item 1 (Compilation

No. 63, 1 October 2026). A provider must apply to enrol with AUSTRAC within 28 days of starting (s 51B) and must maintain an ML/TF risk assessment and AML/CTF policies (ss 26E and 26F).

Initial customer due diligence In force from 31 Mar 2026

Under s 28, a bank must not start providing a service until it has established on reasonable grounds the customer's identity, anyone acting for the customer and their authority, beneficial owners, whether any of them is a politically exposed person (PEP) or designated for targeted financial sanctions, and the nature and purpose of the relationship. For an individual it must take reasonable steps to establish that the customer is the person they claim to be, and verify KYC information "using reliable and independent data" to the extent appropriate to the customer's risk. The delivery channel is a mandatory factor in that risk assessment (s 28(4)(d)). Beneficial owner means an individual who ultimately owns 25% or more of, or controls, a non-individual customer (s 5); Rules r 6-7 eases this for listed companies and government bodies.

Enhanced due diligence

Section 32 requires enhanced measures for high-risk customers, continuing relationships after a suspicious matter report, foreign PEPs, links to Financial Action Task Force (FATF) high-risk jurisdictions and nested services. Rules r 6-20 adds unusually complex or large transactions; r 6-21 requires source of wealth and funds where relevant.

Correspondent banking

A financial institution must not enter a correspondent relationship with a shell bank, or with an institution that deals with one, and must end it, or ask the other institution to end its shell bank link, within 20 days (s 95). Vostro relationships need a documented due diligence assessment and senior officer approval before entry (s 96).

Reporting and records

- **Suspicious matters:** within 3 business days of forming the suspicion, or 24 hours for terrorism financing (s 41). Suspecting that a person is not who they claim to be is itself a trigger.
- **Threshold transactions:** physical currency transfers of $10,000 or more, reported within 10 business days (ss 5 and 43).
- **International transfers:** international funds transfer instruction reports continue until the bank moves to new international value transfer service reports, 31 March 2029 or a later date notified to AUSTRAC, no later than 30 September 2029.

- **Records:** CDD records for 7 years after the relationship ends (s 111); transaction records for 7 years (s 107).

4 Identity verification and onboarding

The reformed Act does not list acceptable documents. AUSTRAC's guidance "Initial CDD for individuals" (updated 31 March 2026) describes this baseline:

- **Collect:** full name, other names, date of birth, residential address and a unique identifier such as a passport or driver's licence number.
- **Verify:** a government-issued primary photographic identification document; or a primary non-photographic document plus a secondary document showing name and address; or other independent and reliable data. An original or a reliable copy may be used.
- **Confirm the person:** compare the customer with the photo ID in person, compare "the name and features of the live video image" on a video call, or use biometric technology "such as a solution provided by an ID verification provider".
- **Screen:** PEP status and the latest Department of Foreign Affairs and Trade (DFAT) Consolidated List, checking alternative spellings.

For individuals without standard evidence, Rules r 6-10 allows identity to be established through reasonable steps, reasonably available data and policies managing the extra risk.

Government verification services

Under the Identity Verification Services Act 2023, businesses reach the Document Verification Service, which checks identity documents against government records, only through an approved gateway service provider. Participation agreements require the individual's express consent, and IDMatch advises that the DVS should not be the sole basis for a decision. Facial images are not provided in response to requests by or on behalf of non-government entities, so face matching for private onboarding is done by the bank or its provider. The Rules also anticipate verification through an entity accredited under the Digital ID Act 2024: suspicious matter and threshold reports must include any reference number such an entity provided (rr 9-3 and 9-7).

Reliance

A bank may rely on KYC information collected and verified by a reporting entity, or by a firm regulated under foreign laws giving effect to the FATF Recommendations, under a written arrangement (s 37A; Rules r 6-29). The arrangement must give the bank all KYC information

before service starts (or within any permitted delay) and copies of the verification data on request, and must be reassessed at least every 2 years (r 6-30). AUSTRAC's guidance (updated 13 October 2026) treats a KYC service provider as outsourcing, not reliance: the bank stays liable.

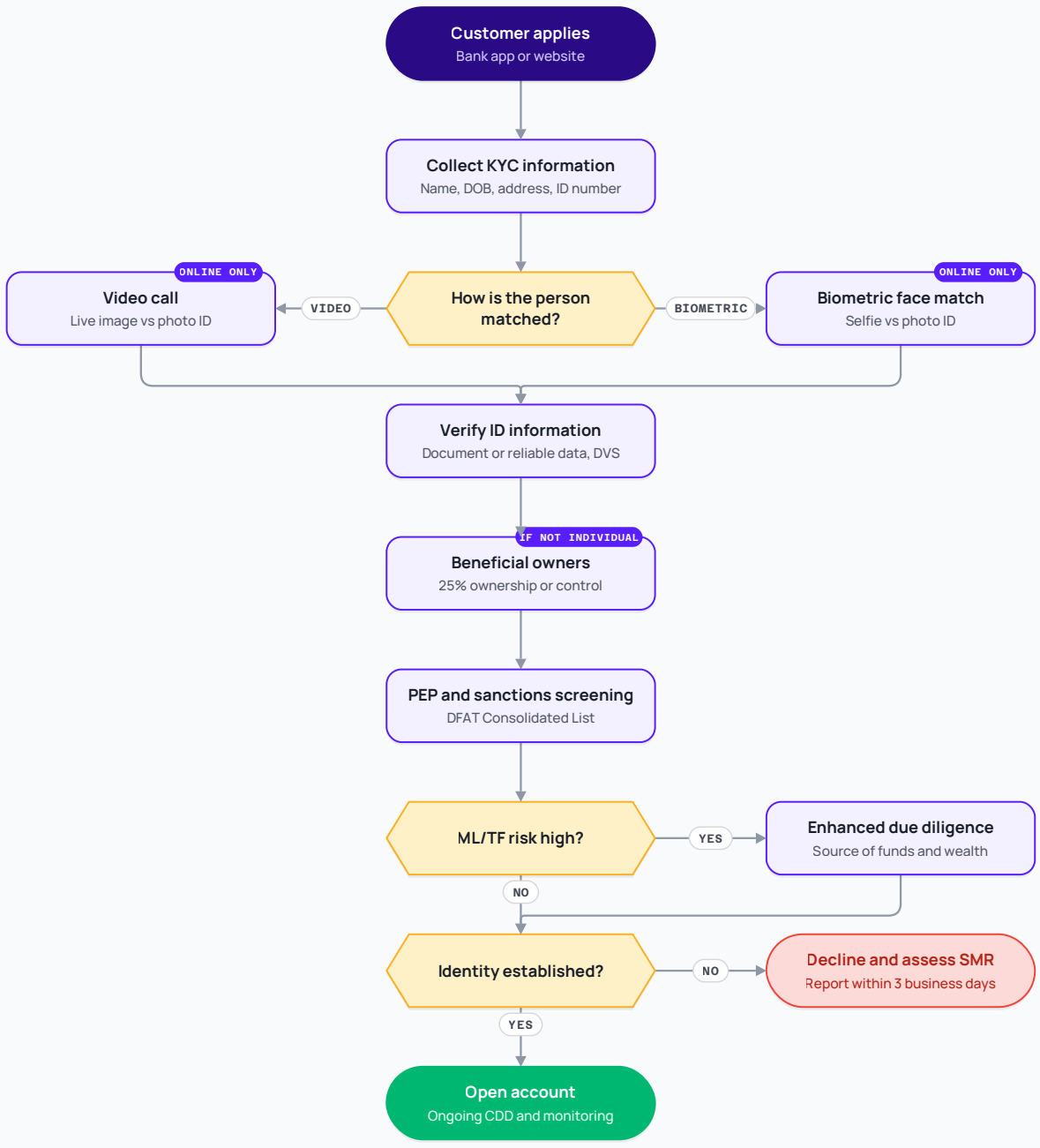


Figure 1. Remote retail account opening at an Australian ADI under the reformed AML/CTF rules.

5 Digital channels: what's different

Bottom line: the AML/CTF rules are channel-neutral, so a bank may onboard fully online, but the step of confirming the applicant is the person on the document moves from a branch comparison to a video call or biometric match, which brings privacy rules for biometric data into play.

Requirement	In person / branch	Online / remote	Difference
Remote onboarding permitted	Yes	Yes; same s 28 outcomes	Same
Risk treatment	Channel assessed as a risk factor	Channel assessed as a risk factor; no automatic EDD	Same
Confirming the person	Compare customer with photo ID	Video call or biometric match via a provider	Differs
Documents	Original or reliable copy	Reliable copy or reliable data; DVS via gateway	Differs
Timing	Account and deposits may precede CDD; no outflows	Same rule under r 6-13	Same
Sanctions and PEP screening	Part of initial CDD	Part of initial CDD	Same
Biometric data	Not usually collected	Sensitive information; consent or exception	Differs
Reliance on third parties	s 37A agreement	s 37A agreement	Same
Record retention	7 years after relationship ends	7 years, including data collected	Same

Liveness and face matching are a method, not a mandate

AUSTRAC names biometric technology as one option but sets no liveness or presentation attack standard. The bank documents its method in its AML/CTF policies (ss 26F and 28).

Open first, release funds later

Rules r 6-13 lets an ADI open an account and accept deposits before initial due diligence is complete, provided s 29 conditions are met (delay essential to avoid interrupting business, additional risk low, policies in place). Due diligence must still be completed as soon as reasonably practicable, and until s 28(1) is satisfied the bank must not transfer money for the customer or otherwise make funds available.

Bank partnerships and outsourced onboarding

Where a technology or fintech partner runs onboarding, the bank remains the reporting entity and liable for due diligence, and APRA's Prudential Standard CPS 230 requires a register of material service providers, due diligence before entering a material arrangement, a formal agreement, and notice to APRA within 20 business days of entering an agreement for a service that supports a critical operation.

No statute mandates strong customer authentication for account access; most banks subscribe to ASIC's voluntary ePayments Code, which allocates liability for unauthorised transactions.

What is changing

The Australian Government Digital ID System opens to the private sector from December 2026 `Announced, from Dec 2026`; use of Digital ID by individuals remains voluntary. The Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2026 would let the AUSTRAC CEO restrict or prohibit high-risk mechanisms, including delivery channels, used to provide designated services `Passed House, before Senate`.

6 Data protection and biometrics

The OAIC's facial recognition guide (29 July 2026) states that biometric templates and facial images used for automated verification or identification are sensitive information. Collection must be reasonably necessary and, under the consent pathway, made with valid consent, unless an exception applies. The OAIC recommends a privacy impact assessment and a retention and destruction protocol for biometric information.

Retention needs reconciling with s 111, which requires records of "the type and content of the data collected" for 7 years after the relationship ends.

From 10 December 2026, Australian Privacy Principle 1.7 requires privacy policies to describe the kinds of personal information used, and the kinds of decisions made, by

computer programs where a decision could significantly affect an individual `Adopted, effective 10 Dec 2026`.

7 Sector-specific obligations

Transitional customer identification procedures

Banks enrolled on 30 March 2026 may keep carrying out the pre-reform "applicable customer identification procedure" for named customer classes under the AML/CTF Transitional Rules 2026 s 7. For medium or lower risk individuals these included an electronic safe harbour: name plus address or date of birth verified from at least two separate electronic data sources (former Rules 2007, paras 4.2.13 and 4.2.14). From 1 July 2026 policies must list each class and the date the old procedure stops for it. The section ceases to have effect on 31 March 2029. Ongoing due diligence under the reformed s 30 applies to all customers from 31 March 2026.

Scams Prevention Framework

Under Part IVF of the Competition and Consumer Act 2010, ADI banking services were designated a regulated sector in May 2026, with ASIC as sector regulator. Banks had to join the Australian Financial Complaints Authority scheme by 1 September 2026; most principles (prevent, detect, report, disrupt, respond) apply from 31 March 2027. A banking code, consulted on by Treasury to 25 June 2026, will set out the reasonable steps expected `Draft code, consultation closed`.

Operational risk and outsourcing

Prudential Standard CPS 230 Operational Risk Management (current version commenced 1 July 2026) requires ADIs to submit their register of material service providers to APRA annually and to treat providers of core technology services and risk management as material unless justified otherwise. CPS 234 Information Security also applies.

8 Risk indicators and red flags

INDICATORS FOR BANKS (AUSTRAC, UPDATED 25 MARCH 2026)

- **Unverifiable ID**: an identification document that cannot be authenticated, or inconsistent details across documents.
- **Shared identifiers**: apparently unrelated customers using the same mobile number, email or IP address.
- **Short-stay accounts**: a visitor or short-term visa holder opening an account during a brief stay.
- **Pass-through activity**: numerous outgoing payments to unrelated parties shortly after incoming funds arrive.
- **Profile changes before withdrawal**: a large withdrawal following changes to identification or contact details.
- **Structuring**: cash deposits split below the $10,000 threshold, across branches, ATMs or third parties.
- **Dormant reactivation**: an inactive account that suddenly shows frequent activity.
- **Higher-risk IP**: access from an IP address linked to a jurisdiction associated with scams.

9 Enforcement and penalties

AUSTRAC's tools include civil penalty proceedings, enforceable undertakings, infringement notices and remedial directions. The maximum civil penalty is 100,000 penalty units per contravention for a body corporate and 20,000 for other persons (AML/CTF Act s 175). At the current Commonwealth penalty unit of $364 (Crimes Act 1914 s 4AA, indexed on 1 July 2026), the corporate maximum is about $36.4 million per contravention. Failing initial due diligence is a separate contravention for each service provided to the customer (s 28(9)).

- **Westpac (2020):** the Federal Court declared breaches on over 19 million occasions and ordered a $1.3 billion penalty on 21 October 2020.
- **Commonwealth Bank of Australia (2018):** the Federal Court ordered a $700 million penalty on 20 June 2018.

- **Bank of Queensland (2023, ongoing):** an enforceable undertaking (s 197) after findings on customer identification, enhanced due diligence and risk assessment, with an external auditor reporting every four months.

Under the Scams Prevention Framework, tier 1 contraventions (prevent, detect, disrupt, respond) carry the greater of 159,745 penalty units, three times the benefit obtained or 30% of adjusted turnover; tier 2 (governance, reporting, codes) the greater of 31,950 penalty units, three times the benefit or 10% of turnover (Competition and Consumer Act ss 58FK and 58FL).

10 Recent changes and what to watch

- **31 March 2029** `Adopted, effective 31 Mar 2029`: the transitional customer identification option ends and international value transfer service reports replace current international transfer reports. Migrate every customer class before this date.
- **31 March 2027** `Adopted, effective 31 Mar 2027`: most Scams Prevention Framework principles start to apply to banks; onboarding and payment controls will be judged against the banking code once made.
- **10 December 2026** `Adopted, effective 10 Dec 2026`: privacy policies must disclose automated decisions, including onboarding outcomes; the Digital ID System is also due to open to private-sector participants this month.
- **Late 2026** `Proposed, consultation closed 31 Jul 2026`: APRA's formal ADI licensing criteria, with the restricted ADI pathway discontinued. Applicants should plan against the draft criteria.
- **12 October 2026** `Bill, passed House only`: the AML/CTF Amendment Bill 2026, introduced in the Senate, would allow AUSTRAC to restrict or prohibit high-risk products, services or delivery channels.
- **1 September 2026** `Partly in force`: Scams Prevention Framework Rules 2026 commence and banks must belong to the complaints scheme for scam disputes.
- **31 March 2026** `In force`: the reformed AML/CTF obligations and AML/CTF Rules 2025 apply, replacing prescriptive identification procedures with outcomes-based due diligence; on 1 July 2026 transitional policies had to name customer classes and stop dates.

11 What this means for identity verification

- **Outcome, not checklist:** evidence each s 28(2) matter and the steps taken to confirm the person.
- **Remote person-matching:** a video call or biometric face match against a government photo ID meets AUSTRAC's description; document the method and its accuracy in the AML/CTF policies.
- **Document checks:** DVS checks need express consent and should not be the only basis for a decision.
- **Payment holds:** block outflows from accounts opened before checks finish.
- **Biometric governance:** obtain consent, run a privacy impact assessment, and keep verification evidence separate from raw templates.
- **Re-verification triggers:** contact-detail changes before large withdrawals, shared identifiers and higher-risk IP addresses should prompt review under ongoing due diligence.

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 KYC onboarding with ID document capture and verification, face match and biometric liveness to confirm the applicant is the person on the document.
- Video KYC for customers who are onboarded through a live video call.
- AML screening against sanctions, PEP and adverse-media lists at onboarding, with ongoing monitoring.
- KYB and beneficial owner verification for business customers.
- A no-code workflow builder to configure risk-based flows, 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

- **Anti-Money Laundering and Counter-Terrorism Financing Act 2006**, Compilation No. 63, 1 October 2026 (C2026C00447), ss 5, 6, 26E, 26F, 28 to 32, 37A, 41, 43, 46, 51B, 95, 96, 107, 111, 175, Federal Register of Legislation, legislation.gov.au
- **Anti-Money Laundering and Counter-Terrorism Financing Rules 2025**, Compilation No. 1, 31 March 2026 (F2026C00274), rr 6-7, 6-10, 6-12, 6-13, 6-20, 6-21, 6-29, 6-30, 9-3, 9-7, legislation.gov.au
- **Anti-Money Laundering and Counter-Terrorism Financing Transitional Rules 2026**, Compilation No. 1, 14 May 2026 (F2026C00452), ss 7 and 8, legislation.gov.au
- **Banking Act 1959**, Compilation No. 69, 31 March 2026 (C2026C00104), ss 8, 9, 66, legislation.gov.au
- **Scams Prevention Framework Act 2025** (C2025A00015), Schedule 1 (Competition and Consumer Act 2010 Part IVF, ss 58FK, 58FL), legislation.gov.au
- **Competition and Consumer (Scams Prevention Framework – Regulated Sectors) Designation 2026** (F2026L00627), ss 11, 12, 101, legislation.gov.au
- **Competition and Consumer (Scams Prevention Framework) Rules 2026** (F2026L01140), commencement 1 September 2026, legislation.gov.au
- **Prudential Standard CPS 230 Operational Risk Management**, determination No. 1 of 2026 (F2026L00475), paras 6 and 48 to 52, legislation.gov.au
- **Prudential Standard CPS 234 Information Security** (F2018L01745), legislation.gov.au
- **Crimes (Amount of a Penalty Unit) Instrument 2026** (F2026N00424), s 5, legislation.gov.au
- **Identity Verification Services Act 2023**, Compilation No. 1, 11 December 2024, legislation.gov.au
- **Privacy and Other Legislation Amendment Act 2024** (C2024A00128), Schedule 1 Part 15 (APP 1.7), legislation.gov.au
- **Crimes Act 1914**, Compilation No. 167, 27 August 2026, s 4AA, legislation.gov.au
- **Anti-Money Laundering and Counter-Terrorism Financing Rules 2007** (former rules), Compilation No. 76, 22 November 2024, paras 4.2.13 and 4.2.14, legislation.gov.au
- **Explanatory statement to the AML/CTF Rules 2025** (replacement, registered 27 May 2026), paras 369 to 375, legislation.gov.au (PDF)
- **Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2026**, Parliament of Australia, aph.gov.au

- **Overview of reliance on customer identification by a third party**, AUSTRAC, last updated 13 October 2026, austrac.gov.au
- **Reliance under customer due diligence arrangements**, AUSTRAC, last updated 27 March 2026, austrac.gov.au
- **A more efficient and transparent bank licensing framework**, APRA, 13 May 2026, apra.gov.au
- **ePayments Code**, ASIC, 20 December 2024, asic.gov.au
- **Who we regulate**, ASIC, 11 August 2026, asic.gov.au
- **2026 Reforms to the AML/CTF Act**, Department of Home Affairs, homeaffairs.gov.au
- **Initial CDD for individuals**, AUSTRAC, last updated 31 March 2026, austrac.gov.au
- **AML/CTF transitional rules 2026**, AUSTRAC, austrac.gov.au
- **Update to AUSTRAC's regulatory expectations for implementation of the AML/CTF reforms**, 18 December 2025, austrac.gov.au
- **Indicators of suspicious activity for the banking sector**, AUSTRAC, last updated 25 March 2026, austrac.gov.au
- **Enforcement actions taken**, AUSTRAC, last updated 30 October 2026, austrac.gov.au
- **Bank of Queensland Ltd enforceable undertaking** (s 197), May 2023, austrac.gov.au (PDF)
- **Licensing guidelines for authorised deposit-taking institutions**, APRA, apra.gov.au
- **Guidelines: Licensing locally-incorporated ADIs**, APRA, August 2021, sections on timeframes, Table 1 and AML/CTF expectations, apra.gov.au (PDF)
- **Financial Claims Scheme: Banks, building societies and credit unions**, APRA, apra.gov.au
- **Scams Prevention Framework**, ASIC, 21 August 2026, asic.gov.au
- **Scams Prevention Framework codes and rules exposure draft**, Treasury consultation, 27 May to 25 June 2026, consult.treasury.gov.au
- **Digital ID regulation**, ACCC, 21 July 2026, accc.gov.au
- **Become a DVS business user**, IDMatch, idmatch.gov.au
- **Facial recognition technology: a guide to assessing the privacy risks**, OAIC, 29 July 2026, oaic.gov.au (PDF)
- **Consolidated List**, DFAT Australian Sanctions Office, list updated 23 July 2026, dfat.gov.au