

personr

The ultimate guide to
KYC & AML
compliance

Tranche Two Edition

Contents

Terminology	2-3
Introduction	4
Trends and Challenges	5
AML/CTF Program	6
Tranche Two	7
What goes into an AML Program	8-9
About Personr	10-11
Frequently asked questions	12
What our customers say about us	13
Meet our team	14

Disclaimer: This notice applies to all the recipients of this document; please note that we reserve the right to alter and update it. This notice is provided on an "as it is" basis and for general informational purposes only; none of its contents shall be interpreted as creating an attorney-client relationship between its recipient and Personr, which shall not under any circumstances be held liable for any damages incurred as a result of actions taken or not taken based on the information contained in this document. This document is a result of the work of our professionals and constitutes the intellectual property of Personr. It may not be disclosed, whether as-is or in any way modified, to any third party without prior authorisation by Personr. In the event of such a disclosure, Personr shall be entitled to equitable relief under the laws of Australia.

Key Terminology

Term	Definition
Anti-money Laundering (AML)	Anti-money laundering refers to the suite of laws, obligations and regulatory measures under the AML/CTF Act by which reporting entities must prevent, detect and disrupt the laundering of proceeds from crime, while providing financial intelligence to government and law enforcement to protect Australia's financial system.
Tranche Two	The second phase of Australia's AML/CTF reforms, which extends obligations to additional sectors.
Designated service	A service that is considered a risk for money laundering and terrorism financing if it has a connection to the specified geographic area. Businesses offering these services must report under the AML/CTF Act and have specific responsibilities.
Customer Due Diligence (CDD)	Customer Due Diligence (CDD) is the process of collecting and verifying information about a customer's identity, beneficial ownership, and business activities to assess and manage the risk of money laundering and terrorism financing.
Ongoing Customer Due Diligence (OCDD)	OCDD ensures the information you have about a customer is accurate, reviewed and up to date. This also makes sure you know when it's necessary to get extra information to verify your customer.
Enhanced Customer Due Diligence (ECDD)	ECDD involves doing extra checks on customer identification, collecting extra information and doing additional research about your client. This allows you to decide if suspicious matters need to be reported.
Know Your Customer (KYC) and Know your Business (KYB)	<p>KYC (Know Your Customer) is the process of verifying the identity of individual customers to ensure they are genuine and to prevent financial crimes such as money laundering or fraud.</p> <p>KYB (Know Your Business) is the process of verifying the legitimacy of a business entity and identifying its ultimate beneficial owners to ensure compliance with regulatory and anti-money laundering requirements.</p>
Politically Exposed Person (PEP)	A politically exposed person (PEP) is an individual who holds a prominent public position or public function. This can include an international, or governmental role and also includes the immediate family of said person. PEPs have influence over government budgets, processes, and other influences and can be targets for corruption and bribery attempts.

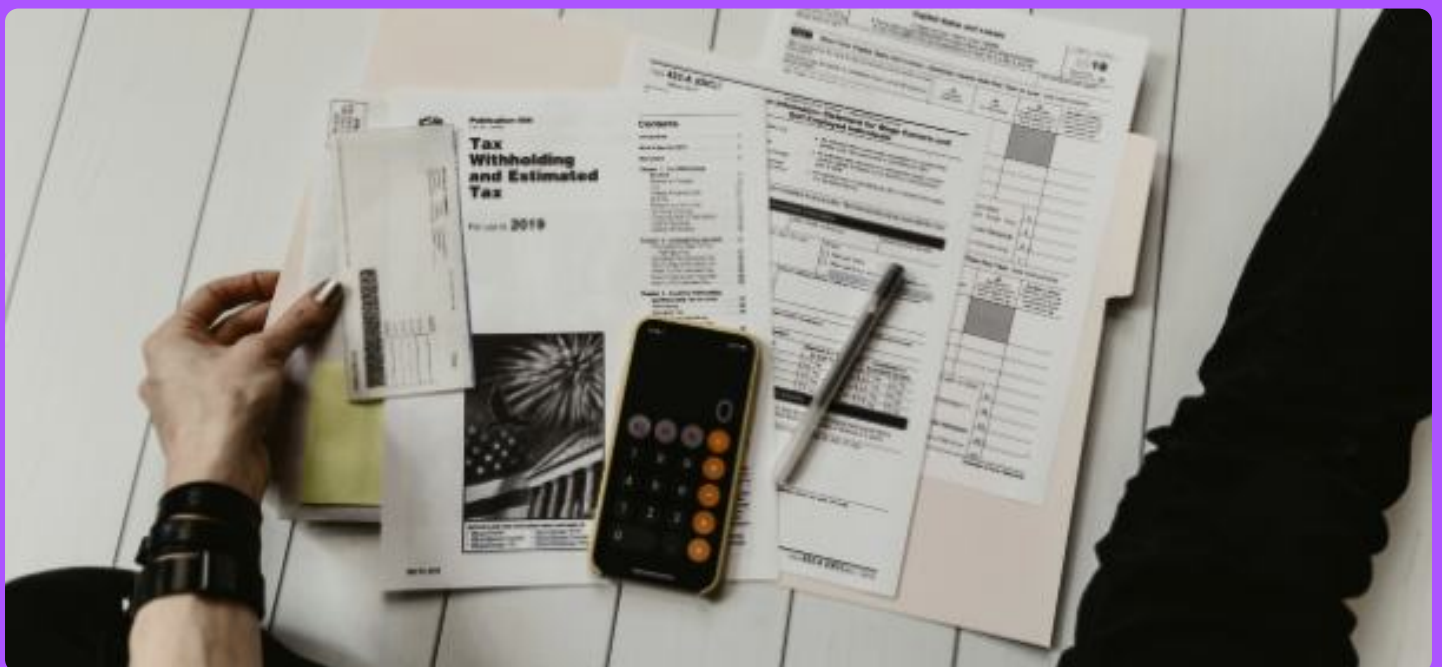
Term	Definition
Ultimate Beneficial Owner (UBO)	A beneficial owner is a person who ultimately holds ownership or control over an entity such as a company, trust, or partnership. This can be through direct means, like owning shares, or indirectly, where someone else holds shares for them. "Control" refers to the power to make decisions on the business financial and operational policies.
Reporting Entity	A reporting entity is a person, business, or organisation that provides a “designated service” under the Anti-Money Laundering and Counter-Terrorism Financing Act and has a geographical link to Australia.
Suspicious Matter Report (SMR)	A Suspicious Matter Report (SMR) is a report that a reporting entity must submit to AUSTRAC when it suspects on reasonable grounds that a transaction or customer may be linked to criminal activity, money laundering, or terrorism financing.
Counter-Terrorism Financing (CTF)	Combating the financing of terrorism. This aims to stop the flow of cash to terrorist organisations. This is a vital step in identifying and preventing money laundering and terrorism.
AUSTRAC	Australian Transaction Reports and Analysis Centre.
Financial Action Task Force (FATF)	The Financial Action Task Force (FATF) is an international body that sets global standards and promotes policies to combat money laundering, terrorism financing, and the financing of weapons proliferation.
Designated Non-Financial Businesses and Professions (DNFBP)	Designated Non-Financial Businesses and Professions (DNFBPs) are non-financial service providers, such as lawyers, accountants, real estate agents, dealers in precious metals or stones, and trust or company service providers, that conduct transactions vulnerable to money laundering or terrorism financing and are therefore subject to AML/CTF obligations.

Recognise and resolve AML mistakes before they become serious problems

As a business owner or manager, you understand the juggling-act of wearing multiple hats to keep your organisation running smoothly. However, one area that often gets overlooked or put off due to its complexity is client identification and AML (anti-money laundering) compliance.

To create a trustworthy business environment and avoid legal and financial ramifications, it's crucial to be proactive in the area of KYC and AML compliance. This involves recognising and addressing compliance mistakes before they escalate into major problems.

Use this essential guide to stay on top of your KYC and AML compliance obligations and ensure that your business is protected from potential legal, reputational, and financial risks.



Trends and Challenges in compliance:

International concern about money laundering and terrorism financing is rising, with financial crime costing up to an estimated US\$3.1 trillion each year.

AUSTRAC is continuing to update and strengthen its AML/CTF framework, with new rules and reforms coming into effect in 2026.

Trends

AUSTRAC regulatory changes

AUSTRAC's changing regulation fits the global trends for AML standards.

Regulations have been changed to identify, mitigate, and manage money laundering and counter-terrorism financing, as well as ensure identity verification services are secure and protect the privacy of Australians.

Tranche Two reforms close the “high-risk” gap by extending KYC, reporting, and record-keeping obligations to DNFBPs.

Updating the 2006 AML/CTF Act strengthens Australia's defences just in time for its next FATF mutual evaluation.

Challenges

Client Verification

Verifying clients can be difficult due to their location, forged documents and understanding beneficial owners. However, with the proper knowledge and tools, navigating these challenges can be easy.

Regulatory requirements

Keeping up with an ever-changing regulatory landscape can be difficult. While regulatory rules are similar worldwide, each country has its own documents and forms regarding compliance. This report will outline Australia's AUSTRAC requirements.

Fraud prevention

Fraud has been rising for many years. The way fraudsters commit the act is also changing, thanks to new technology like AI. Identifying fraud during onboarding is often the most effective way to manage its prevention.

Anti-Money Laundering and Counter-Terrorism Financing program

As a reporting entity, it is required that you establish an AML/CTF program that outlines your adherence to AML/CTF regulations.

An AML/CTF program is a documented framework that explains how your business identifies, mitigates, and manages the risk that its products or services could be used for money laundering or terrorism financing. It plays a critical role in detecting, disrupting, and preventing financial crime, helping to protect your business, your customers, and Australia's financial system.

They apply to all businesses who provide a designated service under the AML/CTF Act, and will soon apply to Tranche Two industries.

Accurate risk assessment and management are essential for compliance. Businesses must identify the specific money laundering and terrorism financing risks they face and establish appropriate controls to manage them.

Mistakes or gaps in identifying these risks can lead to non-compliance and legal penalties. Seeking professional advice when developing your AML/CTF framework can help ensure your program meets AUSTRAC's standards and avoids future enforcement action.

Your AML/CTF program must clearly document the policies, procedures, and controls you use to identify, reduce, and manage risk. It should be risk-based, taking into account the likelihood that your business could be misused for illegal purposes.

This depends on your business's size, type, and complexity, and should consider:

- Who your customers are
- The services you offer
- How you provide these services
- Any dealings with foreign countries

Up-coming changes:

From 1 July 2026, AUSTRAC's regulatory framework will expand under Tranche Two, requiring certain non-financial businesses and professions to implement AML/CTF programs.

These entities will be required to identify and verify customers, report suspicious matters, and maintain risk-based compliance programs consistent with AUSTRAC standards.

What is Tranche Two?

Tranche Two is part of Australia’s Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) reforms. From 1 July 2026, a wider group of professional service providers will come under AUSTRAC regulation.

The reforms aim to close long-criticised gaps by requiring businesses to carry out risk-based customer checks, reporting, and compliance programs, bringing Australia into line with international standards.

This is one of the most significant shifts to Australia’s financial crime landscape in over a decade. Tranche Two is designed to strengthen Australia’s defences against financial crime.

Who it impacts:

The Tranche Two reforms extend regulatory obligations to a broader set of designated service providers, including:

- Accountants
- The Real Estate Sector
- Dealers in Precious Stones and Metals
- Lawyers
- Conveyancers
- Trust and Company Service Providers (TCSPs)



Quick Tip

Create a free account with Personr to get ahead of the Tranche Two regulations so you are prepped, not panicked.

Key Dates to know:

29 August 2025	AUSTRAC tabled the new AML/CTF Rules 2025 in Parliament.
October 2025	Core guidance is expected to be published by AUSTRAC.
Early in 2026	Sector-specific guidance and “starter program kits” for newly regulated sectors.
31 March 2026	Enrolment opens for Tranche Two (newly regulated) sectors.
1 July 2026	AML/CTF obligations commence for Tranche Two entities.

Summary of AML/CTF obligations for Tranche Two Entities

This fact sheet provides an overview of the steps you must take to meet your AML/CTF obligations. It does not cover every requirement or situation in detail.

Key AML/CTF obligations for businesses

☐ Develop and maintain an AML/CTF program:

An AML/CTF program tailored to your business helps safeguard it against the risks of money laundering, terrorism financing, and proliferation financing. The program consists of two key components:

1. Risk assessment – identifies and evaluates the money laundering, terrorism financing, and proliferation financing risks your business may face.
2. Policies, procedures, systems, and controls

☐ Governance and Oversight:

Strong governance ensures accountability for AML/CTF compliance — senior management and the governing body must actively oversee the program, with a dedicated compliance officer responsible for its effective implementation and regular review.

☐ Customer due diligence:

Customer due diligence means understanding who your customers are and identifying any risks of money laundering, terrorism financing, or proliferation financing linked to the services you provide.

You must complete customer due diligence before providing most designated services and continue monitoring customers throughout your business relationship.

If a customer poses a higher risk, you must apply enhanced due diligence measures.

Summary of AML/CTF obligations for Tranche Two Entities

This fact sheet provides an overview of the steps you must take to meet your AML/CTF obligations. It does not cover every requirement or situation in detail.

Reporting Obligations:

If your business is a 'reporting entity' under the AML/CTF Act, you must report certain transactions and suspicious matters to AUSTRAC. These reports help law enforcement identify possible criminal activity and protect Australia's financial system.

In addition, as a reporting entity you must submit an annual AML/CTF compliance report covering the previous calendar year



Suspicious Matter Report

- You must submit an SMR to AUSTRAC when you suspect a person or transaction may be linked to money laundering, terrorism financing, or other criminal activity.



Threshold Transaction Reports

- You must lodge a TTR with AUSTRAC for any cash transaction of \$10,000 or more (or foreign currency equivalent).



Cross-Border Movement Reports

- Report movements of cash or bearer instruments of A\$10,000+ into or out of Australia

Keeping records:

Keeping clear and accurate records helps demonstrate that your business is meeting its AML/CTF obligations. Make sure you record all key activities related to your AML/CTF program and keep these records for at least seven years.

It's good practice to keep:

- A copy of your AML/CTF program
- Customer due diligence information
- Transaction records
- Records of staff training sessions

Identifying and verifying customers with Personr

Let us focus on compliance, so you can focus on your clients.



Client identification and verification

Effortlessly onboard and verify the identity of clients in under 2 minutes, with pre-built and tailored flows to suit your business processes. Clients upload required documents through a secure link, we process their information and provide you with powerful results - including watchlist, sanction and politically exposed person alerts.

Business and UBO Verification

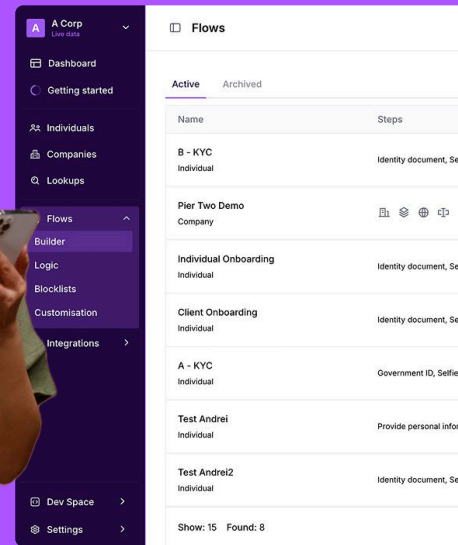
Gain insight into corporate structures and controlling stakes behind-the-scenes. Verify partnerships, trusts, businesses and other entities, including their UBOs and major shareholders. Entities upload their documents through a secure link, verify their UBOs, and we provide you with powerful results - including corporate sanctions and watchlist alerts.



Proof of Verification Certificate

Download accurate and up-to-date records of your client and business verifications, with a range of proof of verification certificates outlining client details, extracted identity data and what they were screened for. Submit to superfunds for easy account-opening, or provide to AUSTRAC for regulatory purposes.

Your single source of truth for AML compliance



Personr is an end-to-end AML compliance platform that serves as the single source of truth for all AML obligations, giving businesses the tools to centralise, track, and manage everything from policy hosting, risk assessments, reporting and record keeping, ensuring every compliance obligation is met in one place.

By using Personr, you are able to verify customers efficiently and spend more time with clients and less time on compliance.

[Book a demo](#) with one of our specialists to learn more.

Our features include:

- KYC 50+ countries
- KYB verification 200+ jurisdictions
- ID Verification
- Global AML Screening
- Biometrics
- Proof of Verification Certificates
- Digital Document Certification
- Entity Verification
- Beneficial Owner Verification
- Document Forgery Check
- Custom Data Collection
- Deepfake Detection
- White-Labeling
- and so much more...



For more information on how we can help transform your business, [book a demo](#) today.

[Book a demo](#)

Frequently Asked Questions



How do I know my data will be safe when I submit it for verification?

Personr employs stringent data security measures, including encryption, secure data storage, and regular security audits, to protect your personal information from unauthorised access or breaches.



Does Personr help me comply with my AUSTRAC obligations?

Yes, we have designed specific flows to help comply with your AUSTRAC obligations.



How long does the identity verification process take?

Our average verification time is 60 seconds for individuals, and three minutes for entities. Exceptions, like blurry photos, may take a little longer.



What if I don't fulfil my obligations?

AUSTRAC is not afraid to review or take action against non-compliant companies and industries.

What our clients are saying



Andrew Lane

Owner and Financial Advisor
at Money & Wealth Management

“It has made it easier and more practical to verify the identification of local and remote clients. Giving peace of mind through what I call a two-way security check.”



Scott Farmer

Owner and Financial Advisor
at Bravium

“Compliance is critical for our financial planning business and having a seamless, efficient and effective solution for AML and identification is a godsend. The client experience is the icing on the cake. We couldn't be happier with the product and the team.”

Meet a few members of the Personr team

Let us focus on compliance, so you can focus on your clients.



Nick Ahrens

Product

nick@personr.co



Charlie Westerman

CEO

charlie@personr.co



Arte Blythe

Marketing

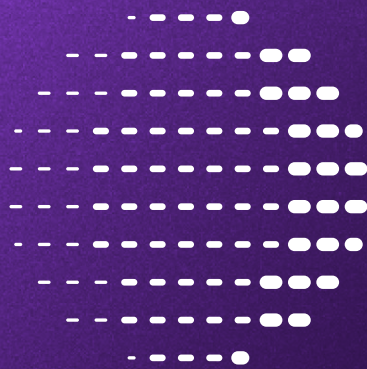
arte@personr.co



Mark O'Hagan

Growth and Sales

mark@personr.co



Give your compliance team [their lunch break back](#)