



# Australia's Money Laundering Scandals

VinciWorks

# Australia's Money Laundering Scandals

Australia is one of only five countries to exempt lawyers, accountants and real estate from anti-money laundering rules. The Australian government has committed to change this, expanding AML/CTF obligations to an additional 100,000 'Tranche-2' entities in Australia, while modernising the AML regime.

These changes come on the back of a series of money laundering scandals which have knocked international confidence in Australian AML efforts. As Australia prepares for a new dawn in AML, be prepared to move on from the AML mistakes of the past.



# Commonwealth Bank of Australia's Money Laundering Scandal: A Deep Dive

The Commonwealth Bank of Australia (CBA), one of the nation's largest and most prestigious financial institutions, was found to have failed in its duty to prevent money laundering on an enormous scale. The bank, which has extensive operations throughout Australia and the Asia-Pacific region, was exposed for neglecting to report over 53,000 suspicious transactions, totalling a staggering \$624 million.

## Background to a scandal

The scandal's roots lay in the misuse of CBA's Intelligent Deposit Machines (IDMs), innovative devices designed to facilitate easy cash deposits for customers. Unfortunately, these machines also provided a perfect conduit for criminals to deposit large sums of cash anonymously, which were subsequently transferred offshore. The bank's internal compliance staff had raised alarms about the suspicious activity, but these warnings fell on deaf ears at the senior management level.

It was the Australian Transaction Reports and Analysis Centre (AUSTRAC), the country's financial intelligence agency, that brought the scandal to light. Their investigation revealed the shocking extent of the bank's failure. Despite internal warnings, CBA had not implemented adequate AML controls to monitor and report suspicious transactions. The culture within the bank was found to prioritise revenue generation over compliance, leading to a systemic breakdown in its duty to prevent illicit activities.

## Systemic Failures

AUSTRAC's findings were damning: the CBA had not just failed to report the transactions, but its senior management had actively ignored internal warnings about the high volume of suspicious activities. This regulatory failure allowed criminals to exploit the bank's systems unchecked for years. The investigation pointed to a weak compliance culture, insufficient AML controls, and a clear disregard for regulatory requirements.

The repercussions for the CBA were swift and severe. AUSTRAC imposed a record-breaking \$700 million fine on the bank, the largest civil penalty in Australian corporate history. The bank's reputation took a significant hit, with customer trust plummeting and its stock value suffering a sharp decline. In response to the scandal, CBA embarked on a comprehensive overhaul of its AML and compliance programs, strengthening its controls and intensifying staff training. Additionally, the bank faced increased regulatory oversight, with requirements to submit regular reports on its progress in improving compliance.

This scandal played out over several years. Between 2012 and 2016, the CBA failed to report the suspicious transactions, and it wasn't until June 2018 that the bank agreed to pay the \$700 million fine to settle the charges with AUSTRAC.

## Westpac and illicit transactions

In a scandal that rocked the financial industry, Westpac Banking Corporation, one of Australia's largest banks, was hit with a record \$1.3 billion fine in 2020 for violating anti-money laundering and counter-terrorism financing (AML/CTF) laws. This scandal revealed deep-rooted systemic failures within the bank and resulted in severe consequences.

Westpac, known for its extensive operations across Australia and the Asia-Pacific region, found itself at the centre of controversy due to its failure to report over 23 million international transactions. These transactions, totalling approximately \$11 billion, potentially facilitated serious crimes, including child exploitation.

The scandal came to light after an investigation by the Australian Transaction Reports and Analysis Centre (AUSTRAC). The investigation unveiled several key issues. Firstly, Westpac failed to report a staggering number of international transactions. Secondly, the bank's inadequate AML/CTF controls allowed customers to misuse its accounts for illicit activities, including child exploitation. Despite internal compliance staff raising concerns about the high volume of unreported transactions, senior management ignored these warnings. The investigation further revealed that the bank had failed to implement adequate AML/CTF controls and ignored regulatory requirements, allowing these illicit activities to go undetected.

## 'Profound failures' at Westpac

The systemic failures within Westpac were profound. The bank had a weak compliance culture that prioritised revenue generation over adherence to AML/CTF regulations. Its controls were insufficient to detect and prevent suspicious transactions. Senior management failed to address compliance concerns, allowing illicit activities to continue unabated. Moreover, the bank consistently ignored warnings from its internal compliance team and failed to comply with regulatory requirements.

The repercussions for Westpac were severe. AUSTRAC imposed a \$1.3 billion fine on the bank, marking the largest civil penalty in Australian corporate history. The scandal significantly damaged Westpac's reputation, leading to a loss of customer trust and a substantial decline in its stock value. In response to the scandal, the bank implemented extensive reforms to its AML/CTF and compliance programs, strengthening its controls and increasing staff training. Additionally, Westpac faced heightened regulatory scrutiny and was required to submit regular reports on its compliance improvements.

The timeline of events spans several years. From 2013 to 2019, Westpac failed to report over 23 million international transactions. In November 2019, AUSTRAC filed a lawsuit against Westpac, and by September 2020, Westpac agreed to pay the record \$1.3 billion fine to settle the case.

## Casinos and money laundering fines

Australian casinos have been embroiled in several anti-money laundering (AML) compliance scandals in recent years, revealing significant lapses in their ability to prevent financial crimes.

In July 2023, the Federal Court ordered two casinos (Crown Melbourne and Crown Perth) to pay a \$450m penalty for breaching AML/CTF Act. The casino's AML/CTF programmes were not based on appropriate risk assessments, did not have appropriate systems and controls to manage the risk, and were not subject to oversight by the board of senior manager.

Similarly, Star Entertainment Group has been under investigation by AUSTRAC, Australia's financial crime regulator, for potential breaches of AML and counter-terrorism financing laws. The investigation, which began with the company's Sydney casino, highlighted ongoing issues with customer due diligence and compliance with AML regulations. This scrutiny has since expanded to include multiple entities within the company, reflecting broader systemic issues within the group.

SkyCity Entertainment Group has also faced serious allegations of non-compliance with AML and counter-terrorism financing laws at its Adelaide casino. AUSTRAC's investigation revealed that SkyCity failed to properly assess money laundering risks, implement adequate transaction monitoring programs, and conduct appropriate due diligence on high-risk customers. As a result, the company has set aside significant funds to cover potential penalties and legal costs associated with these breaches. The group reached an agreement to pay a total penalty of AU\$67m over historical anti-money laundering and counter-terrorism financing failings at its Adelaide casino.

## Proliferation financing cases

AUSTRAC released their first national proliferation financing risk assessment at the end of 2022, and in it they highlighted Australian financial services and infrastructure being used to procure dual use goods and evade sanctions, and certain professionals like lawyers and accountants facilitating proliferation financing through shell companies and export issues.

Australia is uniquely at risk for proliferation financing given its extensive economic relations and trade with Asian markets which are popular destinations for transshipments to high risk countries like North Korea, Iran and Pakistan. Australia also has a high volume of dual-use goods and proliferation-sensitive exports. The large mining industry and exports of materials which are subject to UN sanction also has a risk of diversion to PF networks. The different way of regulating lawyers, accountants and company service providers in Australia caused AUSTRAC to highlight this as a risk factor.

According to AUSTRAC's 2022 PF National Risk Assessment, the key proliferation financing threats facing Australian professional services are:

- ✓ Procurement of dual-use goods and sanctions evasion
- ✓ Abuse of Australia-based corporate structures
- ✓ Use of designated non-financial businesses and professions (DNFBPs)



## Sydney man jailed for North Korean arms shipments

Australia actually saw its first proliferation financing prosecution in 2021 when a Sydney man pleaded guilty to providing brokering services for selling arms related material from North Korea. Chan Han Choi was arrested in 2017 and accused of brokering five transactions for missiles, petrol, and coal on behalf of North Korea to entities in Indonesia. The New South Wales Supreme Court sentenced the man to three and a half years in prison.

## Troll Holdings proliferation financing

In 2022, OFAC settled a case with an Australian freight and logistics company called Toll Holdings. Toll had processed thousands of transactions between North Korea, Iran and Syria, and had used the US financial system to do so. This was for the benefit of sanctioned individuals and entities, and it was due to a complete failure of compliance controls from the company. Toll didn't have in place policies of controls which matched the complexity of its operations. Toll had over 600 payment, invoicing and data systems spread across its business units, few of which talked to each other. The breaches only came to light when an internal whistleblower raised concerns about the company's compliance with US sanctions. The company actually tried to mitigate its risk by ceasing all business with US sanctioned countries in 2016, but the company didn't fully implement policies and procedures to stop payments from sanctioned entities. It didn't test its procedures either, so customers based in US sanctioned countries could still use the company's services, and it took another year for controls to finally prevent shipments to sanctioned countries.

## Sydney couple jailed for Iran sanctions evasion

In 2019, a New South Wales-based couple was convicted and sentenced for contravening

Australian sanctions law relating to Iran. The crimes involved the procurement and supply of approximately 90 tonnes of export-sanctioned nickel alloys to Iran. The couple established and used a joint business venture to procure the production of the nickel alloy from a UK company. Then the nickel alloy was shipped from the UK to a company in Dubai owned by Iran, then forward to Iran in breach of Australian sanctions.

## Taking on clients near PF high risk borders

In 2018, an international bank submitted a suspicious matter report to AUSTRAC regarding Company X. The company had declared its main place of business in the Dalian

province in China. This region is near the border with North Korea and considered a high-risk region for sanctions evasion and proliferation financing activity. Company X received a number of incoming transfers from shipping companies located in Hong Kong and China, and then attempted to remit these funds to an unknown beneficiary in Vladivostok,

Russia. This was a clear risk of proliferation financing related to geographic risk.

## How to mitigate the risk of a scandal

These scandals underscore the importance of robust AML/CTF controls in detecting and preventing suspicious transactions. It highlights the necessity of holding senior management accountable for ensuring compliance with AML/CTF regulations and addressing internal warnings. Regulatory authorities must maintain stringent oversight and enforce compliance to prevent systemic failures. Continuous training for staff is also essential to ensure they are equipped to detect and report suspicious activities effectively.

It's also a stark reminder of the critical importance of effective AML controls and the need for a strong compliance culture within regulated entities. It underscores the necessity of holding senior management accountable for regulatory adherence and responding promptly to internal warnings. Furthermore, it highlights the role of regulatory bodies in maintaining stringent oversight and enforcing compliance to prevent such systemic failures. As many of these institutions work to rebuild their reputation and trust, the lessons from these scandals will undoubtedly shape the future of financial compliance and regulatory practices.

These scandals highlights several critical compliance lessons for Australian regulated entities when tackling money laundering compliance:

### 1. Robust AML/CTF Controls

Implementing and maintaining strong AML/CTF controls is essential. This includes:

- ✓ Regularly updating and enhancing systems to detect and report suspicious transactions.
- ✓ Utilising advanced technology and

software to monitor transactions and flag potential risks.

### 2. Management Accountability

Senior management must take ownership of AML/CTF compliance:

- ✓ Ensure that compliance policies and procedures are effectively implemented and followed.
- ✓ Respond promptly and decisively to internal warnings and compliance issues.
- ✓ Foster a culture where compliance is prioritised and not overshadowed by revenue goals.

### 3. Continuous Staff Training

Regular training programs for all staff levels are crucial:

- ✓ Educate employees on the latest AML/CTF regulations and emerging threats.
- ✓ Provide practical training on identifying and reporting suspicious activities.
- ✓ Promote a culture of vigilance and accountability throughout the organisation.

### 4. Effective Communication and Reporting

Maintaining clear communication channels is vital:

- ✓ Ensure that internal reporting mechanisms are efficient and accessible.
- ✓ Encourage staff to report suspicious activities without fear of retribution.
- ✓ Facilitate regular updates and communication between compliance teams and senior management.

## 5. Regulatory Vigilance and Cooperation

Engage proactively with regulatory authorities:

- ✓ Regularly review and comply with all regulatory requirements and guidelines.
- ✓ Maintain open lines of communication with regulators and report issues promptly.
- ✓ Cooperate fully with regulatory investigations and audits.

## 6. Periodic Risk Assessments

Conduct regular risk assessments to identify and mitigate potential vulnerabilities:

- ✓ Assess the effectiveness of current AML/CTF controls.
- ✓ Identify high-risk areas, products, and customers that may require enhanced scrutiny.
- ✓ Adjust policies and procedures based on the findings of risk assessments.

## 7. Technology Integration

Leverage technology to enhance compliance efforts:

- ✓ Implement automated systems for monitoring and reporting transactions.
- ✓ Use data analytics to identify patterns and anomalies indicative of money laundering.
- ✓ Ensure systems are scalable and adaptable to evolving regulatory requirements and threats.

## 8. Third-Party Due Diligence

Conduct thorough due diligence on third parties, including customers, partners, and suppliers:

- ✓ Verify the identity and legitimacy of third parties.
- ✓ Monitor third-party activities for signs of money laundering or other illicit activities.
- ✓ Establish clear policies for terminating relationships with non-compliant third parties.

## 9. Documentation and Record-Keeping

Maintain comprehensive and accurate records of all transactions and compliance activities:

- ✓ Ensure documentation is readily available for regulatory reviews and audits.
- ✓ Keep detailed records of internal compliance reviews and risk assessments.
- ✓ Document all training programs and staff certifications.

## 10. Ethical Corporate Culture

Foster an ethical corporate culture where compliance is integral to the business:

- ✓ Lead by example from the top down.
- ✓ Reward and recognize employees who demonstrate strong compliance behaviours.
- ✓ Create a zero-tolerance policy for non-compliance and enforce it consistently.

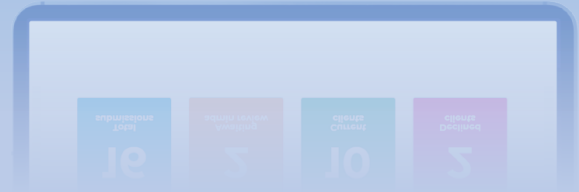
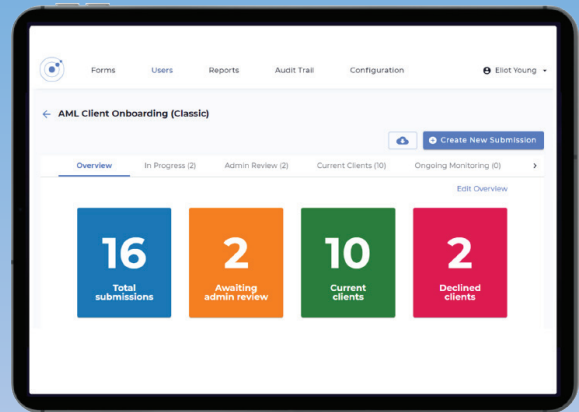
**By integrating these lessons into their compliance strategies, Australian regulated entities can better protect themselves against money laundering risks and ensure they meet regulatory expectations in advance of Tranche-2 reforms which are set to revolutionise Australian anti-money laundering.**



# VinciWorks' AML Client Onboarding Solution - Omnitrack

Ensure seamless AML compliance across your firm with Omnitrack's adaptive client onboarding solution. Our platform streamlines risk assessments, client due diligence, and ongoing monitoring, offering unparalleled flexibility and industry-specific guidance.

Omnitrack, VinciWorks' [AML client onboarding solution](#) enhances both the risk assessment and document collection aspects of client onboarding. Our template workflows adapt to the specific risks posed by each client, based on factors such as jurisdiction, type of entity and industry. This allows you to make informed choices about each client using the risk-based approach. Our comprehensive workflows incorporate industry-specific guidance such as LSAG for law firms.



## How does your firm handle complex AML requirements?

Law firms, accountants, financial institutions, and other regulated entities face rigorous AML processes that vary by industry and jurisdiction. Static forms or outdated software pose significant compliance risks. Omnitrack's AML onboarding solution streamlines these processes with adaptive template workflows that adjust to client-specific risks, ensuring full compliance and informed decision-making.

## Can your client onboarding process adapt to specific needs?

Omnitrack's flexibility allows firms to customise workflows to suit their unique requirements. From risk scoring to sanctions checking, our solution ensures all client details are collected, reviewed, and monitored efficiently. With features like conditional logic and industry-specific guidance, Omnitrack supports thorough client due diligence and regulatory compliance.



# Contact us

[www.vinciworks.com](http://www.vinciworks.com)

[enquiries@vinciworks.com](mailto:enquiries@vinciworks.com)

+44 (0) 208 815 9308

VinciWorks