Identomat

COMPLIANCE GUIDE

Insurance & Insurtech Compliance in Australia

COUNTRY Australia

INDUSTRY Insurance & Insurtech

LAST UPDATED 2 November 2026

KEY REGULATORS Australian Prudential Regulation Authority · Australian Securities and Investments Commission · AUSTRAC

Key takeaways

- Only some insurance products bring an insurer under anti-money laundering law: life policies that carry a prescribed minimum surrender value (a minimum amount payable if the policy is cashed in early), sinking fund policies and annuities. General insurance, life policies with no prescribed minimum surrender value, small-premium life policies and consumer credit insurance are outside it.
- Every insurer needs prudential approval (authorisation for general insurers, registration for life companies) from the Australian Prudential Regulation Authority (APRA), and a financial services licence from the Australian Securities and Investments Commission (ASIC) to sell, advise on or handle claims. Digital and embedded distributors can operate as a licensee's authorised representative instead of holding their own licence.
- Selling online is allowed and the identity rules are the same in every channel. For covered life products the customer must be identified before the policy is issued, and AUSTRAC (the financial intelligence agency) accepts a video call or biometric face matching to confirm a remote applicant is the real person.
- The person receiving a life policy payout is treated as a customer in their own right: their identity must be checked before money is released, even where some checks were delayed at sale.
- Face templates used for verification are sensitive information under the Privacy Act, so they generally need consent and should not be kept longer than needed. From 10 December 2026, privacy policies must also explain automated decisions that significantly affect people.

Australia is open to online and embedded insurance, including direct-to-consumer apps and insurance sold at a partner's checkout, but entry is gated by two federal licences: prudential approval from APRA to carry the risk, and an Australian financial services licence from ASIC to deal with customers. AUSTRAC supervises the life insurers and annuity providers that fall within the Anti-Money Laundering and Counter-Terrorism Financing Act 2006.

The biggest obstacle for a new entrant is usually not identity verification but authorisation: carrying on general insurance business without APRA authorisation is a criminal offence and only APRA-registered companies may issue life policies, so an insurtech that does not want to become an insurer must partner with one. Conduct rules then shape the online journey, most notably the ban on unsolicited offers and the four-day deferral on add-on insurance sold alongside another product.

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

Insurance is regulated at federal level.

Regulator	Remit for insurers	Level	Official site
Australian Prudential Regulation Authority (APRA)	Authorises general insurers, registers life companies, sets prudential standards including operational risk and information security	Federal	apra.gov.au
Australian Securities and Investments Commission (ASIC)	Australian financial services licensing, conduct, claims handling, design and distribution, hawking, add-on insurance, utmost good faith	Federal	asic.gov.au
AUSTRAC (Australian Transaction Reports and Analysis Centre)	AML/CTF regulator and financial intelligence unit for life policy, sinking fund and annuity providers	Federal	austrac.gov.au
Office of the Australian Information Commissioner (OAIC)	Privacy Act, biometric and identity document handling	Federal	oaic.gov.au
Australian Competition and Consumer Commission (ACCC)	Digital ID Regulator (accreditation of identity providers)	Federal	accc.gov.au

Australian Sanctions Office, Department of Foreign Affairs and Trade (DFAT)	Consolidated List of sanctioned persons and asset freezing	Federal	dfat.gov.au

Every financial services licensee must be a member of the Australian Financial Complaints Authority (AFCA) scheme (Corporations Act s 912A(2)©). AFCA resolves insurance complaints and can make decisions binding on the insurer, but it is not a regulator and does not impose fines.

2 Licensing and authorisation

Prudential authorisation (the risk carrier)

A body corporate that carries on insurance business in Australia without being authorised by APRA under section 12 of the Insurance Act 1973 commits a strict liability offence (s 10, 60 penalty units, up to five times that for a company). Life insurance follows a separate regime: under s 17 of the Life Insurance Act 1995, only a company registered under s 21 may issue, or undertake liability under, a life policy. Acting as agent of a registered company is expressly permitted, which allows distribution partnerships. Private health insurers are registered separately and also supervised by APRA.

Conduct licensing (the customer relationship)

Anyone carrying on a financial services business must hold an Australian financial services licence (AFSL) under s 911A of the Corporations Act 2001. Financial services include dealing in and advising on insurance products and, for claims made on or after 1 January 2021, a "claims handling and settling service" (s 766A(1)(eb), s 766G and s 1675A), which covers assessing liability, deciding claims and quantifying or settling them. A person acting as the authorised representative of a licensee is exempt from holding its own AFSL (s 911A(2)(a)). Embedded insurance sold through retailers, travel sites or lending apps can run on this model.

Product governance

An issuer that must prepare a Product Disclosure Statement must make a target market determination before any retail distribution (s 994B, Part 7.8A, design and distribution obligations).

3 AML, KYC and customer due diligence

Which insurance business is in scope

The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act, Compilation No. 63, 1 October 2026) lists as designated services: issuing or undertaking liability under a life policy or sinking fund policy (table 1, item 37, customer: the policyholder); accepting a premium (item 38); making a payment under the policy (item 39, customer: the person paid); and accepting the purchase price of, or paying, a pension or annuity (items 40 and 41). The s 5 definition of "life policy" excludes:

- policies with no prescribed minimum surrender value, a question decided under APRA's prudential standards made under s 230A of the Life Insurance Act;
- regular premium policies with premiums of no more than $1,500 a year, and single premium policies of no more than $3,000;
- consumer credit insurance.

General insurance is not a designated service, and each life product must be tested against the definition.

Customer due diligence

Since 31 March 2026 the regime is outcomes-based. Before providing a designated service, an insurer must establish on reasonable grounds the customer's identity, anyone acting for the customer and their authority, beneficial owners of a non-individual (25% ownership or control, s 5), politically exposed person (PEP) and targeted financial sanctions status, and the nature and purpose of the relationship (s 28(2)). For individuals it must take reasonable steps to establish the customer is who they claim to be, and verify KYC information "using reliable and independent data" in proportion to the risk (s 28(3)). For items 37 and 38, rule 6-34 of the AML/CTF Rules 2025 treats the "on whose behalf" requirement as met once the insurer has collected the full name of each person who may be entitled to a payment, or a description of each class of beneficiaries where they cannot be named.

Enhanced due diligence is mandatory where the customer's risk is high, a suspicious matter report has been made and the relationship continues, the customer or a related person is a foreign PEP, a party is in or formed in a jurisdiction for which the Financial Action Task Force has called for enhanced measures (s 32), or the customer seeks services with no apparent economic or legal purpose or unusually large or complex transactions (rule 6-20). For a foreign PEP, or a high-risk domestic or international organisation PEP, the source of wealth and source of funds must be established (rule 6-23).

Reporting and records

Suspicious matter reports

Within 3 business days of forming a suspicion, or 24 hours for terrorism financing (s 41(2)). A suspicion that a person is not who they claim to be is itself a trigger (s 41(1)(d)).

Threshold transaction reports

Physical currency of $10,000 or more, within 10 business days (s 43 and the s 5 definition).

Ongoing due diligence

Monitoring for unusual transactions and behaviours applies to all customers from 31 March 2026 (s 30, rule 6-35).

Records

Customer due diligence records are kept for 7 years after the relationship ends (s 111), and transaction records for 7 years (Part 10).

Life insurers already enrolled with AUSTRAC on 30 March 2026 may keep applying their pre-reform customer identification procedures to named classes of customers under s 7 of the AML/CTF Transitional Rules 2026, provided their policies record each class and, from 1 July 2026, the date it moves to the new framework. The option ends on 31 March 2029 and is not open to new entrants, and customers handled this way cannot use the new delayed verification or deemed compliance rules (AUSTRAC). Ongoing due diligence obligations already apply to every customer.

4 Identity verification and onboarding

The Act and Rules prescribe no document list. AUSTRAC's guidance on initial customer due diligence for individuals (updated 31 March 2026) gives this baseline:

- **Collect** full name, other names, date of birth, residential address and a unique identifier.
- **Verify** name and date of birth against a government-issued photo identity document, or a non-photo document plus a secondary document showing name and address. Reliable copies, or other reliable and independent data, can replace originals.
- **Confirm the person** by comparing their face with the photo identity document in person, over a video call, or with biometric technology from an identity verification provider.
- **Screen** for PEP status and against the DFAT Consolidated List, checking alternative spellings.

Where someone cannot produce evidence of identity, rule 6-10 allows reasonable steps and risk-based alternative data. Government database checks are available through the Document Verification Service, which businesses reach only through an approved gateway service provider and which should not be the sole basis for a decision (IDMatch).

Collection and verification may be carried out by an agent, such as an adviser, broker or embedded partner, but the insurer remains liable for any failure (s 37). Reliance on another regulated firm's verification is permitted under a written arrangement assessed regularly (ss 37A and 37B) or case by case (s 38).

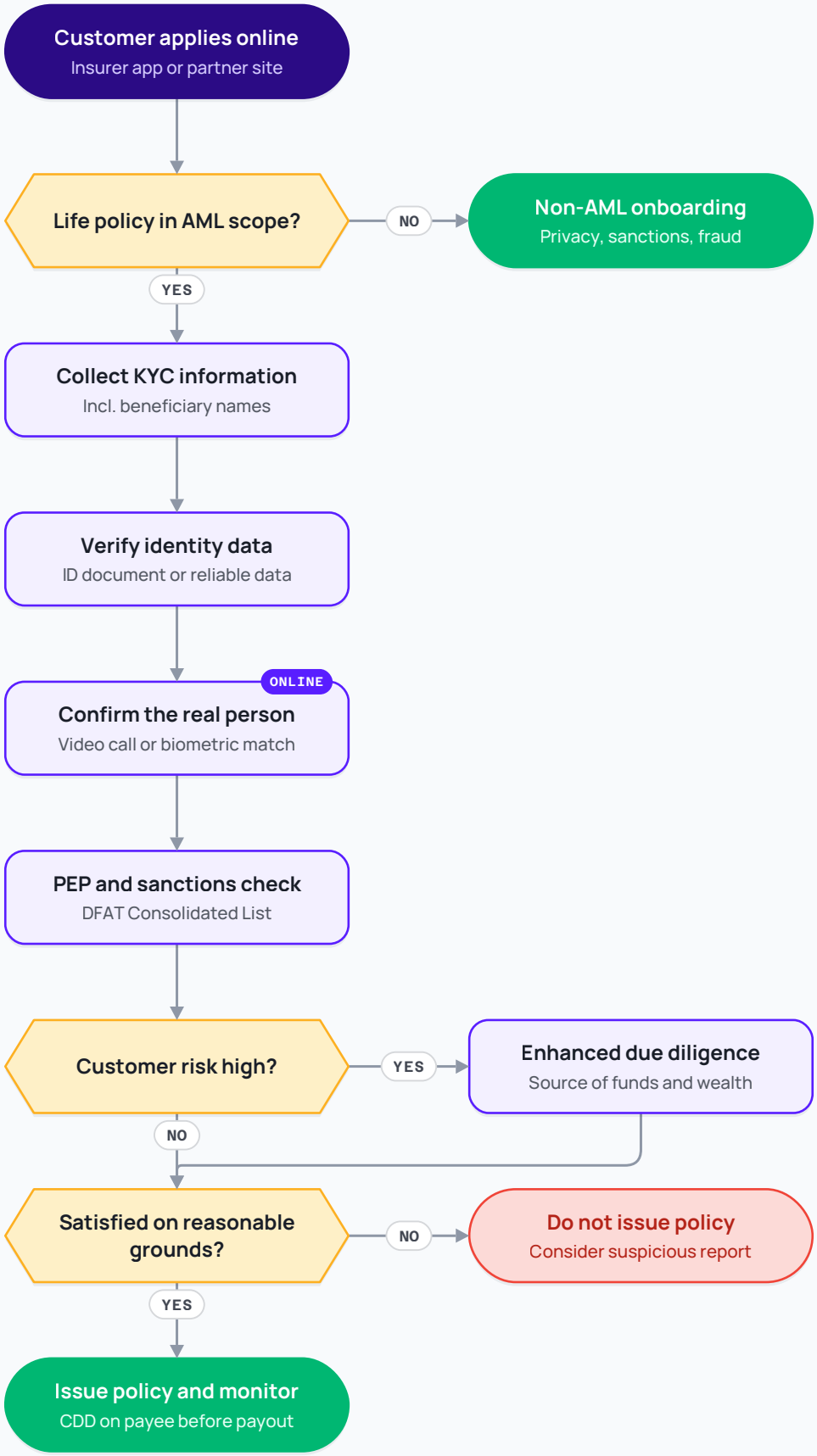


Figure 1. Online onboarding for a life policy within the AML/CTF Act in Australia.

5 Digital channels: what's different

Bottom line: the AML/CTF and insurance conduct rules are channel-neutral, so an online life policy faces the same tests as one sold face to face. What changes online is how identity is evidenced (remote face matching instead of sighting the person) and the privacy rules that come with biometrics.

Requirement	In person / land-based	Online / remote	Difference
Remote onboarding permitted	Yes	Yes, no in-person step required by the Act	Same
Delivery channel as a risk factor	Considered in customer risk	Considered in customer risk, no automatic enhanced checks	Same
Confirming the person is genuine	Face compared with photo ID	Video call or biometric technology	Differs
Document evidence	Originals or reliable copies	Reliable copies or other reliable and independent data	Same
When checks are completed	Identity before the policy is issued; some other checks within 20 business days	Same rule	Same
Payout to a beneficiary	Payee identified before payment	Payee identified before payment	Same
Add-on insurance at the point of sale	Sale deferred 4 days	Sale deferred 4 days, including at online checkout	Same
Unsolicited offers (hawking)	Banned in calls and meetings without prior consent	Banned in other real-time conversations, which can include live chat; email and web offers fall outside the definition	Differs

Biometric data	Usually not collected	Face templates are sensitive information: consent generally needed	`Differs`

Remote identity is outcome-based

Section 28(4)(d) makes the delivery channel a mandatory input to each customer's risk rating, but nothing in the Act or Rules classes non-face-to-face sales as high risk in itself.

Delayed verification stops at the payout

Rule 6-12 allows some checks, such as beneficial ownership, PEP and sanctions status, to be verified within 20 business days after the policy starts if the delay is essential to avoid interrupting normal business and the added risk is low. The customer's identity and the authority of anyone acting for them must still be verified first, and no money may be made available to the customer in the meantime. Because a payment under a life policy is a separate designated service whose customer is the person paid (item 39), digital claims journeys must verify the payee before funds leave.

Embedded and add-on insurance

Add-on insurance, such as cover offered at a car, device or travel checkout, is subject to the deferred sales model in the ASIC Act 2001: the add-on product cannot be sold until a four-day deferral period, which starts once the customer has been given prescribed information, has ended (ss 12DP and 12DQ), unless ASIC has granted an exemption for the product or class of products (s 12DY). The hawking ban (Corporations Act s 992A(4)) covers unsolicited calls, meetings and other real-time conversations, not non-real-time messages.

6 Data protection and biometrics

The Privacy Act 1988 applies to all personal information handled for AML/CTF purposes, including by small businesses that would otherwise be exempt. The OAIC's privacy guidance for reporting entities (updated 28 August 2026) makes three key points:

- Biometric information used for automated verification or identification, and biometric templates, are sensitive information. Collection must be necessary and proportionate and needs consent or an exception, such as collection required by Australian law. The OAIC's view is that consent should generally be sought before biometric verification for customer due diligence.

- The AML/CTF Act does not require insurers to keep scanned copies of identity documents; recording the document details is enough. Copies made before 31 March 2026 may be kept for 7 years after the relationship ends.
- Personal information no longer needed for a permitted purpose must be destroyed or de-identified.

The OAIC's facial recognition guide (29 July 2026) adds a privacy impact assessment and scrutiny of third-party providers. From 10 December 2026, privacy policies must describe decisions that computer programs make, or substantially assist, where they significantly affect individuals, such as automated underwriting or claims triage (OAIC).

7 Sector-specific obligations

Utmost good faith in claims

Every insurance contract implies a duty of the utmost good faith (s 13, Insurance Contracts Act 1984, Compilation No. 33, 8 October 2026). An insurer that breaches it faces a civil penalty of up to 5,000 penalty units (s 13(2A)). For consumer contracts the insured's duty is to take reasonable care not to make a misrepresentation (s 20B), so the clarity of online questions is part of the legal test.

Genetic information in life underwriting

Since 8 October 2026, a life insurer may not solicit or use protected genetic information (whether a person or relative has had, intends or was recommended a genetic test, and the results) in underwriting decisions (ss 33E to 33H). Breach is a strict liability offence (60 penalty units) and a civil penalty (5,000 penalty units). A narrow exception applies where the information is volunteered unsolicited, written consent is given and its use disadvantages no one under the contract.

Operational resilience and outsourcing

Prudential Standard CPS 230 Operational Risk Management (in force since 1 July 2025 and remade from 1 July 2026) requires insurers to treat providers of underwriting, claims management, insurance brokerage, reinsurance and core technology services as material service providers unless they can justify otherwise, keep a register and notify APRA of material operational risk incidents within 72 hours. CPS 234 Information Security requires notification of material information security incidents within 72 hours and covers information assets held by third parties, which can include identity verification vendors.

8 Risk indicators and red flags

AUSTRAC's suspicious activity indicators for the life insurance sector (updated 30 September 2024) include:

LIFE INSURANCE TYPOLOGIES

- **Early surrender at a loss**: accepting a large loss on early surrender without a sound reason.
- **Shared digital identifiers**: several applicants using the same phone number, email or IP address.
- **Unverifiable identity**: documents that cannot be authenticated, or stolen identities used to open policies.
- **Premium mismatch**: premiums inconsistent with stated income, or sudden lump sums replacing regular payments.
- **Beneficiary churn**: frequent changes of beneficiary to people with no apparent link.
- **Account takeover before a claim**: email, phone or identity details changed shortly before a claim or payout.

9 Enforcement and penalties

Penalties are expressed in penalty units; the Commonwealth penalty unit is $364 from 1 July 2026, up from $330 (Crimes Act 1914 s 4AA; Crimes (Amount of a Penalty Unit) Instrument 2026).

Breach	Maximum	Basis
AML/CTF civil penalty provisions, such as providing a service without customer due diligence	100,000 penalty units (about $36.4 million) for a company	Per contravention; each service is a separate contravention (AML/CTF Act ss 28(9), 175)
Financial services without an AFSL; target market breaches	Greatest of 50,000 penalty units, three times the benefit, or 10% of turnover (capped at 2.5 million units)	Per contravention (Corporations Act ss 911A(5B), 994B, 1317G(4))

Breach of utmost good faith by an insurer	5,000 penalty units (about $1.82 million)	Per contravention (Insurance Contracts Act s 13(2A))
Using protected genetic information	5,000 penalty units civil; 60 penalty units offence	Per decision (Insurance Contracts Act s 33H)
General insurance business without APRA authorisation	60 penalty units, up to five times for a company	Strict liability offence (Insurance Act s 10)

AUSTRAC's published enforcement record (30 October 2026) contains no action against an insurer; its court cases have involved other sectors, such as banks, casinos, betting operators and clubs. On 9 October 2026 ASIC announced that the Federal Court had ordered Hollard Insurance Partners to pay $2 million for breaching the duty of utmost good faith in handling a home insurance claim, the first civil penalty against an insurer for that breach (ASIC 26-236MR).

10 Recent changes and what to watch

- **10 December 2026** `Adopted, effective 10 Dec 2026` Privacy policies must disclose automated decisions that significantly affect people, such as automated underwriting or claims decisions.
- **December 2026** `Adopted, opens Dec 2026` The Australian Government Digital ID System opens to private sector participants, a potential further identity verification route for insurers (ACCC).
- **November 2026** `Scheduled, plenary Jun 2027` FATF mutual evaluation of Australia, the first since 2015, with an indicative onsite visit in November 2026 (FATF).
- **9 October 2026** `In force` ASIC announces the first civil penalty against an insurer for breach of utmost good faith, over claim delays.
- **8 October 2026** `In force` Ban on using protected genetic information in life underwriting; application forms and data sources need review.
- **30 September 2026** `Published` ASIC's 2026–27 life insurance priorities target service basics, funeral insurance, cyber resilience and AI.
- **1 July 2026** `In force` Remade CPS 230 commenced; it lists underwriting, claims management and brokerage providers as material service providers for insurers by default.
- **31 March 2026** `In force, optional transitional relief` Reformed AML/CTF regime and Rules 2025 apply; insurers enrolled on 30 March 2026 may keep their previous identification procedures for named customer classes until 31 March 2029.

11 What this means for identity verification

- **Scope by product.** Apply full AML/CTF due diligence to in-scope life, sinking fund and annuity products; screen sanctions everywhere.
- **Remote methods.** Document capture with face matching and liveness, video calls, Document Verification Service checks and accredited Digital ID can all support the outcomes-based test.
- **Beneficiaries and payees.** Capture beneficiary names at sale and verify the payee before any payout, including when a claim follows recent changes to contact details.
- **Biometrics.** Obtain consent, run a privacy impact assessment and keep templates and images only as long as needed.
- **Partners.** Agents and embedded distributors can collect and verify, but the insurer stays liable.
- **Re-verification triggers.** Beneficiary, bank or contact detail changes, surrender and claims.

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 life policy applicants, with ID document capture (including NFC), face match and biometric liveness.
- Screening of policyholders, beneficiaries and payees against sanctions and PEP lists at onboarding and on an ongoing basis.
- Re-verification of the payee before a claim or surrender payout, triggered by your own risk rules.
- No-code workflows that apply full due diligence only to products in AML scope, with an audit trail for each check.
- Cloud, on-premises or hybrid deployment to support data residency and retention policies.

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, ss 5, 6 (table 1 items 37 to 41), 28 to 32, 37 to 38, 41, 43, Part 10 (incl. s 111), 175, Federal Register of Legislation, legislation.gov.au
- **Anti-Money Laundering and Counter-Terrorism Financing Rules 2025**, Compilation No. 1, 31 March 2026, rules 6-10, 6-12, 6-20, 6-23, 6-34, 6-35, and explanatory statement (para 369), legislation.gov.au
- **Insurance Act 1973**, Compilation No. 73, 21 February 2025, ss 10 to 12, legislation.gov.au
- **Life Insurance Act 1995**, Compilation No. 69, 21 February 2025, ss 17 and 21, legislation.gov.au
- **Insurance Contracts Act 1984**, Compilation No. 33, 8 October 2026, ss 13, 20B, 33E to 33H, legislation.gov.au
- **Corporations Act 2001**, Compilation No. 149, 19 September 2026, ss 766A, 766G, 911A, 912A, 992A, 994B, 1317G, 1675A, legislation.gov.au
- **Australian Securities and Investments Commission Act 2001**, Compilation No. 109, 19 September 2026, ss 12DP, 12DQ, 12DY, legislation.gov.au
- **Prudential Standard CPS 230 Operational Risk Management** (determination No. 1 of 2026, F2026L00475) and explanatory statement, paras 6, 32, 48 to 49, legislation.gov.au; APRA, apra.gov.au
- **Prudential Standard CPS 234 Information Security** (F2018L01745), paras 35 and 36, legislation.gov.au
- **Crimes (Amount of a Penalty Unit) Instrument 2026** (F2026N00424), s 5, legislation.gov.au
- **Initial CDD for individuals (Reform)**, AUSTRAC, updated 31 March 2026, austrac.gov.au
- **AML/CTF transitional rules 2026**, AUSTRAC, austrac.gov.au
- **Indicators of suspicious activity for the life insurance sector**, AUSTRAC, updated 30 September 2024, austrac.gov.au
- **26-236MR Hollard fined $2 million for serious insurance claim delay**, ASIC, 9 October 2026, asic.gov.au
- **ASIC's 2026–27 life insurance sector priorities**, supervisory letter, 30 September 2026, asic.gov.au
- **Privacy guidance for reporting entities under the AML/CTF Act**, OAIC, updated 28 August 2026, oaic.gov.au

- **Facial Recognition Technology: a guide to assessing the privacy risks**, OAIC, 29 July 2026, oaic.gov.au
- **New resources on transparency for use of AI and automated decision-making**, OAIC, 30 September 2026, oaic.gov.au
- **Digital ID regulation**, ACCC, updated 21 July 2026, accc.gov.au
- **Business user**, IDMatch (Attorney-General's Department), updated 9 September 2026, idmatch.gov.au
- **Consolidated List**, Australian Sanctions Office, DFAT, list updated 23 July 2026, dfat.gov.au
- **Anti-Money Laundering and Counter-Terrorism Financing Transitional Rules 2026**, Compilation No. 1, 14 May 2026, s 7, and explanatory statement (paras 16, 22, 26), legislation.gov.au
- **Crimes Act 1914**, Compilation No. 167, s 4AA, legislation.gov.au
- **Enforcement actions taken**, AUSTRAC, updated 30 October 2026, austrac.gov.au
- **About AFCA**, Australian Financial Complaints Authority, afca.org.au
- **Assessments calendar**, FATF, fatf-gafi.org