



Australian Government
AUSTRAC

FIGHTING
FINANCIAL
CRIME
TOGETHER

A photograph of a modern city skyline with glass skyscrapers, partially obscured by a large, dark teal diagonal graphic element that runs from the top left towards the bottom right.

AUSTRALIA'S OTHER DOMESTIC BANKS

MONEY LAUNDERING AND TERRORISM FINANCING RISK ASSESSMENT

COPYRIGHT

© Commonwealth of Australia 2021

All material presented in this publication is provided under a Creative Commons Attribution 4.0 International licence (www.creativecommons.org/licenses).

For the avoidance of doubt, this means this licence only applies to material as set out in this document.

The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 licence (www.creativecommons.org/licenses).



USE OF THE COMMONWEALTH COAT OF ARMS

The terms under which the Coat of Arms can be used are detailed on the It's an Honour website (www.pmc.gov.au/government/its-honour).

This risk assessment is intended to provide a summary and general overview; it does not assess every risk or product relevant to Australia's other domestic banks. It does not set out the comprehensive obligations under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act), the *Anti Money Laundering and Counter Terrorism Financing (Prescribed Foreign Countries) Regulations 2018* (AML/CTF Regulations) or the *Anti Money Laundering and Counter Terrorism Financing Rules Instrument 2007 (No. 1)* (AML/CTF Rules). It does not constitute nor should it be treated as legal advice or opinion. The Commonwealth accepts no liability for any loss suffered as a result of reliance on this publication. AUSTRAC recommends that independent professional advice be sought.

CONTACT US

If you have questions about your AUSTRAC compliance obligations, or enquiries regarding the licence and any use of this report please email contact@austrac.gov.au or phone 1300 021 037 (within Australia).

AUSTRAC is committed to continual improvement and values your feedback on its products. We would appreciate notification of any outcomes associated with this report by contacting AUSTRAC at austrac.gov.au/contact-us/form.

CONTENTS

EXECUTIVE SUMMARY	03
PURPOSE	09
BACKGROUND	11
METHODOLOGY	13
OTHER DOMESTIC BANKS: REPORTING TO AUSTRAC	16
CRIMINAL THREAT ENVIRONMENT	18
Money laundering	20
Terrorism financing	22
Predicate offences	24
VULNERABILITIES	32
Customers	33
Products and services	41
Delivery channels	49
Foreign jurisdictions	54
CONSEQUENCES	58
RISK MITIGATION STRATEGIES	62
APPENDICES	66

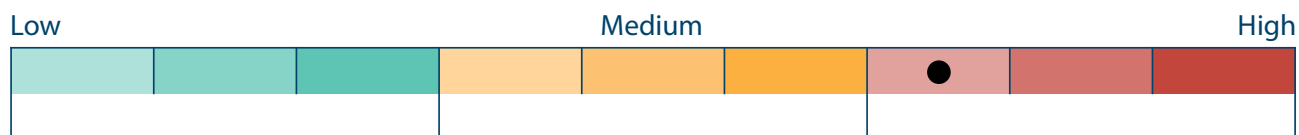


EXECUTIVE SUMMARY

For the purposes of this report, other domestic banks are Australian-owned authorised deposit-taking institutions (ADIs) that are not major banks, community owned or mutual banks. As at June 2021, 12 other domestic banks operate in Australia, providing services to at least five million customers.

The characteristics and activities of individual other domestic banks vary significantly. Consequently, the money laundering and terrorism financing (ML/TF) risks associated with individual other domestic banks also varies. The risk rating criteria used in this assessment is designed to provide an overall rating for the subsector.

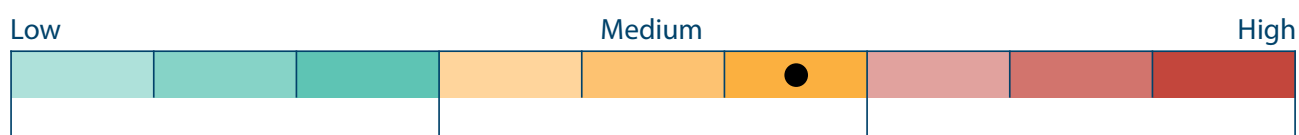
OVERALL RISK RATING



AUSTRAC assesses the overall ML/TF risk associated with other domestic banks as **high**. This rating is based on assessments of the criminal threat environment, inherent vulnerabilities in the subsector and consequences associated with the criminal threat.

Where possible this assessment considers the risks associated with other domestic banks in the context of AUSTRAC's entire reporting population.

CRIMINAL THREAT ENVIRONMENT



AUSTRAC assesses the threat of ML/TF facing other domestic banks as **medium**.

The criminal threat environment is varied and complex. It ranges from simple offences committed by individuals to sophisticated methodologies used by transnational, serious and organised crime groups.¹ The primary threats facing other domestic banks are frauds, money laundering, scams and tax evasion.

The subsector is also exposed to terrorism financing, and criminal proceeds from a range of other predicate crimes such as trafficking in illicit drugs and other goods, bribery and corruption, child exploitation and sanctions violations.

¹ Transnational, serious and organised crime covers a wide range of the most serious crime threats impacting Australia. These are listed in the **Glossary** in **Appendix A**.

MONEY LAUNDERING

The nature and extent of money laundering threats facing other domestic banks is assessed as **high**.

The subsector is exposed to a high volume of suspected money laundering activities. Observed methodologies include sophisticated attempts to conceal illicit funds flows by serious and organised crime groups and opportunistic criminal entities.

Approximately 27 per cent of suspicious matter reports (SMRs) reviewed for this risk assessment related to suspected money laundering. Other domestic banks were also the second most common banking subsector identified in money laundering-related intelligence reports reviewed for this report.

The most common money laundering themes observed in the subsector include:

- suspected misuse by individual customers rather than company customers
- suspected placement through structured cash deposits, often by third parties and suspected money mules
- suspected layering through multiple transaction accounts and across multiple ADIs
- customers combining two or more money laundering methods to evade detection and avoid triggering a report to AUSTRAC.

TERRORISM FINANCING

The nature and extent of terrorism financing threats facing other domestic banks is assessed as **medium**.

While other domestic banks are exposed to suspected terrorism financing activity, associated values are often extremely low and methods are largely unsophisticated and unvaried. For example, little or no effort is made to obscure the source of funds. In some cases, attempts are made to obscure the end beneficiary by sending funds through intermediaries in the destination jurisdiction.

Across the entire reporting population, other domestic banks submitted six per cent of all terrorism financing-related SMRs in the reporting period, and were observed in 14 per cent of terrorism financing-related intelligence reports reviewed for this report. A moderate number of individuals who were charged with a terrorism-related offence between 2014 and 2019 were identified in reports submitted by other domestic banks.

PREDICATE OFFENCES

The nature and extent of threat posed by predicate offending involving other domestic banks is assessed as **high**.²

Predicate offending is varied, complex and was the most common threat category identified in SMRs and intelligence reports reviewed for this report. Key predicate offences include frauds, scams, tax evasion and drug trafficking. Values associated with these activities were sometimes high – in some cases up to tens of millions of dollars.

² For the purposes of this report, a predicate offence is a criminal offence that generates proceeds of crime, or other related crimes such as identity fraud.

Collectively, frauds and scams were the most common predicate offences observed in SMRs and intelligence reports reviewed for this report. While most cases were relatively simplistic in nature, a small number were more sophisticated and had potentially significant consequences. Identity fraud and loan application fraud were the most common fraud types, and the most common scam types were remote access and romance scams.^{3,4} Many scams and frauds were committed online, which is consistent with the subsector's extensive use of remote delivery services.

Suspected tax evasion was observed in a small number of SMRs and approximately 20 per cent of intelligence reports reviewed for this report. While the number of reports relating to personal tax evasion and corporate tax evasion were similar, the associated harm of corporate tax evasion is likely higher with average report values nearly double those relating to personal tax evasion.

The subsector is also exposed to high-impact offences such as child exploitation, bribery and corruption, sanctions violations and trafficking in illicit goods.

VULNERABILITIES



AUSTRAC assesses other domestic banks are subject to a **high** level of inherent ML/TF vulnerability.

Since the characteristics and activities of each reporting entity vary significantly, the ML/TF vulnerabilities associated with each business also varies. The risk rating criteria used in this assessment is designed to provide an overall rating for the subsector. AUSTRAC acknowledges not all vulnerabilities will be relevant for every reporting entity. In addition, some vulnerabilities relate to the nature and characteristics of banking products in general and are not specific to the subsector.

3 Remote access scams (also known as technical support scams) usually involve scammers contacting people over the phone to get access to their computers in an effort to steal their money.

4 Romance scams involve criminals taking advantage of people looking for romantic partners by pretending to be prospective companions – often online. These criminals play on emotional triggers in an effort to get the victim to provide money or sensitive personal details.

Factors that most expose the subsector to ML/TF include:

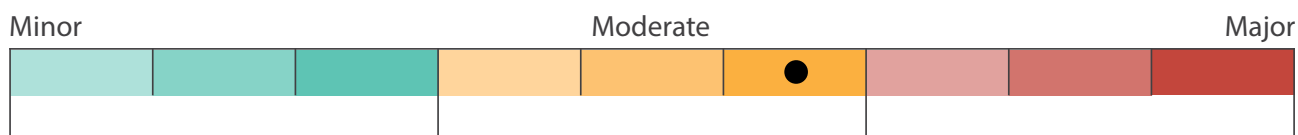
- a **large customer base** including a high proportion of **higher-risk customers**, which can present across a range of categories including:
 - known or suspected criminals⁵
 - politically exposed persons (PEPs)
 - companies, trusts and other legal entities
 - designated non-financial businesses and professions (DNFBPs)⁶
 - financial institutions⁷
 - temporary visa holders.
- products and services that can be used to **store and move funds** into and out of the subsector such as:
 - transaction accounts
 - loan accounts
 - trust accounts.
- a **high exposure to cash**
- delivery channels that facilitate **cash deposits** and **withdrawals**
- an increasing use of **remote service delivery channels**, particularly online banking and ATMs. These channels can offer criminals anonymity, facilitate identity fraud and other financial crimes, and make it harder to detect unusual or suspicious transactions.
- The subsector has a high exposure to foreign jurisdictions, although this is concentrated in a small number of larger banks.

⁵ These entities were identified by data-matching partner agency criminal lists against AUSTRAC reports. Further details of data-matching activities is provided in the **Methodology** section. AUSTRAC assesses that other domestic banks do not knowingly provide products or services to known or suspected criminals.

⁶ The Financial Action Task Force (FATF) *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations (2012- 2020)* define DNFBPs as casinos, real estate agents, precious metal/precious stone dealers, lawyers, notaries, other independent professionals and accountants and trust company service providers. The FATF considers these entities and the services they provide as being highly vulnerable to the risks of exploitation for money laundering and terrorism financing purposes.

⁷ Please refer to the **Glossary** in **Appendix A** for a definition of 'financial institutions'.

CONSEQUENCES



AUSTRAC assesses the overall consequences of ML/TF activity in the subsector as **moderate**.

CUSTOMERS

AUSTRAC assesses criminal activity likely has **moderate** consequences for customers. The most significant impacts relate to financial loss, emotional distress caused by fraud and scam-related offences, and reputational damage, particularly for business customers.

INDIVIDUAL BUSINESSES AND THE SUBSECTOR

Criminal activity can have **moderate** financial, reputational or operational consequences for other domestic banks. These consequences vary between reporting entities and largely depend on the extent to which they understand and mitigate their ML/TF risks, as well as their ability to absorb potential financial losses or withstand reputational damage.

AUSTRALIAN FINANCIAL SYSTEM AND COMMUNITY

Significant or systemic criminal exploitation of the subsector could cause **major** damage to Australia's international economic reputation by undermining the security and safety of Australia's financial sector. Predicate offences such as drug trafficking, frauds and scams also inflict direct societal harms to the Australian community.

NATIONAL AND INTERNATIONAL SECURITY

Criminal exploitation of other domestic banks can have **major** consequences for national and international security. Money laundering through the subsector can allow criminals to preserve illicit assets and finance new crimes. It can help fund transnational, serious and organised crime groups to grow larger and stronger and their activities can impact both national and international security interests.

The potential impacts of terrorism financing can be significant. They include enabling and sustaining activities of Australian foreign terrorist fighters or enabling terrorist acts in Australia or overseas.

RISK MITIGATION STRATEGIES

Individual reporting entities apply risk mitigation strategies with varied results. Overall other domestic banks continue to invest in more advanced ML/TF risk mitigation systems and controls. However, some smaller domestic banks have less sophisticated AML/CTF programs and fewer resources to invest in risk mitigation strategies and financial crime and compliance teams. Some banks could make improvements to transaction monitoring programs and SMR submissions to AUSTRAC.



PURPOSE

This assessment provides specific information to other domestic banks on the ML/TF risks the subsector faces at the national level. Its primary aim is to assist the subsector to identify and disrupt ML/TF risks to Australia's financial system, and report suspected crimes to AUSTRAC.

This risk assessment is not intended to provide targeted guidance or recommendations as to how reporting entities should comply with their AML/CTF obligations. However, AUSTRAC expects other domestic banks to review this assessment to:

- inform their own ML/TF risk assessments
- strengthen their risk mitigation systems and controls
- enhance their understanding of risk in the subsector.

AUSTRAC acknowledges the diversity across the subsector and recommends this assessment be considered according to each business's individual operations.

ASSESSING ML/TF RISK IN AUSTRALIA'S BANKING SECTOR

In September 2018, Australia's Minister for Home Affairs announced nearly \$5.2 million in funding to AUSTRAC to work with industry partners on additional targeted national ML/TF risk assessments for Australia's largest financial sectors – the banking, remittance and gambling sectors.

This report represents one of four risk assessments on Australia's banking sector that are being completed under this program of work. The other assessments focus on major domestic banks, foreign subsidiary banks and foreign bank branches operating in Australia. This approach recognises discrete segments within Australia's banking sector, each facing unique ML/TF risks which may not necessarily be shared across the entire sector.

In 2019, AUSTRAC released its ML/TF risk assessment of Australia's mutual banking subsector. While this report rated the overall ML/TF risk as **medium**, it found the mutual banking sector had a high level of vulnerability to financial crime.

AUSTRAC recommends interested individuals review all banking related risk assessments for a comprehensive picture of the entire sector.



BACKGROUND

For the purposes of this assessment, other domestic banks are Australian-owned ADIs that are not major banks or community owned or mutual banks.

As at June 2021, 12 other domestic banks operate in Australia, providing services to at least five million customers. For the purposes of this assessment, 10 reporting entities have been included in scope as two of the 12 other domestic banks were granted licences by APRA after the reporting period end-date of 31 March 2019.

Combined, other domestic banks hold \$435 billion in assets, representing approximately nine per cent of the ADI market. Other domestic banks offer an extensive range of products and services to retail, corporate, and some institutional and private banking customers. Refer to the **Glossary** in **Appendix A** for an explanation of these terms.

Australia's other domestic banks are recognised as both licensed ADIs and reporting entities providing designated services under the AML/CTF Act. Under the AML/CTF Act, other domestic banks are required to have a compliant AML/CTF program and report to AUSTRAC:

- suspicious matter reports (SMRs)
- threshold transaction reports (TTRs)
- international funds transfer instructions (IFTIs).

Banks in the subsector are also required to provide AUSTRAC with AML/CTF compliance reports.

The characteristics and activities of individual banks across the subsector vary greatly with significant variety in factors like the number and types of customers, and products and services offered. Consequently, the ML/TF risks associated with individual businesses also varies.

AUSTRAC acknowledges not all risks will be relevant for every reporting entity. In addition, some risks relate to the nature of banking products in general, and are not attributes specific to other domestic banks. The risk rating criteria used in this assessment is designed to capture an overall rating for the subsector.

SIZE OF THE SUBSECTOR⁸



12

Number of reporting entities



5 MILLION

Number of customers



Total resident assets

9% of all ADIs



Total deposits

7% of all ADIs



Total loans to households

9% of all ADIs



Loans to households (housing only)

12% of all ADIs

⁸ APRA, *Monthly authorised deposit-taking institution statistics backseries: July 2020*, apra.gov.au/monthly-authorized-deposit-taking-institution-statistics.



METHODOLOGY

The methodology used for this risk assessment draws on Financial Action Task Force (FATF) guidance, which states that ML/TF risk can be seen as a function of criminal threat, vulnerability and consequence. In this assessment:

- **Criminal threat environment** refers to the nature and extent of ML/TF and relevant predicate offences in the subsector.
- **Vulnerability** refers to the characteristics of other domestic banks that make them attractive for ML/TF purposes. This includes features that can be exploited, such as customer types, products and services, delivery channels and the foreign jurisdictions with which the subsector transacts. This report assesses inherent ML/TF vulnerability only.
- **Consequence** refers to the impact or harm that ML/TF activity within the subsector may cause.

This assessment considered 18 risk factors across criminal threat environment, vulnerability and consequence. Each risk factor was equally weighted and an average risk score was determined for each of the three categories. Each category was equally weighted and an average risk score determined the overall inherent risk rating for the subsector.

This report also discusses the level of **risk mitigation strategies** implemented across the subsector. This includes measures that are explicitly mandated under AML/CTF legislation, and other practices reporting entities implement to mitigate ML/TF risk. This section was not risk-rated by AUSTRAC, and overall findings were not applied in the final risk scoring. Reporting entities can consider their level of implementation of risk mitigation strategies against inherent ML/TF vulnerabilities identified in this report to help determine their overall residual risk of criminal misuse.

Further information on the methodology and how this was applied can be found in **Appendix B**.

Five main intelligence inputs informed the risk ratings in this assessment:

1. Analysis of AUSTRAC transaction reports, compliance reports and other holdings, including 2,698 SMRs submitted by other domestic banks between 1 April 2018 and 31 March 2019 (the **SMR sample**).⁹ See the call-out box **Labelling the SMR sample** on page 15 for more detail.
2. A comprehensive review of almost 700 AUSTRAC and partner agency intelligence reports produced between January 2018 and February 2019. Six per cent of these related to other domestic banks (the **IR review**).¹⁰
3. The results of data-matching (the **data-matching** exercise) of IFTIs, TTRs and SMRs submitted to AUSTRAC by other domestic banks between 30 March 2018 and 1 April 2019 and criminal entities who were:
 - recorded as a member of a significant national or transnational criminal group as at May 2020
 - charged with a money laundering or proceeds of crime-related offence between 1 January 2017 and 31 December 2018¹¹
 - charged with a terrorism-related offence between 1 January 2014 and 31 December 2018.¹²
4. Open source information, including public information produced by government agencies, academic institutions, reporting entities and the media.
5. Feedback and professional insights offered during consultations with a range of partner agencies and other domestic bank representatives, as well as industry experts and associations.

⁹ SMRs should be considered indicative of suspicious behaviour only and not conclusive in their own right. This is because reporting entities generally lack visibility of certain threat elements, for example how a customer generates suspected criminal proceeds. To ensure accuracy of ML/TF indicators (threats and vulnerabilities) outlined in the SMR sample, AUSTRAC officers manually reviewed and categorised each report.

¹⁰ The number of intelligence reports may not reflect the actual extent of criminality, and may understate the true extent of ML/TF threats and criminal misuse of the subsector. This is because AUSTRAC does not have visibility of all partner agency intelligence reporting.

¹¹ Includes persons charged under Division 400 of the *Criminal Code* (Cth) and/or sections 81 and 82 of the *Proceeds of Crimes Act 2002* (Cth).

¹² Includes persons charged with a 'Terrorism offence' in section three of the *Crimes Act 1914* (Cth) and/or offences contrary to the *Crimes (Foreign Incursion and Recruitment) Act 1978* (Cth).

LABELLING THE SMR SAMPLE

SMRs are indicative of suspicious behaviour only and are not conclusive in their own right. For example, reporting entities often have no visibility of how a customer generates criminal proceeds. As a result, reporting entities may be unable to include specific information about suspected threat types.

To ensure accurate and consistent insights from SMRs, AUSTRAC analysts reviewed and categorised each report in the SMR sample against 414 possible labels grouped by:

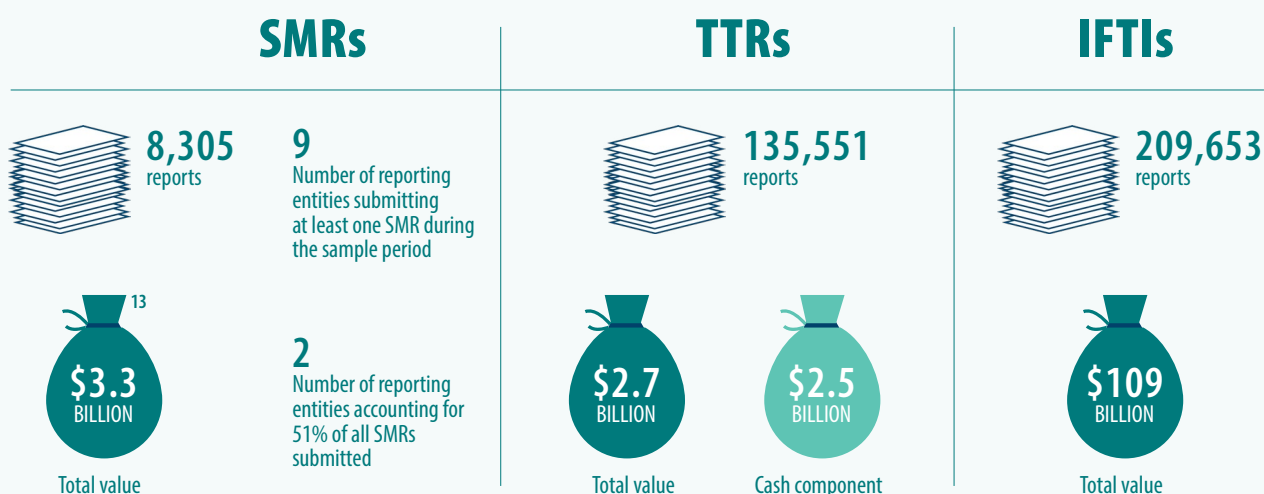
- criminal threat
- suspicious transactional activity
- products and services
- customer type
- entity attribute
- foreign jurisdiction.

For example, a single SMR could be categorised with multiple labels as follows:

SMR CATEGORY	LABEL (EXAMPLE)
Criminal threat	Drug trafficking Money laundering
Suspicious transactional activity	Cash deposits Structuring Money mules
Products and services	Transaction account
Customer type	Company
Entity attribute	Third party DNFBP lawyer
Foreign jurisdiction	Jurisdiction 'X'

OTHER DOMESTIC BANKS: REPORTING TO AUSTRAC

REPORTS SUBMITTED BY OTHER DOMESTIC BANKS BETWEEN 1 APRIL 2018 AND 31 MARCH 2019



¹³ Caution should be exercised when interpreting the recorded value in SMRs. The recorded value may not necessarily relate to suspected criminal misuse or terrorism financing, and may include transactions that occurred outside the reporting period. This is because a reporting entity may not form a suspicion and submit an SMR until multiple transactions are conducted – some of which may have occurred outside the reporting period.

FEEDBACK FOR REPORTING ENTITIES REGARDING SMR SUBMISSIONS

There is significant variance in the quality of SMRs submitted by other domestic banks. While some SMRs included a high level of detail and demonstrated robust enhanced customer due diligence (ECDD) activities, many reports were trigger-based and provided low quality intelligence for law enforcement (i.e. the reports only included the information triggering the alert with no additional context or background provided). In addition, two reporting entities submitted over half of all SMRs during the reporting period. Refer to the **Risk mitigation strategies** section for more details.

SMRs PLAY A CRUCIAL ROLE IN LAW ENFORCEMENT

Under the AML/CTF Act, reporting entities have an obligation to report suspicious matters to AUSTRAC. A reporting entity must submit an SMR under a number of circumstances, including if they suspect on reasonable grounds that information they have concerning a service they are providing, or will provide, may be relevant to the investigation or prosecution of a crime.

SMRs provide valuable intelligence to AUSTRAC. Working with its partner agencies, AUSTRAC pieces together intelligence from a range of sources to develop a picture of criminal activities and networks. Many of AUSTRAC's partner agencies – including the Australian Federal Police (AFP), the Australian Criminal Intelligence Commission (ACIC) and the Australian Taxation Office (ATO) – have access to SMRs to generate investigative leads and conduct further analysis and investigation. High-quality, accurate and timely SMRs give AUSTRAC and our partners the best chance to detect, deter and disrupt criminal and terrorist activity.

WHAT HAPPENS AFTER AUSTRAC RECEIVES AN SMR?

When an SMR is submitted to AUSTRAC, it is processed to detect crime types and surface high priority matters for immediate analysis. Reports and alerts are then assigned to AUSTRAC intelligence analysts to assess and respond in accordance with our national security and law enforcement intelligence priorities.

Additionally, through direct online access to AUSTRAC's intelligence system, SMR information is available to over 4,000 authorised users from more than 35 of AUSTRAC's partner agencies to inform their intelligence gathering efforts and investigations.

REFORMS TO 'TIPPING OFF' RESTRICTIONS

In December 2020, the Australian Parliament passed the *Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Act 2020* (the Amendment Act) to implement the next phase of reforms to the AML/CTF Act.¹⁴ The Amendment Act includes, among other things, reforms to the 'tipping off' provisions under section 123 of the AML/CTF Act to expand the exceptions to the prohibition on tipping off to permit reporting entities to share SMRs and related information with external auditors, and foreign members of corporate and designated business groups.

Importantly, the exception allows reporting entities to share SMR information with other members of its designated business group or corporate group, including members that may be located offshore, as long as the member is regulated by laws of a foreign country that give effect to some or all of the FATF's Recommendations.

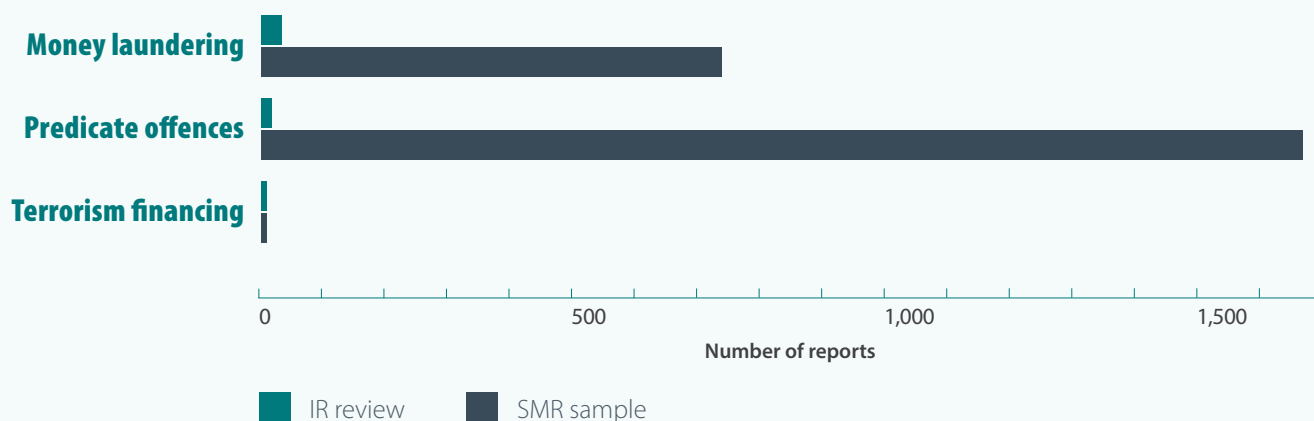
¹⁴ The reforms introduced by the Amendment Act commenced on 17 June 2021.

CRIMINAL THREAT ENVIRONMENT



CRIMINAL THREAT ENVIRONMENT FACTOR	RATING
Money laundering	●
Terrorism financing	●
Predicate offences	●

OTHER DOMESTIC BANKS: DETECTED THREATS



AUSTRAC assesses the criminal threat environment facing Australia's other domestic banks as **medium**.

The criminal threat environment refers to the nature and extent of ML/TF and predicate offences associated with Australia's other domestic banks.

The criminal threat environment is varied and complex. It ranges from simple offences committed by individuals to the use of more sophisticated methods by transnational, serious and organised crime groups. Additionally, the SMR sample and IR review indicate that the absolute extent of criminal activity identified with a nexus to the subsector is moderate to high. The primary threats facing other domestic banks are frauds, money laundering, scams and tax evasion. The subsector is also exposed to terrorism financing, and criminal proceeds from a range of other predicate crimes such as trafficking in illicit drugs and other goods, child exploitation, bribery and corruption and sanctions violations.

MONEY LAUNDERING

AUSTRAC assesses the nature and extent of money laundering threats facing other domestic banks as **high**.

This assessment is based on the number of money laundering-related reports in the SMR sample and IR review, and feedback from partner agencies. The data-matching exercise also indicates the subsector is exposed to individuals charged with money laundering-related offences, as well as members of serious and organised crime groups. See page 34 for an overview of findings from the data-matching exercise.

Money laundering was identified in 27 per cent of the SMR sample and 59 per cent of the IR review.¹⁵ Common themes from these reports include:

- use of transaction accounts, including personal and business accounts
- layering through both domestic and international funds transfers to accounts held with multiple ADIs
- unexplained wealth, where the source of funds could not be determined but was inconsistent with the customer's profile
- large or unusual transactions inconsistent with a customer's profile
- multiple transactions when one transaction would suffice
- face-to-face cash deposits and withdrawals combined with other money laundering indicators
- structured cash deposits
- rapid or complex movement of funds through multiple accounts.

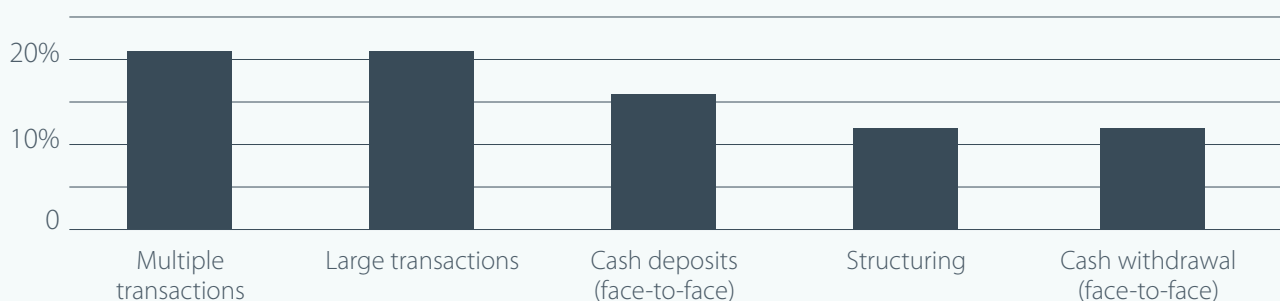
Individuals were observed in most reports in the SMR sample (92 per cent), followed by companies (15 per cent). In approximately eight per cent of reports, both an individual and company were observed. In these instances, suspected layering between personal and business accounts was common.

Customers often combined two or more money laundering methods in an effort to avoid reporting obligations and evade detection. For example, money mules often structured cash deposits, followed by rapid or complex movement of funds. Customers also used products and services across multiple ADIs to further obscure the money trail and integrate illicit funds. This can make it harder to detect unusual or suspicious financial activity because reporting entities do not have visibility of a customer's transactions at other banks.

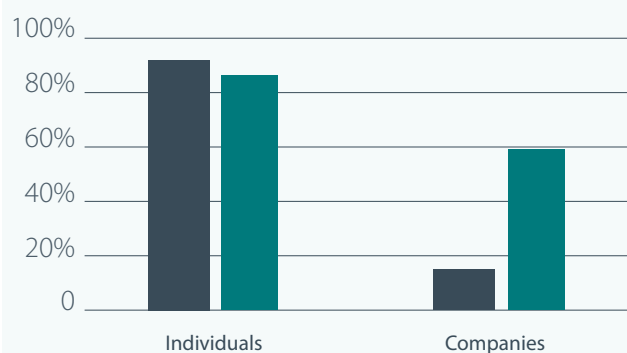
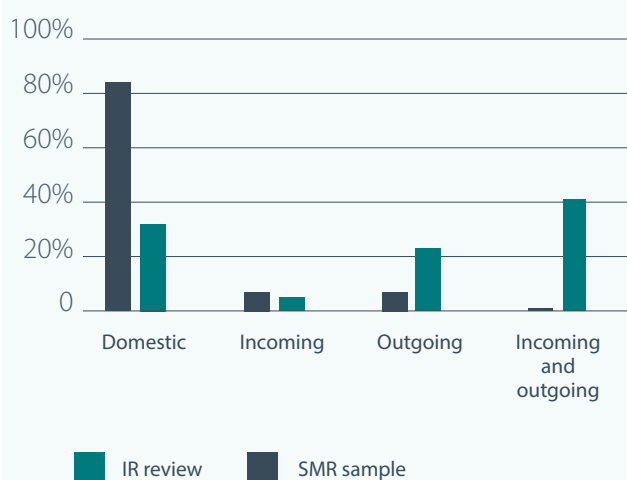
MONEY LAUNDERING BY TRANSNATIONAL, SERIOUS AND ORGANISED CRIME GROUPS

Transnational, serious and organised crime groups use a variety of products and services offered by the subsector to launder illicit funds. Investigations have identified members of these groups, including complicit money mules, making significant cash and cheque deposits and large domestic electronic funds transfers into personal and business accounts. These funds are then layered through domestic and international funds transfers to accounts held at other financial institutions. In some cases involving outgoing international funds transfers, the funds are 'returned' to separate domestic accounts.

¹⁵ In the SMR sample, a report was labelled as 'money laundering' when AUSTRAC analysts deemed the nature or extent of suspicious indicators suggested money laundering was likely. Such indicators can include unexplained wealth, an attempt to obscure the source of funds or purpose of transaction, where the source of funds was possibly linked to proceeds of crime, or when money laundering methodologies were identified (e.g. cuckoo smurfing or rapid movement of funds).

ML-RELATED SMRs: METHODS

i To protect itself from criminal exploitation, the subsector should remain vigilant against emerging money laundering methodologies and closely monitor transactional activity for indicators of any stage of the money laundering cycle.

ML-RELATED REPORTS: CUSTOMER TYPES**ML-RELATED REPORTS: DIRECTION OF FUNDS**

TERRORISM FINANCING

AUSTRAC assesses the nature and extent of the terrorism financing threats facing other domestic banks as **medium**.

This assessment is based on the number of terrorism financing-related SMRs submitted by other domestic banks, findings from the IR review and feedback from partner agencies. The data-matching exercise also indicates other domestic banks are exposed to some suspected terrorist actors.¹⁶

This assessment is lower than determined in previous AUSTRAC assessments and reflects shifting terrorism financing behaviour involving the banking sector. While historically Australia's domestic banks have been used to store and send funds in support of terror organisations and foreign terrorist fighters, the current terrorism financing threat environment in Australia is dominated by self-funded activity, or attempted attacks that require little to no funding.

AUSTRALIA'S TERRORISM FINANCING ENVIRONMENT

Since the territorial collapse of Islamic State of Iraq and the Levant's caliphate in Syria and Iraq, there has been a sharp decline in the number of foreign terrorist fighters departing Australia. However, the security environment continues to evolve and the COVID-19 pandemic, while inhibiting some aspects of the terrorism threat through the restricted cross-border movement of people, has also presented a platform for recruitment and the promotion of extremist narratives online. Amid this evolving environment, supporters and sympathisers in Australia are likely to continue to send funds internationally in support of terrorist activity.

The primary threat to Australia stems from religiously motivated violent extremism in the form of lone actors or small groups, although ideologically motivated violent extremism poses an increasing threat. These actors and groups primarily conduct small-scale, low-cost terrorist attacks using weapons that are inexpensive and easy to acquire, and tactics that do not require specialist skills. The national terrorism threat level at the time of publication is assessed by the National Threat Assessment Centre as **probable**.

It is unlikely significant amounts of terrorist-related funds are flowing into, through or returning to Australia from offshore. Financial outflows may increase if returned foreign fighters begin sending funds to regional countries or radicalise vulnerable members of the community. Restrictions on cross-border movements imposed in response to the COVID-19 pandemic will also limit the ability for foreign fighters to return to Australia. These restrictions are also likely to affect the ability for cash to be moved into or out of Australia for terrorism financing purposes.

¹⁶ These entities were identified by data-matching partner agency criminal lists against AUSTRAC reports. AUSTRAC assesses that other domestic banks do not knowingly provide products or services to known or suspected terrorist actors. See page 34 for a detailed overview of higher-risk customer data-matching results.

Across AUSTRAC's entire reporting population, other domestic banks submitted six per cent of all terrorism financing-related SMRs, and were observed in 14 per cent of terrorism financing-related intelligence reports analysed for this assessment.

Common themes include:

- trigger-based reporting after negative media coverage or a law enforcement request regarding a customer. This does not indicate the account was used for terrorism financing, however it does highlight the exposure of other domestic banks to terrorist actors
- generally unsophisticated and unvaried use of terrorism-financing methodologies
- use of a transaction account to store and rapidly move funds
- little effort to obscure the source or destination of funds
- extremely low-value transactions.

The data-matching exercise identified a moderate number of people charged with a Commonwealth terror offence between 2014 and 2018 transacting with the subsector. Although these individuals were not always customers of other domestic banks, their appearance in reports from the subsector exposes it to a medium risk of terrorism financing. For an overview of known or suspected terrorists that are customers of the subsector see page 34.

i The risk of customers supporting or funding offshore terrorism is reduced given the subsector has limited ability to conduct international funds transfers. Nonetheless, other domestic banks should remain vigilant to current and emerging terrorism financing threats and methodologies. Reporting entities are encouraged to subscribe to [ASIO Outreach](#), which provides security advice to Australian businesses.

IDENTIFYING TERRORISM FINANCING

Terrorism financing can be difficult to identify. It can be difficult to link the source of funds and transactional activity in Australia to the end use, and terrorist activities often require little to no funding. Detection is further complicated given terrorism financing funds are often acquired through legitimate means such as wages, government benefits, loans, family support and business earnings.

In some instances, funds are acquired through fraudulent means such as loan fraud, credit card fraud and fundraising under the guise of charitable giving. Fundraising activities through non-profit organisations and online campaigns can occur. Refer to [AUSTRAC's ML/TF risk assessment of non-profit organisations](#) for more detail.

Common indicators of terrorism financing include:

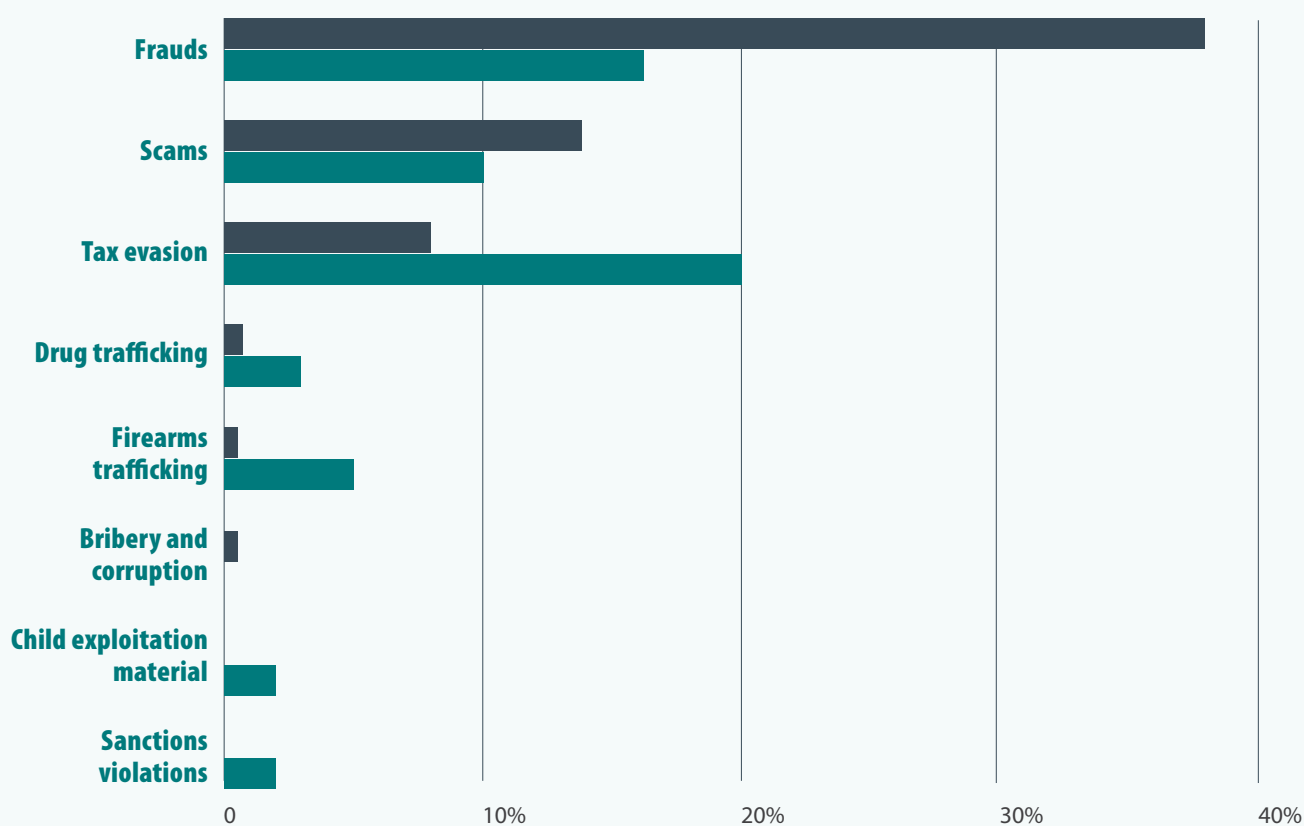
- a customer conducting international funds transfers to multiple beneficiaries located in the same jurisdiction that is deemed higher risk for terrorism financing
- unusual or unusually large cash withdrawals after a financial institution refused to conduct an international transfer to a jurisdiction deemed higher risk for terrorism financing
- open source reporting that any parties to the transaction have links to known terrorist entities or activities.

PREDICATE OFFENCES

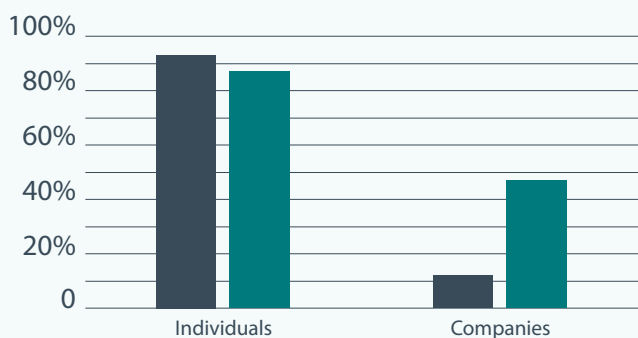
AUSTRAC assesses the nature and extent of threat posed by predicate offending involving other domestic banks as **high**.

This assessment is based on consultations with partner agencies, and findings from the SMR sample and IR review.

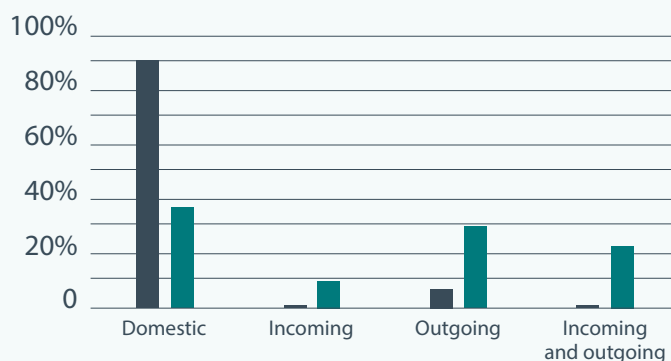
Key predicate offences include frauds, scams, tax evasion and drug trafficking. To a lesser extent, the subsector is also exposed to high-impact offences such as child exploitation, bribery and corruption, sanctions violations and trafficking in illicit goods.



PREDICATE REPORTS: CUSTOMER TYPES



PREDICATE REPORTS: DIRECTION OF FUNDS



■ SMR sample ■ IR review

IDENTIFYING PREDICATE OFFENCES – A CHALLENGE FOR REPORTING ENTITIES

Reporting entities may not be able to identify specific criminal activity, even when funds are suspected to be the proceeds of crime. It can be difficult to determine the predicate offence in the absence of law enforcement intelligence or media reporting. This challenge is amplified where the predicate offence has no nexus to the reporting entity. For example, drug trafficking is very difficult for a reporting entity to identify because it occurs outside of the banking system altogether, unlike frauds, which often involve a bank product or leave a transactional trail. This lack of visibility helps explain discrepancies in reporting volumes of predicate offences between the SMR sample and the IR review.

i SMRs that do not identify a predicate offence can still contain important pieces of intelligence that form part of a bigger picture of offending. Reporting entities should remain vigilant of key criminal market trends in Australia and report any suspicions of related financial transactions to AUSTRAC in a detailed SMR. Guidance on submitting SMRs can be found on [AUSTRAC's website](#).

KEY PREDICATE OFFENCES

FRAUDS

Frauds was the most common predicate offence observed in the SMR sample (38 per cent) and IR review (17 per cent). While most cases were relatively simple in nature, a small number were more sophisticated and had potentially significant consequences. Identity fraud and loan application fraud were most commonly observed. The type of suspected fraud was sometimes difficult for the reporting entity to determine, as evidenced by the portion of SMRs labelled as 'other fraud'.¹⁷ These reports were often submitted where the reporting entity had been notified by another financial institution that their customer was the recipient of fraudulent funds and no further details were given.

Other domestic banks are particularly exposed to identity crime through their online product delivery arrangements. See page 51 for further discussion of these vulnerabilities.

Common themes of identity fraud-related SMRs include:

- a cyber-enabled element – transaction accounts, credit cards and personal loans were applied for online in most instances
- the use of personal details (such as mobile numbers, email addresses or IP addresses) that were associated with previous instances of fraud or seemingly unrelated accounts
- the use of a false address linked to a vacant property
- the use of email domains with fewer security features.

Loan application fraud was often committed using fraudulent identity documents. This type of fraud shared the above indicators, as well as forged or altered payslips that inflated or staged an individual's income.

¹⁷ An SMR was assessed as 'other fraud' or 'other scam' if no information was available to determine the nature of the predicate fraud or scam offence, or the methodology employed to conduct the offence.

SOPHISTICATED IDENTITY FRAUD SCHEME

A financial adviser fraudulently opened more than 30 accounts at one other domestic bank without authorisation from his clients. The fraudulent accounts all shared at least one identical piece of contact information.

Once established, the adviser transferred more than \$4 million of suspected criminal proceeds through the accounts. It is believed the accounts were established for the sole purpose of laundering criminal proceeds.

Common themes observed in romance scam-related reports include:


- outgoing international funds transfers, with the most common destinations being the United States of America (USA), South Africa and Nigeria
- customers denying or ignoring advice from reporting entities that they were being targeted
- in some instances, customers withdrew cash or transferred funds to an external account after the reporting entity declined to process the international funds transfer request.

SCAMS

Scams were observed in 14 per cent of the SMR sample and 10 per cent of the IR review. While many scam typologies were reported, the most common were remote access and romance scams.

Common themes observed in remote access scam-related reports include:

- exploitation of transaction accounts, including mule accounts
- a phone or cyber-enabled element
- rapid domestic electronic transfer following receipt of funds
- some cash withdrawals following receipt of funds.

 AUSTRAC acknowledges that fraud and scam threats are continually evolving. Other domestic banks should remain vigilant to specific fraud and scam methods relevant to their operations and customers, and AUSTRAC encourages the subsector to:

- promote customer education and awareness
- continue strengthening fraud mitigation systems and controls
- report suspected fraud and scam-related activity in SMRs.

PROTECTING VULNERABLE AUSTRALIANS THROUGH FINTEL ALLIANCE

In early 2019, AUSTRAC's public-private partnership Fintel Alliance, established a scams working group to share information on emerging and complex scams to disrupt this crime. Through the working group, Fintel Alliance banking partners worked closely with the New South Wales Police Force to investigate a criminal syndicate targeting vulnerable Australians.

Through financial analysis, Fintel Alliance members identified a variety of methods the syndicate used to gain access to the financial accounts of vulnerable Australians, with the most common scam involving the syndicate 'cold calling' victims and asserting to be technicians employed by the National Broadband Network. The syndicate gained access to victims' bank accounts and then transferred funds out of these accounts.

Following investigation, the head of the syndicate was arrested and charged with dealing with the proceeds of crime. The court found the syndicate head guilty and sentenced them to an 18-month community service order and 150 hours community service. The collaborative effort of Fintel Alliance partners helped to identify, target and dismantle the syndicate, protecting vulnerable members of the Australian community.

TAX EVASION

Tax evasion was observed in eight per cent of the SMR sample and 20 per cent of the IR review. The most common threats include links to the shadow economy, including personal income tax evasion and offshore tax evasion. The extent of suspected personal income tax evasion detected in the SMR sample and IR review was largely comparable with suspected corporate tax evasion. However, the average SMR value in instances of corporate tax evasion was nearly double that of personal income tax evasion. Therefore the associated harm of corporate tax evasion through the subsector is likely higher.

Common themes observed in suspected personal income tax evasion reports include:

- cash transactions, particularly structured in-branch deposits and withdrawals
- transactions inconsistent with a customer's profile
- use of personal transaction accounts or trust accounts
- the use of agent banking arrangements to deposit cash – particularly non-ADI agents
- transactions to or from foreign jurisdictions – particularly known secrecy jurisdictions and global financial hubs. The most common jurisdictions observed in the SMR sample were China, Guernsey, Seychelles, the United Arab Emirates and the United Kingdom (UK).

Methodologies observed in suspected corporate tax evasion reports were varied and largely dependent on the type and sophistication of the beneficial customer. Less sophisticated methods involved large and frequent cash deposits, or customers using their personal bank accounts for business purposes. More complex methods included:

- the creation and exploitation of complex company structures or companies located in known secrecy jurisdictions to obscure beneficial ownership
- transactions to or from foreign jurisdictions – particularly known secrecy jurisdictions and global financial hubs. The most common jurisdictions observed in the SMR sample were the UK, USA, Singapore, China, Guernsey and Jersey.

OTHER HIGH-IMPACT PREDICATE OFFENCES

AUSTRAC assesses the subsector is likely exposed to some criminal proceeds generated from high-impact predicate offences such as drug trafficking, child exploitation, bribery and corruption, sanctions violations and trafficking in illicit goods. This assessment is based on the subsector's large customer base and exposure to serious and organised crime groups that are involved in some of these activities.

i High-impact predicate offences can carry significant levels of associated harm. Reporting entities should remain vigilant to potential exposure to illicit funds flows linked to these activities. This is particularly true for reporting entities that facilitate international transactions or have exposure to foreign-based customers given many of these offences have an offshore link.

Financial intelligence provided by reporting entities enables AUSTRAC and its partner agencies to investigate these offences and mitigate any potential harm.

DRUG TRAFFICKING

Suspected drug use or trafficking was observed in less than one per cent of the SMR sample and three per cent of the IR review. Despite this, AUSTRAC assesses other domestic banks are likely exposed to a moderate amount of criminal proceeds generated by drug trafficking activities. Australians pay some of the highest prices in the world for illicit drugs, making Australia an attractive market for traffickers. The ACIC estimates Australians spent more than \$11 billion on illicit drugs in 2018-19.¹⁸

AUSTRAC assesses that some of these funds will enter the subsector at either placement, layering or integration given the size of the customer base. This finding is supported by partner agency intelligence, which suggests money laundering organisations and drug trafficking organisations exploit other domestic banks to launder drug proceeds.

The data-matching exercise identified approximately \$15 million in transactions through other domestic banks linked to members of serious and organised crime groups, many of which are involved in drug trafficking. While this figure almost certainly includes legitimate transactions, it is likely an under-representation of the actual extent to which known and suspected criminals transact with the subsector. This is because the data-matching exercise only included a sample of known or suspected criminals and reflects transactions that were subject to an SMR, TTR or IFTI submitted by other domestic banks. It does not reflect instances of these entities conducting a range of other banking transactions that could be exploited for criminal purposes (e.g. domestic transfers or purchase of assets).

AUSTRAC acknowledges it is very difficult for reporting entities to distinguish transactions linked to drug proceeds from other money laundering activities in the absence of law enforcement information. This almost certainly accounts for the low number of SMRs submitted by other domestic banks with a direct link to drug activity. SMRs that had a direct link to drug activity were almost always based on low-level suspicious behaviour (e.g. references to drugs in transaction descriptions), or were triggered by law enforcement enquiries or adverse media reporting.

Given the difficulty of identifying drug-related transactions, the low numbers of SMRs and the amount of money spent on illicit drugs by Australians, AUSTRAC assesses it is highly likely some of the 29 per cent of SMRs that identified money laundering as the only threat are linked to drug proceeds.

¹⁸ ACIC, *National Wastewater Drug Monitoring Program Report 09, 2020*, page 15, [acic.gov.au/publications/national-wastewater-drug-monitoring-program-reports/national-wastewater-drug-monitoring-program-report-09-2020](https://www.acic.gov.au/publications/national-wastewater-drug-monitoring-program-reports/national-wastewater-drug-monitoring-program-report-09-2020).

FIREARMS TRAFFICKING

Firearms trafficking was observed in an extremely small number of reports in the SMR sample and five per cent of the IR review. A key theme observed in the IR review was a sudden change in customer activity, such as payment for a firearms licence followed by a significant amount of incoming domestic transfers from multiple first-time payers. All SMRs were submitted in response to media reporting about a customer.

While the exact value of the illicit firearms market cannot be determined, the ACIC estimates there are approximately 260,000 illicit firearms in Australia.¹⁹ This market is composed of firearms, firearm parts and accessories acquired in a variety of ways, including theft from licensed entities, the grey market, or illegal importation.²⁰ Firearms are an enabler of serious and organised crime groups. Even a small number of illegal firearm transactions can result in significant harm to the Australian community, including serious injury and death.

BRIBERY AND CORRUPTION

Bribery and corruption were observed in less than one per cent of the SMR sample and were not observed in the IR review. Common themes observed in SMRs include:

- links to foreign jurisdictions, particularly higher-risk jurisdictions in the Asia-Pacific region
- the presence of companies and other legal structures with unclear beneficial ownership arrangements.

Australia's stable political system, independent judiciary, and well-developed financial services sector make it an attractive destination or transit point for funds derived from foreign bribery and corruption. This is heightened by Australia's proximity to countries in the Asia-Pacific region that have been rated on the lower end of Transparency International's Corruption Perception Index, or whose AML/CTF regimes have been assessed as being of low or moderate effectiveness in recent mutual evaluation reports.^{21, 22} These factors mean that other domestic banks exposed to foreign jurisdictions – particularly to higher-risk jurisdictions – face significant bribery and corruption threats.

19 ACIC, *Illicit firearms in Australia*, 2018, page 7, [acic.gov.au/publications/unclassified-intelligence-reports/illicit-firearms-australia-report](https://www.acic.gov.au/publications/unclassified-intelligence-reports/illicit-firearms-australia-report).

20 The grey market consists of all long-arms that were not registered or surrendered as required during gun buybacks following the National Firearms Agreement in 1996, [acic.gov.au/about/priority-crime-themes/illicit-firearms](https://www.acic.gov.au/about/priority-crime-themes/illicit-firearms).

21 Transparency International, *Corruption Perception Index 2019: Asia Pacific*, January 23, 2020. Viewed: 9 November 2020, [transparency.org/en/news/cpi-2019-asia-pacific](https://www.transparency.org/en/news/cpi-2019-asia-pacific).

22 FATF, *Consolidated assessment ratings*, 2020, [fatf-gafi.org/media/fatf/documents/4th-Round-Ratings.pdf](https://www.fatf-gafi.org/media/fatf/documents/4th-Round-Ratings.pdf).

CHILD EXPLOITATION

Misuse of other domestic banks to fund child exploitation activities was observed in an extremely small number of reports in the SMR sample and two per cent of the IR review. While not specific to the subsector, banks are used to facilitate payments for access to child exploitation material, as well as to facilitate 'grooming' and child sex tourism. Offenders often use various reporting entities across the banking and remittance sectors to make offshore payments to try and avoid being detected. Other domestic banks that do not facilitate international funds transfers have a much lower exposure to child exploitation because transfers to higher-risk jurisdictions are often associated with child exploitation activity.


Identifying child exploitation activity

Identifying transactions linked to child exploitation can be challenging. Transaction values often appear to be legitimate or can be confused with potential fraud activity. The following indicators are drawn from the 2019 Fintel Alliance financial indicators report *Combating the sexual exploitation of children for financial gain*:

- low value transactions between \$15 and \$500
- transfers to a recognised higher-risk jurisdiction for child exploitation, particularly the Philippines, Thailand or Mexico
- no work or family links between the sender and the destination country
- use of credit cards or ATMs in higher-risk jurisdictions
- attempts to obfuscate the sender's identity, such as name variations
- attempting to disguise activity by describing payments as 'accommodation', 'education', 'school', 'uniform', or 'medical bills'
- payments for use of virtual private network (VPN) software, screen capture and live-streaming programs, and metadata stripping and anonymising software.

SANCTIONS VIOLATIONS

Sanctions violations were not observed in the SMR sample, but were identified in two per cent of the IR review. Sanctions violations have the potential for significant consequences to national and international security. These violations generally involve higher-risk jurisdictions and the presence of companies or other legal structures.

 The business unit responsible for onboarding customers is the first line of defence in embedding a strong risk and control environment into the daily business as usual activities. In relation to sanctions controls, it is the reporting entity's responsibility to understand the customer's source of funds and wealth, expected account activity, ownership structure, as well as the associated and controlling parties. Customer screening against sanctions lists may be ineffective if sufficient information is not obtained at the time the account is opened.

MODERN SLAVERY AND ENVIRONMENTAL CRIMES

Instances of suspected modern slavery and environmental crimes were not identified in the SMR sample or IR review. However, the subsector may be exposed given the size of the customer base and retail banking products that are vulnerable to criminal misuse.

Modern slavery


The *Modern Slavery Act 2018* defines modern slavery as practices that include human trafficking, slavery, servitude, forced labour, debt bondage, forced marriage, and the worst forms of child labour.²³ The Australian Institute of Criminology estimates there were between 1,300 and 1,900 victims of human trafficking and modern slavery in Australia between 2016 and 2017.²⁴

In addition to the very high human cost of these offences, modern slavery generates significant criminal proceeds. The International Labour Organisation estimates that forced labour alone creates more than US\$150 billion in illegal profit globally per year.²⁵ The extent of these financial flows with a link to Australia is unknown. However, Australia is primarily a destination country for the victims of human trafficking and slavery, and associated criminal proceeds may flow offshore or circulate domestically.²⁶

Environmental crimes

Environmental crimes incorporate an array of offences, including wildlife trafficking, logging and the dumping of illegal waste, among others. These offences can generate significant illicit profits and attract lower criminal penalties than other crimes, making them lucrative for criminals. The value of proceeds generated from environmental crimes in Australia is unknown. The United Nations Environment Programme and INTERPOL estimate the global market is worth in excess of US\$91 billion, making it the fourth most profitable crime type in the world.²⁷

Wildlife trafficking is of particular concern in Australia. Traffickers often sell native wildlife to overseas buyers, where they can receive significant mark-ups. Animals can be sold to breeding facilities in foreign jurisdictions, where they are 'laundered' and then on-sold.

 Reporting entities are encouraged to consider Fintel Alliance's [Illegal Wildlife Trafficking Financial Crime Guide to identify suspicious activity and report it to AUSTRAC](#).

23 For more see: homeaffairs.gov.au/criminal-justice/Pages/modern-slavery.aspx.

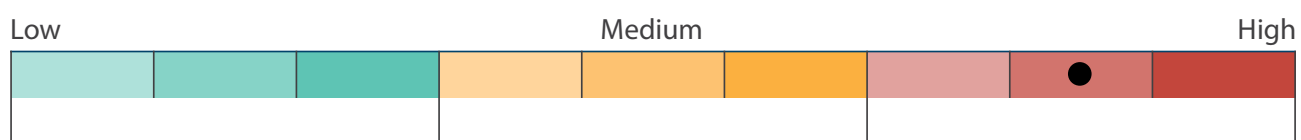
24 Lyneham S, Dowling C & Bricknell S, *Estimating the dark figure of human trafficking and slavery victimisation in Australia*, Australian Institute of Criminology (AIC), 2019, page 6, aic.gov.au/publications/sb/sb16.

25 International Labour Organization, *Profits and poverty: The economics of forced labour*, 2014, page 13, ilo.org/global/publications/ilo-bookstore/order-online/books/WCMS_243391/lang-en/index.htm.

26 Joint Standing Committee on Foreign Affairs, Defence and Trade, *Hidden in plain sight: An inquiry into establishing a Modern Slavery Act in Australia 2017*, page 56, aph.gov.au/Parliamentary_Business/Committees/Joint/Foreign_Affairs_Defence_and_Trade/ModernSlavery/Final_report.

27 INTERPOL, *UNEP-INTERPOL report: value of environmental crime up 26%*, 4 June 2016. Viewed: 9 November 2020, interpol.int/en/News-and-Events/News/2016/UNEP-INTERPOL-report-value-of-environmental-crime-up-26.

VULNERABILITIES



CRIMINAL VULNERABILITY FACTOR	RATING
Customers	●
Products and services	●
Delivery channels	●
Foreign jurisdictions	●

Vulnerability refers to the characteristics of a subsector that make it susceptible to criminal exploitation.

AUSTRAC assesses that other domestic banks are subject to a **high** level of inherent vulnerability related to ML/TF and other predicate offences. AUSTRAC's assessment of vulnerabilities falls into four broad categories:

- customers
- products and services
- delivery channels
- exposure to foreign jurisdictions.

CUSTOMERS

AUSTRAC assesses the subsector's customer base presents a **high** level of inherent ML/TF vulnerability.

The key vulnerability posed by the subsector's customer base is its size and diversity. Other domestic banks are also exposed to a high number of higher-risk customers.

SIZE OF THE CUSTOMER BASE

Other domestic banks have a large customer base. Combined, they service at least five million customers and hold approximately \$243 billion in deposits and \$435 billion in assets.²⁸ The size of the customer base increases the subsector's exposure to criminal entities and ML/TF exploitation. It also creates challenges in proactively detecting criminal misuse.

Customer profiles vary widely across the subsector. Some reporting entities are regional in focus and serve tens of thousands of customers while others are national in scope with well over one million customers. While the customer base is dominated by individuals, the subsector also services non-individual customers including companies, trusts and other legal entities (including some reporting entities that only service non-individual customers).

Non-individual customers pose a higher inherent ML/TF vulnerability because of the increased ability to obscure beneficial ownership, the source of funds or the purpose of transactions.

AUSTRAC expects the size of the subsector's customer base to continue to grow gradually over the coming years. An increasing number of challenger and neo-banks is likely to draw customers away from traditional financial institutions to other banking subsectors. Additionally, the introduction of Open Banking to the Australian market will make it easier for customers to transfer their information to new entities.

HIGHER-RISK CUSTOMERS

Other domestic banks have a high exposure to higher-risk customers. This assessment is based on industry customer risk ratings, SMRs, results from the data-matching exercise and qualitative insights from industry and partner agencies.

Higher-risk customers can present across a range of categories including:

- known or suspected criminals
- PEPs
- companies, trusts and other legal entities
- DNFBPs
- financial institutions
- temporary visa holders.

28 APRA, *Monthly authorised deposit-taking institution statistics backseries: July 2020*, apra.gov.au/monthly-authorised-deposit-taking-institution-statistics.

KNOWN OR SUSPECTED CRIMINALS




AUSTRAC assesses a small number of known and suspected criminals present a high inherent ML/TF vulnerability to the subsector. This assessment is based on the results of the data-matching exercise that identified the proportion of customers who were:²⁹

- recorded as a member of a significant national or transnational criminal group as at May 2020
- charged with a money laundering or proceeds of crime-related offence between 1 January 2017 and 31 December 2018³⁰
- charged with a terrorism-related offence between 1 January 2014 and 31 December 2018.³¹

Data-matching indicated that a moderate proportion of individuals charged with terrorism-related offences were identified as customers of the subsector. Transactions involving these individuals were generally low value.

A low proportion of individuals charged with money laundering or proceeds of crime-related activities were identified as customers of other domestic banks. Likewise, there was a low proportion of significant national or transnational criminal group members that were identified as customers of the subsector. The most common transactions linked to these individuals were IFTIs to New Zealand, UK, China, USA and Hong Kong Special Administrative Region of the People's Republic of China (Hong Kong SAR).

TRANSACTIONS LINKED TO KNOWN AND SUSPECTED CRIMINALS

MEMBERS OF SERIOUS ORGANISED CRIME GROUPS		ENTITIES CHARGED WITH ML OR PROCEEDS OF CRIME OFFENCE		ENTITIES CHARGED WITH TERRORISM-RELATED OFFENCE	
Proportion of POIs	Value of transactions	Proportion of POIs	Value of transactions	Proportion of POIs	Value of transactions
	\$\$		\$		\$
LEGEND		\$ = Low	\$\$ = Medium	\$\$\$ = High	

²⁹ This analysis was completed on IFTIs, TTRs and SMRs submitted by other domestic banks between 30 March 2018 and 1 April 2019. A high, medium, or low rating reflects the number of individuals identified as customers of the subsector taken as a proportion of the total number of individuals in each category (money laundering, serious and organised crime, and terrorism).

³⁰ Includes persons charged under Division 400 of the *Criminal Code* (Cth) and/or sections 81 and 82 of the *Proceeds of Crimes Act 2002* (Cth).

³¹ Includes persons charged with a 'Terrorism offence' in section three of the *Crimes Act 1914* (Cth) and/or offences contrary to the *Crimes (Foreign Incursion and Recruitment) Act 1978* (Cth).

DISPLACEMENT OF HIGHER-RISK CUSTOMERS TO OTHER DOMESTIC BANKS

AUSTRAC assesses that other domestic banks face ML/TF vulnerability due to displacement of some higher-risk customers from Australia's major banks, including members of serious and organised crime groups and individuals linked to terrorism. This displacement is likely driven by recent improvements in ML/TF risk mitigation strategies by major banks and generally occurs after:

- a major bank exits a customer after identifying adverse information or suspicious activity
- a major bank chooses not to onboard a customer after conducting rigorous customer due diligence (CDD) at onboarding.

These customers may then seek to be onboarded by other domestic banks, particularly if they perceive ML/TF risk mitigation strategies to be less mature or robust than the major banks'.

While a moderate number of PEPs are customers of the subsector, they rarely appeared in either the SMR sample or IR review. Overall, 16 reports in the SMR sample noted involvement of a PEP. Two-thirds of these related to domestic PEPs, which primarily involved suspected money laundering, bribery and corruption, and personal income tax evasion. Reports relating to foreign PEPs involved suspected bribery and corruption. Large transactions, multiple transactions, and face-to-face cash deposits were the most common transaction types linked to both domestic and foreign PEPs.

i Industry feedback indicates ECDD on PEP customers rarely returns adverse findings and very few are refused at onboarding, subject of an SMR or de-banked. AUSTRAC acknowledges the risk treatments applied, however assesses the overall number of PEP customers will continue to present a high ML/TF vulnerability.

POLITICALLY EXPOSED PERSONS

A PEP is an individual who holds a prominent public position or role in a government body or international organisation, either in Australia or overseas.³² They can be an attractive target for bribery and corruption given their capacity to influence government spending and budgets, procurement processes, development approvals and grants.

³² The AML/CTF Act defines three types of PEPs: domestic, foreign and international organisation PEPs. Immediate family members and/or close associates of these individuals are also considered PEPs. Refer to the AML/CTF Act for further details.

COMPANIES, TRUSTS AND OTHER LEGAL ENTITIES

Some companies, trusts and other legal entities can expose a reporting entity to higher ML/TF vulnerability. The extent of vulnerability depends on multiple factors including associated industries and business types, jurisdiction of head office and transparency of beneficial ownership.

Companies, trusts and other legal entities generally conduct larger and more frequent transactions. This can complicate detection of suspicious activity and obscure the source, destination and beneficial ownership of funds, particularly when combined with a complex structure of entities, intricate banking arrangements, or with an offshore nexus. Entities that operate in sectors deemed more vulnerable to ML/TF – such as gambling, natural resource extraction, remittance services and other DNFBP industries – also pose higher risks to reporting entities.³³

Other domestic banks service a large number of companies, trusts and other legal entities. These customers were identified in 15 per cent of the SMR sample and 47 per cent of the IR review. Common themes observed in these reports include:

- suspected involvement in a variety of offences including frauds, scams, tax evasion and money laundering
- the use of personal accounts in combination with business or trust accounts
- links to offshore personal or business accounts.


While not specific to the subsector, criminals actively exploit vulnerabilities associated with companies to launder illicit funds. For example:

- There are limitations in the identity verification process when registering a company in Australia. This can create opportunities for criminals to use stolen identities to establish a company that is subsequently used to launder criminal proceeds.
- Criminal entities often appoint a family member or 'cleanskin' associate as a director or shareholder to distance themselves from the purportedly legitimate entity.³⁴
- Australian companies can be registered by foreign nationals. Transnational, serious and organised crime groups exploit this vulnerability by compelling individuals on temporary visas to register companies that are subsequently used to place, layer and integrate illicit funds.
- Criminals may own or control multiple companies that are registered or operate in various jurisdictions. Banking arrangements linked to these companies are then used to facilitate global movement of funds and evasion of taxation obligations.

Company shareholders are also generally protected from being held criminally liable for the actions of a company, its employees or directors. This makes it harder for law enforcement authorities to restrain assets and proceeds derived from criminal activities.

33 The FATF recognises some correlation exists between the extraction of natural resources, high corruption risks and the incidence of grand corruption, particularly where significant revenues from extractive industries are combined with weak governance systems. FATF, Best Practices Paper, *The use of the FATF Recommendations to Combat Corruption*, 2013, fatf-gafi.org/media/fatf/documents/recommendations/BPP-Use-of-FATF-Recs-Corruption.pdf.

34 A 'cleanskin' is a person without a criminal history nor identifiable links to criminals who acts on behalf of a criminal entity in order to provide a veneer of legitimacy to such activities.

 AUSTRAC expects the subsector to continue strengthening systems and controls aimed at increasing transparency and oversight of beneficial ownership, and mitigating vulnerabilities relevant to company customers and other legal entities. When a suspicion is formed on obscure beneficial ownership or an unknown source of funds, AUSTRAC expects reporting entities to submit detailed SMRs.

DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

DNFBPs are recognised globally by the FATF and domestically by Australian law enforcement and financial regulators, as potentially attractive to misuse by serious and organised crime groups and other criminals. This is because of their:

- role as a gateway to the financial sector
- capacity to create corporate vehicles for layering and integrating purposes
- expert and specialist knowledge
- ability to lend legitimacy to complex transactions and activities
- ability to obfuscate illicit activity.

Lawyers and accountants have specialist knowledge and services that can be exploited by those seeking to conceal wealth or launder criminal proceeds. They can establish complex legal and banking structures, execute financial transactions, facilitate the purchase of high-value assets and act as trustees or directors of companies. They often have a strong understanding of the regulatory environment and their professional status can be used to provide a veneer of legitimacy to otherwise suspicious transactions. Lawyers and accountants can also accept large amounts of cash on behalf of criminals, which may be deposited into the firm's trust account and co-mingled with legitimate funds. There may also be a perception among criminals that funds held by their lawyer or accountant cannot be seized by law enforcement, and that transactions executed by these professionals cannot be subject to investigation.

Real estate agents are also exploited by criminals, particularly in the layering and integration phases of money laundering. Criminals might seek to purchase real estate with large amounts of cash, which may ultimately be deposited into an account held by a customer of the subsector. Criminals are also known to seek help from real estate agents to purchase real estate under market value with illicit funds and later sell the property at market value a number of years later.

AUSTRAC assesses some high-risk DNFBPs will present ongoing ML/TF risk to the subsector. This assessment is primarily based on partner agency information that indicates the subsector is being criminally exploited by these professionals. In the reporting period, several SMRs related to DNFBPs including real estate agents, high-value dealers (namely jewellery and gold dealers) and lawyers. These reports outlined suspected money laundering and tax evasion by these entities and included the following suspicious activities:

- incoming and outgoing domestic funds transfers to real estate companies and associated trust accounts
- under and non-reporting of taxation obligations
- requests by real estate agents to transact in cash.

PROFESSIONAL FACILITATORS AND TRUSTED INSIDERS – ENABLERS OF CRIME IN AUSTRALIA'S FINANCIAL SYSTEM

Professional facilitators are industry professionals and subject matter experts who provide their specialist skills and knowledge, either wittingly or unwittingly, for the benefit of clients seeking to disguise their criminal activity and the proceeds of crime. While thematically very similar, the trusted insider is an individual with legitimate or indirect access to privileged information, techniques, technology, assets or premises, whose access can facilitate harm. Both professional facilitators and trusted insiders can include individuals working in DNFBP industries.


Serious and organised crime groups will continually seek opportunities to exploit professional facilitators and trusted insiders across Australia's financial sectors. Criminals may specifically target other domestic banks to facilitate tax evasion and the movement of funds internationally. AUSTRAC expects other domestic banks to report any suspicions of professional facilitators or enabling parties to illicit activity, and encourages mature risk mitigation strategies for limiting insider threats.

FINANCIAL INSTITUTIONS

Financial institution customers may pose a higher ML/TF vulnerability because they have many hundreds or thousands of customers of their own (underlying customers). This means providing services to a single financial institution exposes other domestic banks to many underlying customers. Other domestic banks also have limited visibility of these underlying customers and their transactions, meaning banks partially rely on the quality of the financial institution's AML/CTF controls.

Financial institution customers are also more likely to conduct a large volume of transactions and some may conduct high-value transactions. In addition, some financial institution customers may expose other domestic banks to a high volume of cash transactions, particularly if they allow their underlying customers to make deposits into an account held at the other domestic bank.

Risks posed by a financial institution customer highly depend on factors such as the types of products or services it offers, the composition of its customer base and the jurisdictions it operates in.

 AUSTRAC encourages other domestic banks to remain aware of enduring ML/TF risks posed by DNFBPs and continue providing detailed SMRs when a suspicion is formed.

TEMPORARY VISA HOLDERS

Visitor visa holders

AUSTRAC assesses a small number of visitor visa holders who become customers of other domestic banks present a high ML/TF risk. While not isolated to the subsector, partner agencies report known and suspected instances of criminal exploitation by visitor visa holders. Common methodologies include members of transnational, serious and organised crime groups using fly-in fly-out visitors as money mules to establish bank accounts for money laundering. Once the accounts are opened, they are turned over to the controlling criminal entity and the money mule leaves Australia.

Indicators of suspicious activity by a visitor visa holder may include:


- establishing a banking profile shortly after arriving in Australia
- applying for products that do not match the profile of a tourist, such as business accounts
- large or frequent cash deposits, sometimes made anonymously or by third parties
- international transfers out of Australia, sometimes soon after deposits are made
- significant domestic transfers to unknown third parties
- transactional activity after an individual's visa has expired, especially if done in person (likely a visa over-stayer) or if it is known that the person has left Australia (likely an account being operated by a third party)
- use of a transient address, such as hotels or short-stay serviced apartments.

FLY-IN FLY-OUT MONEY MULES

Partner agency investigations identified an Australia-based criminal entity using fly-in fly-out money mules to establish transaction accounts at multiple major and other domestic banks. At all times, the accounts were under the control of the criminal entity.

Once the accounts were established, financial investigations identified over \$2 million dollars domestically transferred into the accounts believed to be the proceeds of scam activity.

After the money mules left Australia, the controlling criminal entity continued to transact on the accounts. This included multiple cash deposits and withdrawals, and multiple high-value transfers to remittance companies to send funds offshore.

 AUSTRAC encourages reporting entities to check an individual's visa status at onboarding if indicators suggest they are in Australia on a temporary basis. Knowledge of visa status can be used to determine a customer's expected transactional behaviour, as well as whether a transaction is suspicious or not. Transactions that may seem innocuous for a citizen or permanent resident could be deemed suspicious for someone on a temporary visa.

During consultation for this report, one reporting entity highlighted their company policy which requires staff to be satisfied that an individual has a significant connection to Australia prior to being onboarded. Subsequent CDD processes often involve seeking visa information from the individual if they provide foreign identification or contact details when applying for a banking product. The policy also mandates ECDD is conducted if it is discovered the individual holds a visa type they consider higher risk.

AUSTRAC acknowledges that some other domestic banks have a higher exposure to legitimate customers holding temporary visas. For example, reporting entities operating in regions with a high turnover of fly-in fly-out temporary workers.

Student visa holders

AUSTRAC assesses a small number of student visa holders who become customers of other domestic banks present a high ML/TF risk. While not isolated to the subsector, partner agencies report known and suspected instances of criminal exploitation by these individuals.

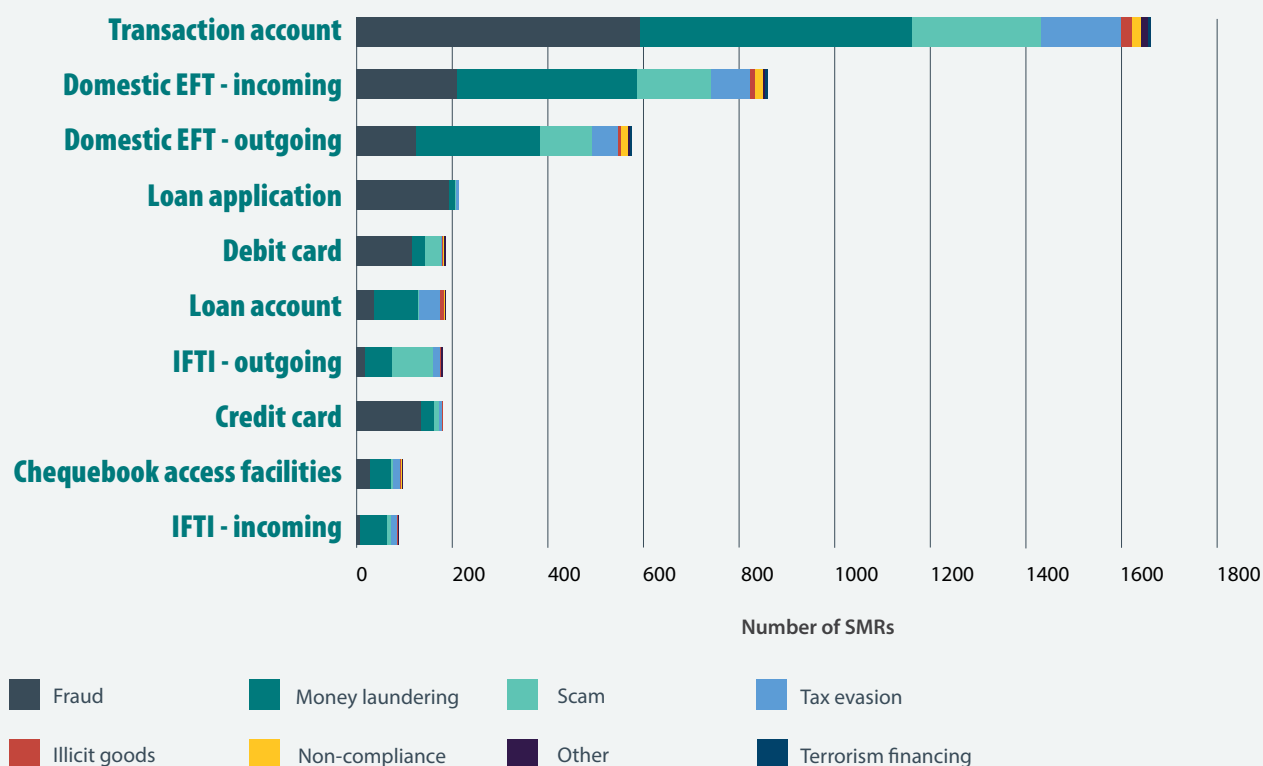
Common money laundering methodologies that have been linked to student visa holders include:

- excessive cash deposits into transaction accounts
- receiving large value transfers with no clear source or reason
- opening and operating multiple accounts at multiple institutions.

Student visa holders often receive funds into their account from overseas senders. This financial activity is not considered suspicious. However, multiple or large cash deposits made into these customers' accounts can be a red flag for illicit activity.

PRODUCTS AND SERVICES

MOST COMMON PRODUCTS OR SERVICES AND THREAT – SMR SAMPLE



AUSTRAC assesses the nature and extent of the products and services offered by other domestic banks pose a **high** inherent ML/TF vulnerability.

ML/TF vulnerability largely stems from the subsector's high exposure to cash and the large number of products and services offered that can be used to store and move illicit funds. Products most vulnerable to ML/TF include transaction accounts, trust accounts, loan products and credit cards.

There is wide variation in the number and type of products and services offered by individual reporting entities. These range from very small operations with specific product offerings to much larger operations that offer a broad range of products and services.

USE OF CASH

Although criminals are increasingly moving into the digital and cyber domains, cash-based money laundering remains a major threat in Australia. This is particularly evident in the placement stage because the proceeds of crime are often generated in cash and the layering stage because cash is very difficult to trace.

Other domestic banks have a high exposure to cash. While dealing with cash transactions is an inherent part of banking operations, it also increases the industry's exposure to the proceeds of crime. A reporting entity's exposure to money laundering placement risk also significantly increases when facilitating a large volume and high value of cash transactions. Because cash transactions provide anonymity they are also key to the shadow economy, and appear frequently in instances of personal tax evasion.

TTRs AND CASH-RELATED SMRs BETWEEN 1 APRIL 2018 AND 31 MARCH 2019

- Total number of TTRs submitted to AUSTRAC: **135,551**
- Total cash value of TTRs: **\$2.5 billion**
- Largest cash deposit: **\$1.2 million**
- Largest cash withdrawal: **\$1.15 million**
- Total number of cash-related SMRs: **4,009**
- Total value of cash-related SMRs: **\$219 million**
- **34%** of the SMR sample identified at least one suspicious cash transaction.
- **84%** of the IR review identified at least one suspicious cash transaction.

In the reporting period, other domestic banks submitted more than 135,000 TTRs for a total value of approximately \$2.5 billion. High exposure to cash transactions is partly due to the combination of large branch and ATM networks and the significant presence of agent banking relationships. Several reporting entities have also introduced the use of intelligent deposit machines (IDMs). As well as providing normal ATM functions, IDMs also accept cash deposits and credit a customer's account in real time, further increasing the convenience of transacting in cash. ML/TF vulnerabilities associated with IDMs are discussed in **Delivery channels** on page 50.

A number of reporting entities allow customers to directly deposit cash into multiple product types, including loan, credit card and trust accounts. Often, these funds can also be withdrawn as cash or quickly transferred and layered through various domestic and offshore accounts. This can significantly hamper efforts to quickly detect cash-based proceeds of crime or trace illicit funds.

Suspicious cash transactions were observed in approximately one-third of the SMR sample. Key themes observed include:

- cash deposits (50 per cent)
- cash withdrawals (50 per cent)
- structured transactions, either deposits or withdrawals (25 per cent)
- cash deposit followed by rapid movement of funds (15 per cent).

Partner agency investigations have also uncovered cash-based money laundering in the subsector, including exploitation by transnational, serious and organised crime groups and money mules (see discussion in **Criminal threat environment** on page 18).

PUSH AND PULL FACTORS ON CASH USE

As electronic payments become more popular, cash use is in steady decline in Australia.³⁵ The Reserve Bank of Australia calculates that cash payments as a share of consumer payments have more than halved between 2010 and 2019. The number of other domestic bank SMRs containing a suspicious cash transaction declined from 66 per cent in 2013-14, to 48 per cent in 2018-19.

The COVID-19 pandemic has had a significant impact on cash use. On the one hand, many Australian businesses encouraged customers to make cashless payments, accelerating the adoption of electronic payment methods for household transactions. On the other, the Reserve Bank of Australia notes that the amount of cash on issue grew strongly in 2020, reflecting demand to hold cash for "precautionary purposes and as a store of value".³⁶ Overall, the Reserve Bank noted a "substantial increase in high-value cash withdrawals at branches" in the first half of 2020.³⁷

A sustained climate of very low interest rates could see cash withdrawals increase among some customer cohorts, such as older Australians.

35 Reserve Bank of Australia, *Panic, Pandemic and Payment Preferences*, Reserve Bank of Australia, 2020. Viewed: 18 May 2021, [rba.gov.au/speeches/2020/sp-ag-2020-06-03.html](https://www.rba.gov.au/speeches/2020/sp-ag-2020-06-03.html).

36 T Richards, C Thompson and C Dark, *Retail central bank digital currency: Design considerations, rationales and implications*, Reserve Bank of Australia, 2020, page 31, [rba.gov.au/publications/bulletin/2020/sep/pdf/retail-central-bank-digital-currency-design-considerations-rationales-and-implications.pdf](https://www.rba.gov.au/publications/bulletin/2020/sep/pdf/retail-central-bank-digital-currency-design-considerations-rationales-and-implications.pdf).

37 L Delaney, N McClure and R Finlay, *Cash Use in Australia: Results from the 2019 Consumer Payments Survey*, Reserve Bank of Australia, 2020, page 50, [rba.gov.au/publications/bulletin/2020/sep/pdf/retail-central-bank-digital-currency-design-considerations-rationales-and-implications.pdf](https://www.rba.gov.au/publications/bulletin/2020/sep/pdf/retail-central-bank-digital-currency-design-considerations-rationales-and-implications.pdf).

ABILITY TO STORE AND MOVE FUNDS AND VALUE

By their nature, banking products and services are designed to store or move funds. Such activity makes banking products inherently vulnerable to ML/TF activity. The extent of this vulnerability depends on the specific features of a product and its exposure to customer, jurisdiction and delivery channel risk.


Combined, other domestic banks offer hundreds of products and services. The extent of product offerings is a vulnerability in itself. Criminals are known to probe the features of similar products to find gaps and inconsistencies to exploit for illicit purposes.

The products and services most vulnerable to ML/TF and criminal misuse include:

- transaction accounts
- trust accounts
- loan accounts
- credit card accounts.

EXAMINING VULNERABILITY OF PRODUCTS AND SERVICES: AUSTRAC'S PRODUCT RISK MATRIX

To better assess the inherent vulnerability of products and services offered by other domestic banks, AUSTRAC developed a product risk matrix (the matrix). The results and ratings from this exercise can be found in the table on page 46.

 Note that ratings contained in the matrix are used as an analytical technique for the purposes of this risk assessment only. Reporting entities must conduct their own product risk assessments, and should not rely on the matrix ratings to assess the ML/TF risks associated with individual products.

APPROACH






















Products and services were first grouped into broad categories (e.g. investment accounts and services). For each product category, four aspects were assessed:

1. The vulnerability perception rating is an average of other domestic banks' responses to the perceived inherent vulnerability of their products or services across four ML/TF risk factors:
 - the extent to which cash can be placed using the product or service
 - the extent to which funds or value can be stored using the product or service
 - the extent to which funds or value can be moved domestically using the product or service
 - the extent to which funds can be moved overseas using the product or service.
2. The detected exploitation rating assesses the known or suspected criminal misuse of a product or service category. This was determined by analysing information from the SMR sample, IR review and survey responses from partner agencies.
3. The value of median transaction indicates the median amount of funds flowing through a product or service and was determined by data provided by other domestic banks.
4. Transaction volume indicates how many transactions were conducted per product or service category over a 12-month period. This was determined using data provided by other domestic banks.

The overall rating combines these four aspects to determine a final score for each product or service category.

Discussion in this section focuses on the four product and service categories that had the highest overall rating.

PRODUCT AND SERVICE VULNERABILITY RATINGS

PRODUCT/ SERVICE	VULNERABILITY PERCEPTION RATING	DETECTED EXPLOITATION	VALUE OF MEDIAN TRANSACTION	TRANSACTION VOLUME	OVERALL RATING
Transaction accounts		High	\$	Very high	
Trust accounts		Medium	\$	Medium	
Credit cards		Medium	\$	Medium	
Home loans		Medium	\$	Medium	
Term deposits		Low	\$\$	Low	
Savings accounts		Negligible	\$	Medium	
Bank cheques		Low	\$	Low	
Personal loans		Medium	\$	Low	
Business loans		Medium	\$	Low	
Merchant services		Negligible	\$	High	
Foreign currency accounts		Negligible	\$\$	Low	
Trade finance		Negligible	\$\$	Low	
Pensions and annuities		Low	\$	Low	
Super and approved deposit funds		Low	\$	Low	
Asset financing		Negligible	\$	Low	

TRANSACTION ACCOUNTS

Transaction accounts are by far the most common and versatile products offered by other domestic banks. They are also the most commonly misused product. They were identified in two-thirds of the SMR sample and more than half of the IR review. Common themes observed in these reports include:

- placement of criminal proceeds, particularly cash
- layering of criminal proceeds between accounts held with the same reporting entity as well as other domestic ADIs
- opening of fraudulent accounts, usually to receive illicit funds that are almost immediately withdrawn or transferred.

Transaction accounts enable fast and effective storage and movement of funds domestically and internationally, exposing the product to foreign jurisdiction risk. Reporting entities often require a customer to hold a transaction account to access other banking products or services, such as bank cheques. These accounts are also used as transit points for cash deposits or withdrawals, which is a well established part of many ML/TF methodologies. Very high numbers of transactions are made using transaction accounts, which can make identifying criminal exploitation difficult.

Because transaction accounts are the most basic product offered by banks – and because their provision poses almost no financial risk to reporting entities – these accounts can be quickly and easily established, particularly online. This is exploited by criminals who use stolen identities or money mules to establish networks of accounts that they can use to place or layer criminal proceeds. Higher-risk international funds flows are further discussed in the **Foreign jurisdictions** section on page 54.

SMR SAMPLE: SUSPICIOUS FINANCIAL ACTIVITY INVOLVING A TRANSACTION ACCOUNT

TRANSACTION TYPE	% OF SMRs
Domestic electronic funds transfer into account	37
Domestic electronic funds transfer out of account	26
Cash withdrawal	24
Cash deposit	21
International funds transfer out of Australia	8
International funds transfer into Australia	5

TRUST ACCOUNTS

Reporting entities and partner agencies consider trust accounts to be highly vulnerable to ML/TF. Although they appeared relatively infrequently in the SMR sample (two per cent), the average amount of a trust account SMR was more than double the average SMR value.

Trust accounts are used by some DNFBPs such as lawyers, accountants and real estate agents, to hold client money on trust for a specific purpose. These professionals are generally higher-risk customers whose services are actively sought out, and misused, by criminals to place, layer and integrate criminal proceeds. Trust accounts also obscure beneficial ownership by co-mingling funds from multiple sources and separating the legal owner of the funds (the trustee) from the beneficiary of the funds (the beneficial owner). Trust accounts also allow cash deposits, including via IDM or third parties in some instances. This increases vulnerability to ML/TF exploitation.

CREDIT CARD ACCOUNTS

Seven per cent of the SMR sample involved the use of a credit card or related account. These reports were often submitted on suspicion of identity and loan application fraud. Common themes included:

- applying for a credit card with false identity documents or falsified supporting documents with the intention of immediately reaching the limit of the credit card (often through the purchase of high-value goods) and not repaying the debt
- paying for everyday expenses with credit cards, which are then paid off through structured cash deposits funded by criminal proceeds.

The characteristics of credit card accounts can make them vulnerable to exploitation for ML/TF. These products can often be applied for and approved with no face-to-face contact required, making them attractive to fraudsters. The ability to deposit cash directly into credit card accounts is a significant vulnerability that can allow criminals to place illicit funds into the financial system. Cash advances can also be used to withdraw cash from a credit card account (although advances incur significant costs and are less likely to be used).

Credit card accounts also allow individuals to access legitimate funds that can be paid off with criminal proceeds because they are a form of a loan account. This provides the criminal with a legitimate source for cash and high-value assets.

LOAN ACCOUNTS

Loan accounts and loan applications were identified in seven and eight per cent of the SMR sample respectively. Common themes in these reports include:

- applying for loans with falsified payslips or staged wages³⁸
- applying for loans with false identity documents and immediately withdrawing the funds in cash or transferring them to another financial institution
- paying off home and vehicle loans with structured cash payments to integrate illicit funds into the financial system.

Loan accounts are exploited to facilitate ML/TF and fraudulent activity in a number of ways. Partner agencies report them as particularly vulnerable to criminal misuse. For example:

- home and car loans provide criminals with an ostensibly legitimate source of funds to purchase high-value assets such as vehicles and property, which are then repaid using criminal proceeds. In this scenario, loan accounts that accept cash deposits are particularly vulnerable to misuse.
- personal loans can be fraudulently obtained and the funds quickly disbursed.

³⁸ Purposely depositing funds into a bank account in a fashion designed to imitate wage payments. Bank statements showing these payments are then used to prove income when applying for financial products.

DELIVERY CHANNELS

AUSTRAC assesses the delivery channels through which other domestic banks offer their products and services present a **high** inherent ML/TF vulnerability.

Across the subsector, face-to-face customer contact has declined over the past decade as business decisions and customer preferences shift to remote service delivery channels, particularly online banking. These channels give criminals anonymity, which can be exploited to perpetrate financial crimes, and make it harder to detect suspicious transactions. Other domestic banks are also exposed to a high level of inherent ML/TF vulnerability related to agent banking and other third-party product delivery arrangements.

LEVEL OF CUSTOMER CONTACT

Other domestic banks use a range of delivery channels to provide their products and services to customers. This includes in-branch, ATMs, phone, online and through third-party arrangements. While some reporting entities maintain national branch networks, most have limited branch networks or maintain an online presence only.

Other domestic banks report a decline in face-to-face transacting as customers continue to adopt more remote delivery channels. This shift has been facilitated by increasingly comprehensive and easy-to-use mobile apps, as well as the rollout of IDMs.

The trend towards more remote product delivery channels increases ML/TF vulnerability by making it easier to impersonate a customer for financial gain or to transact anonymously. These features are exploited by criminals to distance themselves from illicit activity.

IMPACT OF COVID-19 ON CUSTOMER CONTACT

While bank branches are exempt from mandated COVID-19 closures, some other domestic banks have implemented measures to reduce face-to-face contact with customers where possible. For example, banks have encouraged customers to use online banking and have directed relationship managers to interact with customers over the phone or via videoconferencing where possible.

It is likely these changes will accelerate the trend away from face-to-face product delivery and towards online banking.

BRANCHES

Combined, the subsector operates approximately 1,000 branches across Australia. In-branch transactions generally provide reporting entities with more opportunity to identify suspicious behaviour. Face-to-face deposits and withdrawals were identified in 16 per cent and 12 per cent of the SMR sample respectively. Common themes in these reports include:

- individuals depositing cash into multiple accounts during the same transaction. This can indicate cuckoo smurfing. Details provided in SMR submissions can assist AUSTRAC and partner agencies to identify links between otherwise unrelated accounts.
- individuals struggling to answer simple questions or providing inconsistent answers on factors like the source of funds or reason for the transaction.

ATMs

Combined, the subsector operates approximately 1,300 ATMs, including IDMs. ATMs are a key delivery channel exploited by criminals to launder the proceeds of crime across all three phases of the money laundering cycle. ATMs let customers withdraw cash, which can facilitate the layering and integration of funds. Some ATMs also accept cash deposits – a feature that can be used to place criminal proceeds into the financial system and is highly vulnerable to criminal misuse. IDMs are a type of ATM that accept cash deposits and have additional features (see below).

ATM use was observed in 15 per cent of the SMR sample. Nearly one-third of these reports involved a suspicious cash deposit, and transactions were often structured and subsequently layered through transfers to separate accounts.

Intelligent deposit machines

IDMs are a type of ATM that have additional features, such as reconciling cash deposits in real time, conducting cardless deposits, transferring money between accounts, and depositing cheques. The first IDMs were introduced to the Australian market in 2012, and some reporting entities now operate these machines. Use of IDMs across the subsector is expected to grow.

While IDMs provide convenience for both the bank and the customer, they also expose reporting entities to unique inherent ML/TF vulnerability compared to in-branch deposits and their use can make it harder to identify criminal proceeds. For example, IDMs allow cardless cash deposits to be made by third parties, sometimes anonymously. IDMs also reconcile deposits to accounts in real time without the need for human intervention and most can be accessed 24/7. When combined with the speed offered by the New Payments Platform (NPP), criminals can exploit IDMs to anonymously place criminal proceeds into a transaction account and move funds through multiple accounts held with different reporting entities in just one or two minutes.³⁹

Professional money laundering organisations and other criminal groups exploit the increased anonymity provided by cardless deposits to distance themselves from illicit funds.

VERIFYING THIRD-PARTY CASH DEPOSITORS

Third-party cash deposits are highly vulnerable to ML/TF activity, particularly when made through delivery channels that allow a high level of anonymity such as IDMs. These channels employ few, if any, authentication measures to identify depositors. Where identifying details such as mobile numbers are required, they are often not verified. This allows criminals to deposit funds into third-party accounts anonymously and obscure the source of funds. Third-party cash deposits using IDMs are usually reconciled in real time, increasing ML/TF vulnerability because criminals can then layer funds quickly through multiple accounts, sometimes held with multiple institutions.

Steps taken to verify a customer's identity at an ATM or IDM (e.g. through mobile authentication) would likely help to mitigate money laundering activity through these delivery channels and impact cuckoo smurfing operations. Using mobile authentication methods may allow law enforcement and intelligence agencies to identify otherwise unrelated transactions through matching mobile numbers or provide intelligence on previously unknown mobile numbers associated with criminals.

 Reporting entities are encouraged to consider Fintel Alliance's [Cuckoo Smurfing Financial Crime Guide](#) to detect suspicious activity and report it to AUSTRAC

³⁹ The NPP is discussed on page 53.

ONLINE BANKING

The vast majority of transactions facilitated by other domestic banks originate online – either through banking apps or through websites. A large and increasing number of products can also be applied for online. This has been driven by consumer demand for speed and convenience. One other domestic bank reports that nearly 50 per cent of at-call accounts for the 2019 financial year were established online.

While this trend is driven by consumer demand, the increasingly online nature of banking introduces inherent ML/TF vulnerabilities. The speed with which transactions can be executed using online banking is attractive for criminals trying to layer illicit funds. With one device, a money launderer can direct funds through multiple bank products with different financial institutions, masking the true source or destination of the funds. This effect is compounded by the introduction of the NPP, which allows transactions to happen in seconds.

With no face-to-face interaction or CCTV monitoring, online banking also introduces an additional element of anonymity that is attractive to criminals. For example, an individual applying for a bank account online may not be subject to visual identification. Cyber-enabled frauds were commonly identified in the SMR sample – in particular fraudulent loan applications and opening accounts using stolen identities, which are then used to place and layer illicit funds.

Mobile banking applications

Tech-savvy criminals reportedly probe products to identify vulnerabilities to exploit. This is particularly relevant to products delivered online, where 'probing' is done in relative anonymity. The increasing number of products that can be applied for and delivered online amplifies this vulnerability. While not specific to other domestic banks, partner agencies have identified criminals who spend hours testing new versions of mobile apps deployed by banks to discover and exploit features to perpetrate crimes faster and more anonymously.



Reporting entities should carefully consider the financial crime implications of introducing new features into banking apps – even minor updates can be exploited by criminals.

COMPLEXITY OF PRODUCT DELIVERY ARRANGEMENTS

Other domestic banks primarily use outsourcing arrangements to allow customers to make cash transactions in locations where they do not have a branch. This creates ML/TF vulnerability because outsourcing lengthens and complicates the product delivery chain, making it harder for a reporting entity to detect and act on suspicious activity. This vulnerability can be exacerbated by poor governance arrangements.

AGENT BANKING ARRANGEMENTS


Many other domestic banks have agent banking arrangements with other ADIs and non-ADI third parties. These can include enabling customers to conduct certain transactions through another ADI's branch network, a newsagent or post office.

An agent banking arrangement consists of:

- an account provider offering deposit accounts to customers (i.e. the other domestic bank)
- an agent bank accepting deposits, including cash deposits, on behalf of the account provider, but not maintaining the customer's accounts.

While these arrangements give customers greater access to their accounts, particularly in rural areas, they also introduce inherent ML/TF vulnerability into the product delivery chain, including:

- lengthening the product delivery chain to incorporate a third party between the customer and the reporting entity, which may make transaction monitoring difficult
- third-party ADIs do not have visibility or knowledge of customer transactional history and are therefore less likely to identify activity that is unusual or inconsistent with the customer's profile
- limiting the ability for the reporting entity to ask questions about large or suspicious transactions
- confusion around AUSTRAC reporting obligations, which can lead to missed reports or double reporting
- false positive hits on transaction monitoring systems – outsourced arrangements sometimes have deposit limits well under \$10,000, forcing customers to break deposits into multiple transactions, which can look like structuring
- missing signs of a suspicious transaction because the staff of non-ADI agents fulfil many different non-financial functions in their day-to-day work
- less timely detection of suspicious transactions because agent banks supply transactional details to reporting entities retrospectively.

 During consultations, some reporting entities were unsure who was responsible for reporting TTRs to AUSTRAC in agent bank arrangements. In these arrangements, the account provider is providing the designated service and is therefore required to submit a TTR if the designated service involves a threshold transaction. However, an account provider and agent bank can enter into a contractual arrangement permitting the agent bank to report TTRs on the account provider's behalf. Where such an arrangement is in place, AUSTRAC expects the account provider to ensure appropriate risk management processes are in place for agent bank monitoring and assurance.

Please refer to the [AUSTRAC website](#) for more details on reporting obligations in agent banking relationships.

THIRD-PARTY ELECTRONIC BILLERS

Third-party electronic billers help businesses collect payments and consumers pay their bills. Transactions facilitated by third-party billers are vulnerable to ML/TF because they mask the source of funds, meaning payer details are not visible to the reporting entity. Transaction descriptions are also not required, further limiting a reporting entity's ability to investigate the source of funds.

Many credit card and loan accounts offer the ability to repay loans using third-party billers. This means criminals could exploit the lack of visibility created by third-party billers to layer illicit funds.

i Customers who want to receive third-party biller payments must have an ABN or ACN. This means incoming payments into a transaction account should be indicative of business earnings. This may be a good starting point for commencing ECDD if the transaction account is held by an individual whose recorded occupation is not consistent with the payments.

NEW PAYMENTS PLATFORM

The NPP is open access infrastructure for fast payments in Australia. It enables simply-addressed payments, which are completed in near real time. The NPP exposes reporting entities to ML/TF vulnerability due to the speed of transactions which limits the opportunity to identify and freeze suspicious transactions, enabling criminals to layer funds between accounts quickly.

Third-party commercial payment services can also use the NPP infrastructure to provide 'overlay services'.⁴⁰ While there is only one overlay service operating currently, it is expected more will be launched in the near future. These could introduce unintended ML/TF vulnerability to payments and increase the complexity of product delivery arrangements.

i AUSTRAC recommends that other domestic banks complete a risk assessment to fully understand the implications of using overlay services and adjust systems and controls accordingly.

CONSUMER DATA RIGHT – OPEN BANKING

The Consumer Data Right is a framework designed to enhance a consumer's ability to access the data businesses hold about them and authorise this data to be shared with accredited third parties. The first sector to which the Consumer Data Right applies is the banking sector (also known as Open Banking). Open Banking is designed to encourage greater competition, efficiency and the creation of more tailored products and services. The regime is currently undergoing a phased rollout.

By design, Open Banking will empower customers to access and use their data to better meet their banking needs. While the ML/TF risks of Open Banking are yet to be fully understood, more complex financial services arrangements could result if a customer chooses to use an increased number of financial service providers where previously they only used another domestic bank. This disaggregation of transactions across multiple financial services providers reduces other domestic banks' visibility of funds flows, making it more difficult to monitor and identify suspicious or unusual activity – such as layering – and therefore disrupt money laundering activities.

⁴⁰ Overlay services include things such as value-added payment services or improved customer experiences, which can involve implementing new message flows or payment types between participants. Source: rba.gov.au/publications/bulletin/2018/sep/the-new-payments-platform-and-fast-settlement-service.html.

FOREIGN JURISDICTIONS

AUSTRAC assesses the other domestic bank subsector has a **high** inherent ML/TF vulnerability to foreign jurisdiction risk.

While not all reporting entities facilitate international funds transfers, those that do are generally highly exposed to foreign jurisdictions, including to higher-risk jurisdictions.⁴¹ Combined, the subsector submitted a high number and value of IFTIs to AUSTRAC in the reporting period.

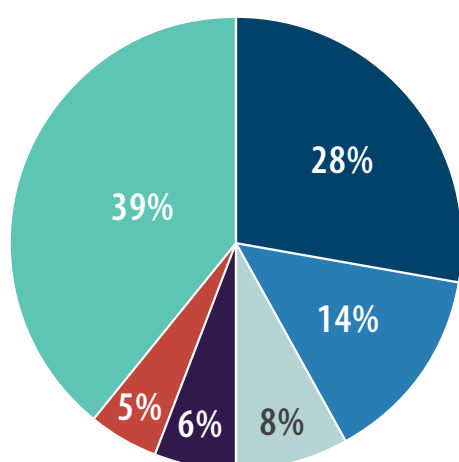
Exposure to foreign jurisdictions poses ML/TF vulnerability because it creates opportunities for international movement of criminal proceeds and the funding of overseas terrorist activity. Further, transactions with foreign jurisdictions add complexity, helping to obscure beneficial ownership and beneficiary customers, and increase potential for offshore tax evasion. This is particularly true when funds have transited through third countries, such as global financial centres (see below). The movement of funds across borders can also create legal impediments for law enforcement to exercise their powers of investigation or arrest.

MOVEMENT OF FUNDS OR VALUE INTERNATIONALLY

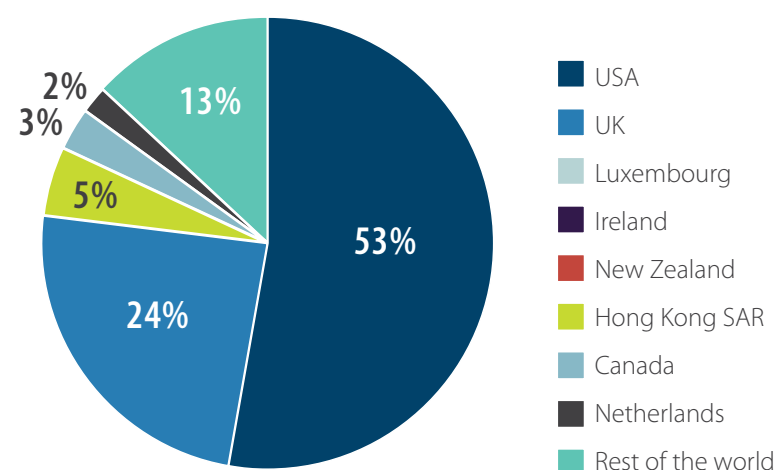
Combined, other domestic banks submitted more than 200,000 IFTIs with a total value of \$109 billion.⁴² Over three-quarters of IFTIs submitted by the subsector related to outgoing transactions, with the vast majority destined for the USA or UK.

International transactions were identified in approximately 12 per cent of the SMR sample and in over one-third of the IR review. The most common jurisdictions in these reports were Singapore, USA, China, UK, Hong Kong SAR, Malaysia and Lebanon.

Incoming IFTIs (\$)



Outgoing IFTIs (\$)



⁴¹ Some reporting entities that do not facilitate international transactions directly use agent banking relationships or third-party arrangements with other financial institutions or remitters to provide this service to their customers. These relationships and associated ML/TF vulnerabilities are discussed on page 51 in the **Delivery channels** section.

⁴² IFTI-related figures associated with jurisdictions carry a 95 per cent confidence rating unless otherwise specified. Extremely small variations may exist for certain jurisdictions due to reporting anomalies, but these do not impact the findings made in this report.

TRANSACTIONS WITH HIGHER-RISK JURISDICTIONS

A very large proportion of IFTIs submitted by the subsector involved a higher-risk jurisdiction, in particular a significant volume of funds flows through global financial centres.⁴³ In total, 90 per cent of IFTIs reported involved a higher-risk jurisdiction.⁴⁴ This figure drops to nine per cent when transactions involving global financial centres are removed.

i While most transactions are likely to be associated with legitimate activities, it is critical other domestic banks develop an understanding of their customers' transactions with higher-risk jurisdictions to assess their risk exposure and detect criminal behaviour.

GLOBAL FINANCIAL CENTRES

Four jurisdictions considered higher risk for money laundering in this report are also home to the world's top four financial centres as ranked by the Global Financial Centres Index. These jurisdictions are hubs of financial trade and house the headquarters of many large corporations. The result is significant financial flows into and out of these jurisdictions to support commercial activity.

By value, more than 80 per cent of IFTIs submitted by other domestic banks involved a global financial centre. Such vast transactional volumes allow criminals to obscure the movement of illicit funds among legitimate financial activity.

Global financial centres are also home to a significant number of highly skilled professional facilitators, such as lawyers and accountants, who help clients structure corporate entities in order to minimise taxes and navigate regulation, but can also help criminals – wittingly or unwittingly – to obscure the source or destination of funds. This additional layer of obfuscation is compounded by the fact that reporting obligation thresholds for international funds transfers can differ between Australia and global financial centres, complicating efforts to obtain end-to-end visibility of funds flows.

Nonetheless, while the amount of illicit funds moving to global financial centres is substantial, AUSTRAC assesses that they are proportionally lower when compared to other jurisdictions deemed high risk for money laundering. This is because:

- the value of legitimate transactions involving these jurisdictions is very high and inflates the overall figure
- risk is partly mitigated by strong AML/CTF regimes in these four jurisdictions, which sets them apart from many of the other jurisdictions deemed higher risk for money laundering.

For these reasons, this report displays both the value of IFTIs associated with all jurisdictions considered higher risk for money laundering and the same figure minus IFTIs associated with global financial centres.

⁴³ This report considers the following jurisdictions as global financial centres: Hong Kong SAR, Singapore, UK and USA in line with the Global Financial Centres Index.

⁴⁴ This finding was made by data-matching the source or destination of IFTIs with a list of foreign jurisdictions considered higher risk for money laundering, terrorism financing, tax evasion and child exploitation. These higher-risk jurisdiction lists were compiled with the assistance of expert advice from international institutions, non-profit organisations and partner agencies.

DETERMINING HIGH-RISK JURISDICTIONS

There is no one-size-fits-all list of high-risk jurisdictions. Reporting entities should adopt a risk-based approach when determining which jurisdictions to consider high risk for their business. AUSTRAC encourages the use of a range of sources that assess jurisdictions on different AML/CTF factors, including but not limited to their regulatory frameworks, threat environment and domain-specific vulnerabilities.

Some reporting entities may choose to use off-the-shelf solutions that risk-rate jurisdictions. If doing so, reporting entities should consider their own risk profile and ensure they can customise default risk ratings to accurately reflect their business.

AUSTRAC has made its own determination about which jurisdictions are considered higher-risk for this report. This takes into account Australia-specific factors, such as top source or destination jurisdictions for higher-risk financial flows, as well as global factors, such as the strength or weakness of a jurisdiction's AML/CTF regulatory regime. Open source information AUSTRAC has drawn on to inform these decisions include:

- the European Union's list of high-risk third countries with strategic deficiencies in their AML/CFT regimes
- the European Union's list of non-cooperative jurisdictions in taxation matters
- the FATF's high-risk and other monitored jurisdictions
- Transparency International's Corruption Perception Index
- the US Department of State's International Narcotics Control Strategy Report.

IFTIs INVOLVING HIGHER-RISK JURISDICTIONS

Incoming value

Outgoing value



5%


\$91.4
BILLION

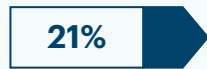

95%



Jurisdictions considered higher risk for money laundering (including global financial centres)



21%


\$2.6
BILLION


79%



Jurisdictions considered higher risk for money laundering (less global financial centres)



17%


\$14.2
BILLION

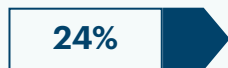

83%



Jurisdictions considered higher risk for tax evasion



24%


\$311
MILLION


76%



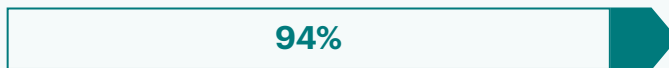
Jurisdictions considered higher risk for terrorism financing



6%


\$405
MILLION


94%



Jurisdictions considered higher risk for child exploitation

Risk Level	Percentage
Minor (Light Teal)	11.11%
Minor (Medium Teal)	11.11%
Minor (Dark Teal)	11.11%
Moderate (Light Orange)	11.11%
Moderate (Medium Orange)	11.11%
Moderate (Dark Orange)	11.11%
Major (Light Red)	11.11%
Major (Medium Red)	11.11%
Major (Dark Red)	11.11%

CONSEQUENCE FACTOR	RATING
Customers	●
Individual businesses and the subsector	●
Australian financial system and community	●
National and international security	●

AUSTRAC assesses that the overall consequences of ML/TF and other predicate offences involving other domestic banks is **moderate**. Consequences include the potential impact or harm that ML/TF and other financial crimes may cause.

Financial crime that impacts other domestic banks has consequences for customers, individual businesses, the subsector as a whole, and the broader Australian economy. The exploitation of other domestic banks to facilitate the financing of terrorism has consequences for national and international security.

CUSTOMERS

AUSTRAC assesses that ML/TF and predicate offences involving other domestic banks has **moderate** consequences for customers of the subsector.

Other domestic banks report customers are impacted by criminal activity in various ways and to varying degrees. This depends on the type of customer, their ability to detect criminal exploitation, and their capacity to absorb potential financial losses. For example, larger, more sophisticated customers such as corporations are better placed to detect and prevent criminal exploitation or absorb financial losses.

The type of criminal activity is another variable that affects the level of harm to customers. For example, bank guarantees against unauthorised transactions generally cover customers for financial losses from frauds. However, victims of scams are likely to suffer unrecoverable financial losses.

Generally, impacts of criminal activity on customers can include:

- financial losses from frauds, identity theft or scams
- emotional or psychological distress caused by financial abuse or identity theft
- negative impact on a customer's credit score for those targeted by loan fraud
- potential criminal implications for customers unknowingly targeted by fraudsters and scammers (i.e. those used as money mules)
- reputational damage for business customers
- for corporate customers, indirect costs associated with combating or preventing criminal exploitation, in particular IT security costs to build cyber resilience.

INDIVIDUAL REPORTING ENTITIES AND THE SUBSECTOR

AUSTRAC assesses that ML/TF and predicate offences involving other domestic banks has **moderate** consequences for individual reporting entities and the subsector as a whole.

While criminal exploitation can damage a reporting entity's reputation, existing customers are likely to continue their relationship with their bank, particularly where there may be financial consequences for a customer ending their relationship (e.g. where they hold a term deposit). However, there may be serious damage to a reporting entity's reputation if they are subject to significant and systemic criminal exploitation, particularly if it is found that an entity's risk mitigation strategies were insufficient to prevent or detect exploitation. This could affect a reporting entity's ability to attract and retain customers – an issue that may become more prominent if the banking sector becomes more competitive, including as a result of Open Banking reforms (see Consumer Data Right - Open Banking on page 53).

Impacts of criminal activity on individual reporting entities or their business groups can be financial, reputational or operational.

Financial costs may include:

- direct loss of revenue from fraud
- indirect loss of revenue from reimbursing customers following criminal exploitation, or payment of civil penalties in the event of serious non-compliance
- increased fraud insurance premiums
- potential downgrade of business group credit rating and associated increase of funding costs
- increased costs to combat criminal attacks, in particular IT security costs to build cyber resilience
- increased costs to improve AML/CTF compliance management
- increased costs or allocation of resources to investigate criminal activity or complaints
- negative impact on share price
- increased public relations costs to counteract reputational damage.

Reputational costs may include:

- damage to brand
- dissatisfaction or loss of investors, customers, partners or debtors
- reduced ability to attract investment and business, and skilled staff.

Operational impacts may include:

- heightened regulatory oversight or law enforcement action
- civil or criminal penalties in the event of serious non-compliance
- loss of staff or change of senior management personnel
- tightening of systems and controls on certain products, services or delivery channels, which could lead to the loss of certain customers.

AUSTRALIAN FINANCIAL SYSTEM AND COMMUNITY

AUSTRAC assesses that ML/TF and predicate offences involving other domestic banks has **major** consequences for the Australian financial system and the community.

Significant or systemic breaches of AML/CTF controls could damage Australia's international economic reputation in relation to the security and safety of Australia's financial sector.

Other consequences of criminal activity on the Australian financial system and the community can include:

- societal harm inflicted upon the community through offences such as drug trafficking, frauds or scams
- reduced government revenue due to tax evasion, affecting the delivery of critical government services
- money laundering resulting in the preservation of illicit assets, the financing of new crimes and the corruption of public officials and private enterprise⁴⁵
- purchases of real estate with the proceeds of crime, driving property prices up and pricing legitimate buyers out of the market.

⁴⁵ D Chaikin, *Effectiveness of anti-money laundering obligations in combating organised crime with particular reference to the professions*, Australian Institute of Criminology, 2018, pages 124-130.

NATIONAL AND INTERNATIONAL SECURITY

AUSTRAC assesses that ML/TF and predicate offences involving other domestic banks has **major** consequences for national and international security.

Serious and organised crime groups in Australia can grow larger and stronger when they are able to launder their illicit funds. Their activities can impact both national and international security interests. For example:

- domestic security can be threatened by gang-related violence (e.g. outlaw motorcycle gangs)
- drug trafficking organisations are critical customers for transnational, serious and organised crime groups based in foreign jurisdictions. These groups can have a negative impact on the security situations in source countries (e.g. cartels engaged in intra-cartel violence).

The potential harm to national and international security from terrorism financing is significant. Potential impacts can include:

- sustaining and enabling the activities of Australian foreign terrorist fighters
- enabling terrorist acts both in Australia and overseas.

Sanctions breaches by customers of other domestic banks can also have consequences for national or international security, especially where they undermine sanctions regimes that are designed to restrain rogue governments or violent non-state actors.

Lastly, bribery and corruption can have negative impacts on economic security and the rule of law in source jurisdictions.



RISK MITIGATION STRATEGIES

Risk mitigation strategies include measures that are mandatory under AML/CTF legislation and other practices reporting entities implement to mitigate ML/TF risk.

Individual reporting entities apply risk mitigation strategies with varied results. While other domestic banks continue to invest in more advanced ML/TF risk mitigation systems and controls, some smaller reporting entities have less sophisticated AML/CTF programs and fewer resources available for robust financial crime and compliance teams. Some banks could make improvements to transaction monitoring programs and SMR submissions to AUSTRAC.

CUSTOMER DUE DILIGENCE

Reporting entities generally employ CDD and ECDD processes to verify customers' identities and assess the legitimacy of their wealth or business operations. During industry consultations, reporting entities described their customer risk rating models and the range of factors they consider when determining a customer's risk rating. These generally include customer type, customer industry or occupation, and the type of financial product or service sought. Many reporting entities noted the customer type holds less weight than the products for which they are applying. The products being applied for add important context for the CDD process.

i Some reporting entities provide products and services that target specific customer types, such as certain types of trust accounts that may be attractive to a DNFBP. Reporting entities should consider the additional risks posed by products targeted towards specific customer types, and should ensure ECDD and ongoing CDD processes involve updating customer information should they apply for a product outside of their traditional profile.

Customers are assessed at onboarding and are classified as low, medium or high risk. A customer's risk rating may increase the frequency with which a reporting entity conducts ongoing CDD, along with more strenuous know your customer (KYC) refresh requirements and greater scrutiny of the customer's transactions. Generally, medium and high-risk customers are subject to more rigorous ECDD (due to the increased risks associated with their transactions or behaviour), and low-risk customers are not subject to ECDD unless flagged elsewhere. In some instances, reporting entities noted they will not onboard a high-risk customer.

Reporting entities highlighted that customer information provided and verified at onboarding will often quickly become out of date. Given this, reporting entities must ensure their transaction monitoring programs can be used to identify contemporary information such as employment status.

i Reporting entities should regularly review their processes and ensure appropriate mitigation strategies are in place to proactively detect higher-risk customers.

OUTSOURCING OF CDD AND OTHER AML/CTF PROCESSES

The Australian banking sector is looking to increase the globalisation of their compliance operations and significantly expand their risk management and compliance teams by engaging offshore personnel with the required expertise or outsourcing aspects of these processes to third parties. This approach may increase the banks' capacity and strengthen their capability to manage and respond to increasing global ML/TF risks. The increased capacity may improve the quality and timeliness of transaction monitoring and reporting by the banks, and outsourcing AML/CTF processes can also lower operating costs.

Outsourcing CDD and other AML/CTF processes to offshore subsidiaries or third parties may carry risks, including diminished accountability and control by the domestic entity, and jurisdictional risk, such as exposing reporting entities to criminal actors based in foreign jurisdictions or threats that might be more prevalent in such certain jurisdictions. Reporting entities should also be mindful of the circumstances in which disclosures to offshore entities are permissible under the AML/CTF Act. It is recommended reporting entities proposing to engage in offshore outsourcing should engage with AUSTRAC at the earliest opportunity.

TRANSACTION MONITORING PROGRAMS

The use of off-the-shelf transaction monitoring programs is very common across the subsector. However, industry representatives report that these systems are subject to a high degree of customisation. For example, one reporting entity with more significant international correspondent banking relationships confirmed their transaction monitoring program was weighted more heavily by foreign jurisdiction risk.

During consultations, reporting entities described a range of scenario-based profiles, business rules, parameters and alerts to detect suspicious activity. Following detection, bank policies require unusual transactions to be escalated and ECDD to be completed where appropriate. The information collected will then be used for reporting and to update customer risk profiles. Reporting entities also described the difficulty transaction monitoring programs have with institutional or corporate customers due to the large variety of transactional profiles and small numbers of clients and transactions.

In recent years AUSTRAC has identified instances where some transaction monitoring and ECDD processes were poorly designed and executed, and suspicious matters were not always reported to AUSTRAC. Ensuring accurate information is received from customers at onboarding can reduce the likelihood of transaction monitoring failures. For example, a misspelt name or address may result in a high-risk transaction not being appropriately flagged for escalation. It is important that reporting entities upgrade and adjust their transaction monitoring programs frequently to reflect changes with their own ML/TF risk assessments and other external considerations (such as guidance released by AUSTRAC and other international bodies such as the FATF).

i The mere presence of a transaction monitoring program is not adequate by itself. Reporting entities should ensure that:

- flagged transactions are appropriately reviewed and escalated if necessary
- suspicious matters are reported to AUSTRAC
- transaction monitoring programs are frequently reviewed to ensure business rules and detection parameters are relevant and reflect contemporary ML/TF threats.

RISK ASSESSMENTS

During consultations, every reporting entity described risk assessment processes built into their AML/CTF programs. As well as customer risk assessments (described above), reporting entities also outlined processes to risk assess products, delivery channels and foreign jurisdictions.

i A robust risk assessment is the centrepiece of an effective AML/CTF regime. It is important that risk assessment processes have the capacity to generate a genuine understanding of ML/TF exposure at an individual reporting entity level. This means the use of off-the-shelf risk assessment tools needs to be tailored to ensure they reflect the actual risks posed to other domestic banks operating within different contexts. Not only do risk assessments need to be business-specific, they also need to be regularly updated to ensure changes in risk profiles and systems, as well as the nature of products or delivery channels, are addressed in a timely and effective way.

SUSPICIOUS MATTER REPORTING TO AUSTRAC

The quality and quantity of SMR submissions by other domestic banks varies significantly between individual reporting entities. To some degree, this variation is consistent with differences between reporting entities, notably the scale of operations and complexity of products, services and delivery channels. However, it also likely reflects varied levels of understanding of ML/TF risks and effectiveness of CDD, ECDD and transaction monitoring processes.

There were examples of good SMR reporting practices from the subsector. This included reports containing detailed transaction histories, records of contact with the customer or suspicious party, and relevant information uncovered from carrying out ECDD.

AUSTRAC observed instances in which SMR submissions could be improved. For example:

- **Including a more detailed grounds for suspicion.** This information-rich section provides valuable intelligence for AUSTRAC and its partner agencies. Reporting entities are encouraged to include all information from ECDD activities and financial investigations in the grounds for suspicion.
- **Avoiding trigger-based reporting.** Trigger-based reporting is a practice in which a reporting entity submits an SMR solely on the basis of a trigger generated by their transaction monitoring system without conducting further investigation to form suspicion on reasonable grounds. Similarly, template reporting where there is little unique detail in the grounds for suspicion. Such reports provide little intelligence value and generally cannot be actioned.
- **Including more contextual or identifying information** obtained during post-transaction analysis, such as account numbers, source of wealth or source of income. Trigger-based reports and reports submitted repeatedly on the same customer should contain additional contextual information to increase their intelligence value for AUSTRAC and partner agencies.

- **Summarising suspicions** by including a short summary at the top of the grounds for suspicion section of the SMR. This would help expedite review and assessment of reports by AUSTRAC and partner agencies.
- **Including documents that provide additional context.** If relevant, include bank statements, CCTV footage, account opening forms or identity verification documents to provide AUSTRAC analysts with a more detailed and complete picture of suspicious transactions while also helping to triage work.

During consultations, some reporting entities had questions about SMR reporting. AUSTRAC encourages reporting entities to have policies and procedures in place to help staff identify and report suspicious matters.

FURTHER RESOURCES ON SUSPICIOUS MATTER REPORTING

Further guidance on submitting SMRs can be found on [AUSTRAC's website](#). AUSTRAC has also developed the following resources to help reporting entities understand what makes a good SMR, and how SMRs help protect Australia from financial crime and terrorism financing.

- [Frequently asked questions](#) about suspicious matter reporting
- [Tips](#) on how to make effective suspicious matter reports to AUSTRAC
- [Reference guide](#) with real-life examples
- [Checklist](#) containing key elements and details required.

AUSTRAC encourages all other domestic banks to review these resources and consider if their reporting could be improved.

APPENDIX A: GLOSSARY

NAME	DESCRIPTION
Authorised deposit-taking institution (ADI)	An authorised deposit-taking institution (ADI) is a body corporate authorised under the <i>Banking Act 1959</i> , to carry on banking business in Australia (e.g. a bank, building society or credit union), the Reserve Bank of Australia or a person who carries on state banking.
AML/CTF	Anti-money laundering and counter-terrorism financing.
AML/CTF program	A document that sets out how a reporting entity meets its AML/CTF compliance obligations.
Beneficial owner	An individual who owns 25 per cent or more, or otherwise controls the business of an entity.
Corporate and institutional banking	Corporate and institutional banking are specialised divisions within a bank that offer a comprehensive suite of products and services for businesses and large institutions, both locally and abroad. In particular they provide complex financing and advisory functions for corporate and government clients.

NAME	DESCRIPTION
Cuckoo smurfing	A money laundering process where criminal proceeds are used to make a cash deposit to an innocent person in Australia who is expecting to receive a money transfer from overseas. This deposit is made on behalf of a complicit remittance provider. The remittance provider makes the equivalent payment to the criminal overseas. Using this method, funds do not physically move internationally, nor is there a money trail.
Customer due diligence (CDD)	Customer due diligence (CDD) is the process where pertinent information of a customer's profile is collected and evaluated for potential ML/TF risks.
Designated business group (DBG)	A designated business group (DBG) is a group of two or more reporting entities who join together to share the administration of some or all of their anti-money laundering and counter-terrorism financing obligations.
Designated non-financial businesses and professions (DNFBPs)	The FATF Recommendations defines designated non-financial businesses and professions (DNFBPs) as casinos, real estate agents, precious metal/precious stone dealers, lawyers, notaries, other independent professionals, accountants, as well as trust and company service providers.
Enhanced customer due diligence (ECDD)	Enhanced customer due diligence (ECDD) is the process of undertaking additional customer identification and verification measures in certain circumstances deemed to be high risk.
Financial Action Task Force (FATF)	The Financial Action Task Force (FATF) is an inter-governmental body focused on fighting money laundering, terrorism financing and other related threats to the integrity of the international financial system, by ensuring the effective implementation of legal, regulatory and operational measures.
Financial institutions	<p>FATF defines a financial institution as any natural or legal person who conducts as a business one or more of the following activities or operations for or on behalf of a customer:</p> <ul style="list-style-type: none"> • acceptance of deposits and other repayable funds from the public • lending • financial leasing • money or value transfer services • issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money) • financial guarantees and commitments • participation in securities issues and the provision of financial services related to such issues • individual and collective portfolio management

NAME	DESCRIPTION
Financial institutions cont.	<ul style="list-style-type: none"> • safekeeping and administration of cash or liquid securities on behalf of other persons • otherwise investing, administering or managing funds or money on behalf of other persons • underwriting and placement of life insurance and other investment related insurance • money and currency changing • trading in money market instruments, foreign exchange, exchange, interest rate and index instruments, transferable securities, commodity futures trading.
Global financial centres	For the purposes of this report, global financial centres refer to the jurisdictions that are home to the top four cities in the Global Financial Centres Index 26.
Inherent risk	Inherent risk represents the amount of risk that exists in the absence of AML/CTF controls implemented by the reporting entity.
Integration	The final stage of the money laundering cycle, in which illicit funds or assets are invested in further criminal activity, 'legitimate' business or used to purchase assets or goods. At this stage, the funds are in the mainstream financial system and appear to be legitimate.
Intelligent deposit machine (IDM)	Intelligent deposit machines (also known as Smart ATMs) are a type of ATM that have additional features, such as reconciling cash deposits in real time, conducting cardless deposits, transferring money between accounts and depositing cheques.
International funds transfer instruction (IFTI)	<p>An international funds transfer instruction (IFTI) involves either:</p> <ul style="list-style-type: none"> • an instruction that is accepted in Australia for money or property to be made available in another country, or • an instruction that is accepted in another country for money or property to be made available in Australia.
Layering	The second stage of the money laundering cycle, which involves moving, dispersing or disguising illegal funds or assets to conceal their true origin.
ML/TF	Money laundering and terrorism financing.
Placement	The first stage of the money laundering cycle, in which illicit funds first enter the formal financial system.

NAME	DESCRIPTION
Politically exposed person (PEP)	<p>A politically exposed person (PEP) is an individual who holds a prominent public position or role in a government body or international organisation, either in Australia or overseas. Immediate family members and close associates of these individuals are also considered PEPs. PEPs often have power over government spending and budgets, procurement processes, development approvals and grants.</p> <p>The AML/CTF Act identifies three types of PEPs:</p> <ul style="list-style-type: none"> • Domestic PEP – someone who holds a prominent public position or role in an Australian government body. • Foreign PEP – someone who holds a prominent public position or role with a government body in a country other than Australia. • International organisation PEP – someone who holds a prominent public position or role in an international organisation, such as the United Nations (UN), the World Trade Organisation (WTO) or the North Atlantic Treaty Organisation (NATO).
Predicate offence	For the purpose of this risk assessment, a predicate offence is any offence that generates proceeds of crime.
Private banking	Private banking consists of personalised financial services and products offered to high net-worth individual clients. It includes a wide range of wealth management services including investing and portfolio management, tax services, insurance and trust and estate planning.
Residual risk	Residual risk is the amount of risk that remains after a reporting entity's AML/CTF controls are accounted for.
Retail banking	Retail banking provides financial services to individual customers as opposed to large institutions. Services offered generally include savings and checking accounts, mortgages, personal loans, debit and credit cards and certificates of deposit.
Suspicious matter report (SMR)	<p>A report that must be submitted by a reporting entity under the AML/CTF Act if they have reasonable grounds to suspect that a transaction may be related to money laundering, terrorism financing, tax evasion, proceeds of crime or any other serious crimes under Australian law. An SMR must also be submitted if the reporting entity has reasonable grounds to suspect the customer or an agent of the customer is not who they say they are.</p>
Structuring	Making or receiving a series of cash transactions intentionally structured to be below the \$10,000 reporting threshold.
Threshold transaction report (TTR)	A report submitted to AUSTRAC about a designated service provided to a customer by a reporting entity that involves a transfer of physical or digital currency of \$10,000 or more or the foreign currency equivalent.
Trade-based money laundering (TBML)	The process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illicit origin.

NAME	DESCRIPTION
Transnational, serious and organised crime (TSOC)	<p>Transnational, serious and organised crime covers a wide range of the most serious crime threats impacting Australia including:</p> <ul style="list-style-type: none"> • manufacture and trade of illicit commodities, including drugs and firearms • sexual exploitation of children • human trafficking and slavery • serious financial crime • cyber crime. <p>Key enablers of TSOC include money laundering, identity crime and public sector corruption.</p>
Trigger-based reporting	<p>Where a reporting entity submits a suspicious matter report to AUSTRAC solely on the basis of a trigger generated by their transaction monitoring system without conducting further investigation.</p>



APPENDIX B: RISK ASSESSMENT METHODOLOGY

The methodology used for this risk assessment follows FATF guidance, which states that ML/TF risk at the national level should be assessed as a function of criminal threat, vulnerability and consequence.

This risk assessment considered 18 risk factors across the above three categories and each risk factor was assessed as low, medium or high, as per the table below. These assessments were based on quantitative and qualitative intelligence inputs, including analysis of SMR and other reporting data, intelligence assessments from partner agencies, and feedback from industry.

The average scores of the criteria provides the total risk score for each category, and the average of the three risk scores for each category provides the overall risk rating for the subsector. Each risk factor was equally weighted and an average risk score was determined for each of the three categories. Each category was equally weighted and an average risk score determined the overall inherent risk rating for the subsector.

CRIMINAL THREAT ENVIRONMENT		
Low	Medium	High
Minimal variety of money laundering methodologies. There is a low level of involvement by SOCGs and other high-risk entities.	Money laundering methodologies are moderately varied. There is a medium level of involvement by SOCGs and other high-risk entities.	Money laundering methodologies are highly varied. There is a high level of involvement by SOCGs and other high-risk entities.
Low number of money laundering cases in the subsector, and low associated values.	Moderate number of money laundering cases in the subsector, and moderate associated values.	High number of money laundering cases in the subsector, and high associated values.
Minimal variety of terrorist financing methodologies. None or a very small number of terrorist groups and their financiers, associates and facilitators using the subsector.	Terrorist financing methodologies are somewhat varied. There is a small number of terrorist groups, financiers, associates and facilitators using the subsector.	Terrorist financing methodologies are highly varied. There are several terrorist groups, financiers, associates and facilitators using the subsector.
Very few instances of terrorism financing in the subsector, with negligible or very low associated values.	Some instances of terrorism financing in the subsector, with low associated values.	Multiple instances of terrorism financing in the subsector, with moderate or high associated values.
Minimal variety of predicate offences. There is a low level of involvement by SOCGs and other higher-risk entities.	Predicate offences are moderately varied. There is a medium level of involvement by SOCG and other higher-risk entities.	Predicate offences are highly varied. There is a high level of involvement by SOCG and other higher-risk entities.
Low number of predicate offences in the subsector, and low associated values.	Moderate number of predicate offences in the subsector, and moderate associated values.	High number of predicate offences in the subsector, and high associated values.

VULNERABILITIES		
Low	Medium	High
Subsector has a small customer base.	Subsector has a medium customer base.	Subsector has a large customer base.
Few higher-risk customers.	A moderate number of higher-risk customers.	A high number of higher-risk customers.
Provision of product or service rarely involves cash, or involves cash in small amounts.	Provision of product or service sometimes involves cash, or involves cash in moderate amounts.	Provision of product or service often involves cash, or involves cash in large amounts.
Funds and/or value are not easily stored or transferred.	Funds and/or value can be stored or transferred with a small amount of difficulty.	Funds and/or value are easily stored or transferred.
Product or service is provided predominantly through direct contact, with minimal remote services.	Mix of direct and remote services.	Predominantly remote services, with minimal direct contact.
Subsector tends to have simple and direct delivery arrangements.	Subsector tends to utilise some complex delivery arrangements.	Subsector tends to utilise many complex delivery arrangements.
Funds and/or value are generally not transferred internationally.	Moderate amount of funds and value can be transferred internationally.	Significant amounts of funds and/or value are easily transferred internationally.
Transactions rarely or never involve high-risk jurisdictions.	Transactions sometimes involve high-risk jurisdictions.	Transactions often involve high-risk jurisdictions.

CONSEQUENCES		
Minor	Moderate	Major
Criminal activity enabled through the subsector results in minimal personal loss.	Criminal activity enabled through the subsector results in moderate personal loss.	Criminal activity enabled through the subsector results in significant personal loss.
Criminal activity enabled through the subsector does not significantly erode the subsector's financial performance or reputation.	Criminal activity enabled through the subsector moderately erodes the subsector's financial performance or reputation.	Criminal activity enabled through the subsector significantly erodes the subsector's financial performance or reputation.
Criminal activity enabled through the subsector does not significantly affect the broader Australian financial system and community.	Criminal activity enabled through the subsector moderately affects the broader Australian financial system and community.	Criminal activity enabled through the subsector significantly affects the broader Australian financial system and community.
Criminal activity enabled through the subsector has minimal potential to impact on national security and/or international security.	Criminal activity enabled through the subsector has the potential to moderately impact on national security and/or international security.	Criminal activity enabled through the subsector has the potential to significantly impact on national security and/or international security.

APPENDIX C: STATISTICS

Note that figures within the same category in the tables below may exceed 100 per cent. This is because multiple attributes may be present in the same report.

MONEY LAUNDERING ATTRIBUTES FROM SMR SAMPLE AND IR REVIEW

ATTRIBUTE	SMR SAMPLE	IR REVIEW
Reports that identified money laundering	27%	50%
Top 5 suspicious transaction activities		
Multiple transactions	21%	N/A
Large transactions	21%	N/A
Cash deposits (face-to-face)	16%	N/A
Structuring	12%	N/A
Cash withdrawals (face-to-face)	12%	N/A
Customer type		
Individual	92%	86%
Company	15%	59%
Trust	2%	0%
Sole trader	1%	0%
Involved PEP		
Yes	0.6%	4.5%
No	99.4%	95.5%

ATTRIBUTE	SMR SAMPLE	IR REVIEW
Involved DNFBP		
Yes	2.4%	13.6%
No	97.6%	86.4%
Product used		
Transaction account	66%	68%
Loan accounts	7%	0%
Credit card accounts	7%	0%
Chequebooks	4%	4.5%
Bank cheques	2%	9%
Trust accounts	2%	0%
Term deposits	1%	0%
Involved a higher-risk jurisdiction		
Yes	4.3%	64%
No	95.7%	36%
Involved cash		
Yes	55%	95%
No	45%	5%

PREDICATE OFFENCE ATTRIBUTES FROM SMR SAMPLE AND IR REVIEW

ATTRIBUTE	SMR SAMPLE	IR REVIEW
Reports that identified a predicate offence	77%	68%
Key predicate offences		
Frauds	38%	17%
Scams	14%	10%
Tax evasion	8%	20%
Other high-impact predicate offences	1.3%	12%
Other high-impact predicate offences		
Drug trafficking	0.85%	3%
Firearms trafficking	0.4%*	5%
Bribery and corruption	0.4%	0%
Child exploitation	0.04%	2%
Sanctions violations	0%	2%
Modern slavery	0%*	0%

*determined using keyword analysis

ATTRIBUTE	SMR SAMPLE	IR REVIEW
Top 5 suspicious transaction activities		
Multiple transactions	15%	N/A
Large transactions	14%	N/A
Cash withdrawals (face-to-face)	9%	N/A
Cash deposits (face-to-face)	6%	N/A
Structuring	6%	N/A
Customer type		
Individual	93%	87%
Company	12%	47%
Trust	2%	0%
Sole trader	1%	0%
Involved PEP		
Yes	0.6%	0%
No	99%	100%
Involved DNFBP		
Yes	2%	3%
No	98%	97%
Product used		
Transaction account	63%	53%
Credit card accounts	8%	3%
Loan accounts	6%	0%
Chequebooks	3%	3%
Bank cheques	2%	7%
Trust accounts	1%	0%
Term deposits	1%	0%
Involved a higher-risk jurisdiction		
Yes	10%	63%
No	90%	37%
Involved cash		
Yes	28%	77%
No	72%	23%

TERRORISM FINANCING ATTRIBUTES FROM SMR SAMPLE AND IR REVIEW

ATTRIBUTE	SMR SAMPLE	IR SAMPLE
Reports that identified terrorism financing	0.3%	14%
% of all TF-related reports across entire reporting population	6%	9.7%
Top 5 suspicious transaction activities		
Multiple transactions	37.5%	N/A
Structuring	25%	N/A
Large transactions	12.5%	N/A
Cash deposits (face-to-face)	0%	N/A
Cash withdrawals (face-to-face)	0%	N/A
Customer type		
Individual	62.5%	100%
Company	62.5%	0%
Trust	12.5%	0%
Sole trader	12.5%	0%
Involved PEP		
Yes	0%	0%
No	100%	100%
Involved DNFBP		
Yes	12.5%	0%
No	87.5%	100%
Product used		
Transaction account	50%	50%
Term deposits	12.5%	17%
Trust accounts	12.5%	0%
Loan accounts	0%	0%
Credit card accounts	0%	0%
Chequebooks	0%	0%
Bank cheques	0%	0%
Involved a higher-risk jurisdiction		
Yes	37.5%	33%
No	62.5%	77%
Involved cash		
Yes	25%	83%
No	75%	17%



AUSTRAC.GOV.AU

