



Australian Government

AUSTRAC

FIGHTING  
FINANCIAL  
CRIME  
TOGETHER



# AUSTRALIA'S MAJOR 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](http://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](http://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](http://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 major 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](mailto: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](http://austrac.gov.au/contact-us/form).

# CONTENTS

---

|  |           |
|--|-----------|
| <b>EXECUTIVE SUMMARY</b>                 | <b>03</b> |
| <b>PURPOSE</b>                           | <b>08</b> |
| <b>BACKGROUND</b>                        | <b>10</b> |
| <b>METHODOLOGY</b>                       | <b>12</b> |
| <b>MAJOR BANKS: REPORTING TO AUSTRAC</b> | <b>15</b> |
| <b>CRIMINAL THREAT ENVIRONMENT</b>       | <b>17</b> |
| Money laundering                         | 19        |
| Terrorism financing                      | 27        |
| Predicate offences                       | 29        |
| <b>VULNERABILITIES</b>                   | <b>40</b> |
| Customers                                | 41        |
| Products and services                    | 50        |
| Delivery channels                        | 58        |
| Foreign jurisdictions                    | 65        |
| <b>CONSEQUENCES</b>                      | <b>69</b> |
| <b>RISK MITIGATION STRATEGIES</b>        | <b>73</b> |
| <b>APPENDICES</b>                        | <b>78</b> |



# EXECUTIVE SUMMARY

---

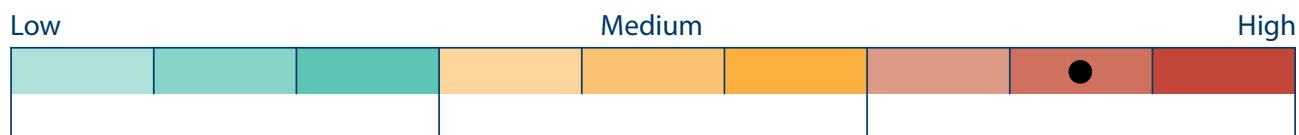
For the purposes of this assessment, Australia's major banks are the four largest authorised deposit-taking institutions (ADIs) in Australia.<sup>1</sup> This subsector sits at the centre of the financial services industry, together controlling approximately three-quarters of assets held by all ADIs and serving some 47 million customers. By providing an extensive range of products and services to retail, corporate, institutional and private banking customers, major banks play a critical role in supporting economic activity across Australia.

---

<sup>1</sup> Wholly owned subsidiaries of the four major banks are also considered within the scope of this risk assessment.



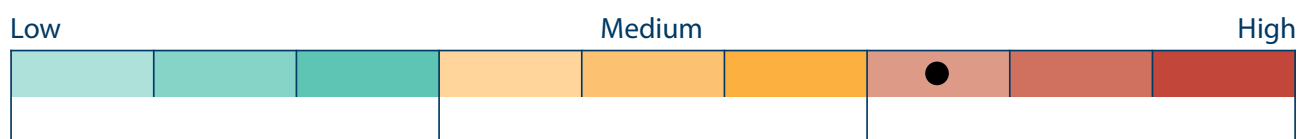
## OVERALL RISK RATING



AUSTRAC assesses the overall money laundering and terrorism financing (ML/TF) risk associated with Australia's major banks to be **high**. This rating is based on assessments of the criminal threat environment, inherent vulnerabilities in the subsector and consequences associated with the criminal threat. These assessments are influenced by a number of factors, including but not limited to, the scale of the subsector's operations, the size of its customer base, the breadth and accessibility of products and services offered, and the subsector's jurisdictional reach.

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

## CRIMINAL THREAT ENVIRONMENT



AUSTRAC assesses the threat of ML/TF facing Australia's major banks as **high**.

The criminal threat environment facing major banks is varied, complex and extensive. A review of intelligence holdings and suspicious matter reports (SMRs) submitted by the subsector indicates the primary threats facing major banks are money laundering, tax evasion, drug trafficking, frauds and scams. To a lesser extent, major banks are also exposed to other high-impact predicate offences such as sanctions violations, bribery and corruption, child exploitation and modern slavery. While likely limited, exposure to these crimes is inevitable given the scale and international reach of the subsector, as well as its extensive range of products and services.

## MONEY LAUNDERING

The nature and extent of money laundering threats facing Australia's major banks is assessed as **high**.

Suspected money laundering was reported in nearly half (46 per cent) of SMRs sampled for this report, while major banks were identified in two-thirds of all money laundering-related intelligence reports reviewed for this assessment.<sup>2</sup> In addition, data-matching identified more than half of the individuals charged with Commonwealth money laundering-related offences between 1 January 2017 and 31 December 2018 in reports submitted by major banks.

<sup>2</sup> See **Methodology** for an outline of the intelligence report review undertaken for this report.

Money laundering methodologies faced by major banks are highly varied and range from relatively simple to very sophisticated and were identified across all stages of the laundering cycle. A high level of misuse of the subsector's extensive cash deposit facilities and the use of complex company structures and associated banking arrangements to obscure the source and beneficial ownership of funds was identified. Major banks are also exposed to money laundering through the purchase of high-value assets, particularly real estate. This is largely due to the subsector's dominance of the home loan markets and provision of tailored products to real estate agents and other high-value asset dealers.

## TERRORISM FINANCING

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

Major banks submitted almost three-quarters of all terrorism financing-related SMRs in the reporting period, although many of these were based on adverse media about a customer rather than suspicious transactions. Therefore, actual exploitation of the subsector is likely to be more limited. Major banks were identified in nearly half (46 per cent) of all intelligence reports about suspected terrorism financing. Data-matching identified more than half of entities charged with a terrorism-related offence between 2014 and 2018 in reports submitted by the subsector. Despite their high exposure to suspected terrorism financing, associated values are generally low and the methods employed are largely unsophisticated and unvaried.

## PREDICATE OFFENCES

The nature and extent of predicate offending faced by major banks is assessed as **high**.<sup>3</sup>

The subsector was identified in more intelligence reports relating to predicate offending than any other banking subsector. These reports often involved sophisticated methods or serious and organised crime entities – factors that make predicate offences difficult to detect.

Tax evasion was the most common predicate offence identified impacting the subsector, appearing in 19 per cent of intelligence reports and nine per cent of the SMR sample. While instances of suspected corporate and personal income tax evasion were almost equal, the threat posed by corporate tax evasion is likely to be more significant due to higher associated values.

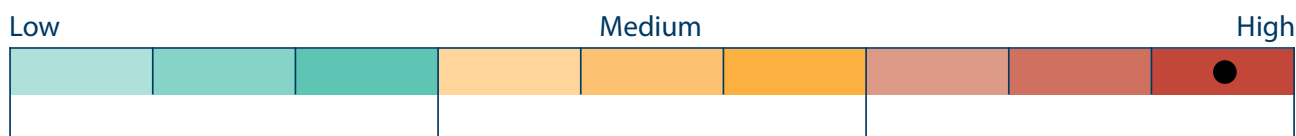
While not as prevalent in reporting, AUSTRAC assesses drug trafficking to be the second most common predicate offence affecting major banks. This assessment is based on findings from the intelligence report review coupled with the size of Australia's illicit drug market, the scale of the subsector and its exposure to cash deposits. These factors likely expose major banks to a significant amount of drug proceeds. It is also assessed that a portion of SMRs and intelligence reports that were identified as relating to 'money laundering' alone, highly likely involve the proceeds of drug trafficking.

Frauds appeared in eight per cent of intelligence reports, while scams appeared in three per cent. These intelligence reports tended to highlight serious offending – most involved the exploitation of a company or had an offshore nexus. Intelligence reports generally identify serious criminal activity so they likely under-represent the overall volume of frauds and scams impacting major banks. The SMR sample identified slightly higher rates of frauds (nine per cent) and scams (five per cent).

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

<sup>3</sup> 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.

## VULNERABILITIES



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

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

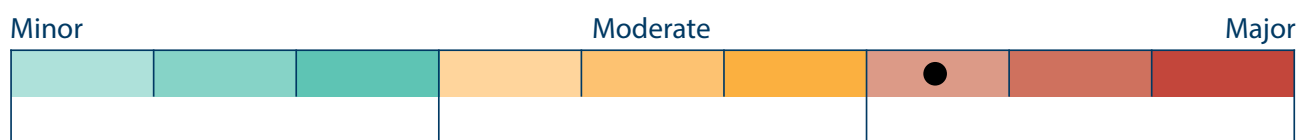
- **a very large customer base**, with approximately 47 million customers. The subsector also has more high-risk customers than all other reporting entities combined, although this is generally proportionate to the size of the customer base. Major banks also have a significant number of customers in **higher-risk** categories. These can include:
  - known or suspected criminal entities<sup>4</sup>
  - politically exposed persons (PEPs)
  - companies, trusts and other legal entities
  - designated non-financial businesses and professions (DNFBPs)<sup>5</sup>
  - temporary visa holders
  - high net-worth individuals
  - financial institutions.<sup>6</sup>
- **very high exposure to cash** due to extensive national cash deposit and withdrawal infrastructure, and a large number of products and services that can be used to **store and move funds** easily and quickly. Products assessed as most vulnerable to ML/TF include:
  - transaction accounts
  - credit card accounts
  - bank cheques
  - trust accounts
  - correspondent banking services.
- the level of face-to-face customer contact is declining in favour of **remote service delivery channels**, particularly online banking and ATMs. These channels can offer criminals anonymity, facilitate identity fraud and other financial crimes, and complicate detection of unusual or suspicious transactions.
- very high exposure to **foreign jurisdiction risk**. In the reporting period, major banks facilitated \$3.5 trillion in international funds transfers – more than all other AUSTRAC reporting entities combined. This exposes the subsector to a high level of foreign jurisdiction risk, and can make it difficult to detect the movement of criminal proceeds offshore.

<sup>4</sup> 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 major banks do not knowingly provide products or services to known or suspected criminals.

<sup>5</sup> 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.

<sup>6</sup> 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 **major**.

### CUSTOMERS

Criminal activity can have **major** consequences for customers. The most significant impacts relate to financial loss, emotional distress as a result of fraud and scam-related offences, and reputational damage, particularly for business customers.

### INDIVIDUAL REPORTING ENTITIES AND THE SUBSECTOR

Criminal activity can have **moderate** financial, reputational or operational consequences for major banks. Given their size, major banks are likely to be able to absorb the financial impacts of criminal activities. However, reputational damage because of systemic criminal exploitation of a major bank may have serious consequences on its ability to attract and retain customers. This may be accentuated if Australia's banking sector becomes more competitive.

### 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 and child exploitation also inflict direct societal harms to the Australian community.

### NATIONAL AND INTERNATIONAL SECURITY

Criminal exploitation of major 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 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

Major banks have a mixed record of applying risk mitigation strategies. On one hand, major banks make significant investments to counter ML/TF risk, engage regularly with AUSTRAC, and some entities have undergone or are undergoing an uplift in their AML/CTF systems, controls and policies. On the other hand, there have been significant and systemic deficiencies detected in the subsector over recent years. Governance and assurance around AML/CTF compliance has been identified as a particular concern, and risk mitigation strategies are not always applied consistently across a reporting entity.





# PURPOSE

---

This assessment provides specific information to Australia's major banks on the ML/TF risks the subsector faces at the national level. Its primary aim is to assist major banks 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 Australia's major 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.

## 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 other 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, Australia's major banks are the four largest ADIs in Australia.

Major banks sit at the centre of the financial services industry and together control 73 per cent of assets held by all ADIs.<sup>7</sup> By providing an extensive range of products and services to retail, corporate, institutional and private banking customers, major banks play a critical role in supporting economic activity across Australia.<sup>8</sup> For example, the subsector's extensive branch networks are important financial access points for many Australians. Major banks are also a key conduit for international transactions into and out of Australia, and serve as important correspondents for other financial institutions.

Reflecting the subsector's size and importance to the economy, the Australian Prudential Regulation Authority (APRA) assess major banks as domestic systemically important banks. This designation means that APRA imposes higher loss absorbency capital requirements on major banks compared to other ADIs.<sup>9</sup>

<sup>7</sup> APRA, *Monthly authorised deposit-taking institution statistics backseries: July 2020*, [apra.gov.au/monthly-authorised-deposit-taking-institution-statistics](https://apra.gov.au/monthly-authorised-deposit-taking-institution-statistics).

<sup>8</sup> Please refer to **Glossary** in **Appendix A** for an explanation of these terms.

<sup>9</sup> APRA, *Information Paper: Domestic systemically important banks in Australia*, 2013, [apra.gov.au/sites/default/files/information-paper-domestic-systemically-important-banks-in-australia-december-2013.pdf](https://apra.gov.au/sites/default/files/information-paper-domestic-systemically-important-banks-in-australia-december-2013.pdf).

Major banks are recognised as reporting entities providing designated services under AML/CTF Act. Under the AML/CTF Act, major 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).

Major banks are also required to provide AUSTRAC with AML/CTF compliance reports.

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 major banks. The risk rating criteria used in this assessment is designed to capture an overall rating for the subsector.

## SIZE OF THE SUBSECTOR<sup>10</sup>



**4**

Number of reporting entities



**47 MILLION**

Number of customers



Total resident assets

**73%** of all ADIs



Total deposits

**47%** of all ADIs



Total loans to households

**63%** of all ADIs



Loans to households  
(housing only)

**78%** of all ADIs

<sup>10</sup> APRA, *Monthly authorised deposit-taking institution statistics backseries: July 2020*, [apra.gov.au/monthly-authorised-deposit-taking-institution-statistics](https://apra.gov.au/monthly-authorised-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 major 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 it was applied can be found in **Appendix B**.

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

1. Analysis of transaction reports, compliance reports and other holdings, including reviewing and labelling 8,000 SMRs submitted by major banks between 1 April 2018 and 31 March 2019 (the **SMR sample**). See the call-out box **Labelling the SMR sample** on page 14 for more detail.
2. A comprehensive review of almost 700 AUSTRAC and partner agency intelligence reports produced between January 2018 and February 2019. Fifty-two per cent of these related to major banks (the **IR review**).<sup>11,12</sup>
3. The results of data-matching (the **data-matching exercise**) of IFTIs, TTRs and SMRs submitted to AUSTRAC by major banks between 30 March 2018 and 1 April 2019 and criminal entities who were:
  - recorded as a member of a significant transnational, serious and organised crime group as at May 2020
  - charged with a money laundering or proceeds of crime-related offence between 1 January 2017 and 31 December 2018<sup>13</sup>
  - charged with a terrorism-related offence between 1 January 2014 and 31 December 2018.<sup>14</sup>
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 major banks' representatives, as well as industry experts and associations.

11 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.

12 A limited number of reports outside of this date range were included where they were deemed to be of high value to the report.

13 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).

14 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)                             |
|--|---|
| <b>Criminal threat</b>                   | Drug trafficking<br>Money laundering        |
| <b>Suspicious transactional activity</b> | Cash deposits<br>Structuring<br>Money mules |
| <b>Products and services</b>             | Transaction account                         |
| <b>Customer type</b>                     | Company                                     |
| <b>Entity attribute</b>                  | Third party<br>DNFBP lawyer                 |
| <b>Foreign jurisdiction</b>              | Jurisdiction 'X'                            |

# MAJOR BANKS: REPORTING TO AUSTRAC

## REPORTS SUBMITTED BY MAJOR BANKS BETWEEN 1 APRIL 2018 AND 31 MARCH 2019

### SMRs



**174,507**  
reports



<sup>15</sup>  
**\$66.1**  
BILLION  
Total value

### TTRs



**2.2+**  
MILLION  
reports



**\$50.3**  
BILLION  
Total value



**\$42.9**  
BILLION  
Cash component

### IFTIs



**15+**  
MILLION  
reports



**\$3.5**  
TRILLION  
Total value

<sup>15</sup> 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 values of 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

The quality and quantity of SMRs submitted by major banks has increased in recent years. Reports are generally detailed and contemporary. Refer to the section **Risk mitigation strategies** 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.

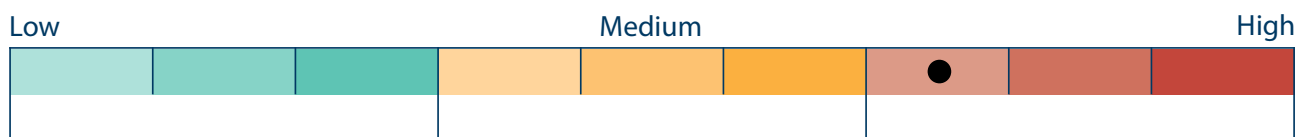
### REFORMS TO 'TIPPING OFF' RESTRICTIONS

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.<sup>16</sup> 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.

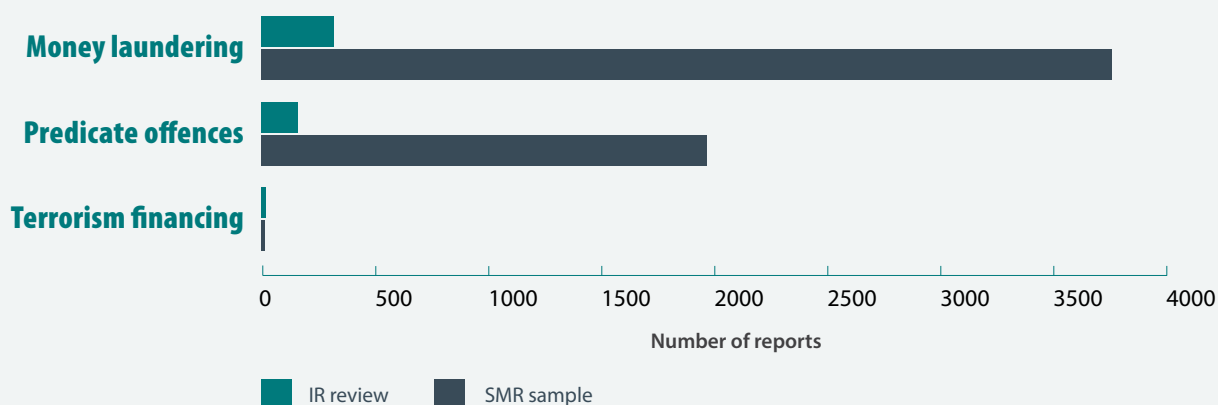
<sup>16</sup> The reforms introduced by the Amendment Act commenced on 17 June 2021.

# CRIMINAL THREAT ENVIRONMENT



| CRIMINAL THREAT ENVIRONMENT FACTOR | RATING      |
|------------------------------------|-------------|
| Money laundering                   | <div></div> |
| Terrorism financing                | <div></div> |
| Predicate offences                 | <div></div> |



**MAJOR BANKS: DETECTED THREATS**

AUSTRAC assesses the criminal threat environment facing Australia's major banks as **high**.

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

The criminal threat environment facing major banks is complex and varied. Intelligence reports and the data-matching exercise indicate that criminal actors, including members of serious and organised crime groups, are more likely to exploit major banks than any other banking subsector. Additionally, the absolute extent of criminal activity identified with a nexus to major banks is almost certainly higher than any other financial sector in Australia.

Money laundering is the primary threat facing major banks, followed by tax evasion, drug trafficking, frauds and scams. Instances of criminality range in sophistication from opportunistic offending to highly complex schemes. While the overall terrorism financing threat to major banks has likely declined in recent years, the subsector has a nexus to many known or suspected cases of terrorism financing in Australia.

## MONEY LAUNDERING

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

This assessment is based on the high proportion of money laundering-related SMRs identified in the SMR sample, as well as a high representation of major banks in money laundering-related intelligence reports.<sup>17</sup> The data-matching exercise, where individuals on criminal lists were matched against transaction reports from major banks, also suggests major banks are highly exposed to known or suspected criminal entities (this process is discussed further in **Higher-risk customers** on page 42).<sup>18</sup>

Money laundering was the most common threat type reported in the SMR sample (46 per cent), and two-thirds of money laundering-related intelligence reports involved the exploitation of at least one major bank. In addition, the data-matching exercise identified that more than half of those charged with a Commonwealth money laundering-related offence between 1 January 2017 and 31 December 2018 appeared in reports submitted by major banks. Although these individuals were not always major bank customers, their presence in reports from the subsector exposes it to a high risk of money laundering.

The subsector is exploited at all stages of the money laundering process, and across all directions (domestic, incoming, outgoing, through and returning). Because of the sheer size of the subsector, its global reach, and the number of products and services that create fast and efficient means for placing, layering and integrating criminal funds, nearly every money laundering methodology observed by AUSTRAC and partner agencies intersects with the subsector at some stage.

Money laundering methodologies are highly varied and range from relatively simple to very sophisticated. The most commonly observed methodologies involve:

- Significant misuse of the subsector's extensive cash deposit infrastructure by both opportunistic criminals and serious and organised crime groups. Key features of organised crime involvement included cuckoo smurfing, offsetting arrangements, and the use of money mules and other third-party depositors.<sup>19</sup>
- Use of complex company structures and associated banking arrangements to obscure the source and beneficial ownership of funds.
- The purchase of high-value assets.

While difficult to detect, intelligence indicates the subsector is also exposed to trade-based money laundering (TBML).

<sup>17</sup> 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).

<sup>18</sup> AUSTRAC assesses that major banks do not knowingly provide products or services to known or suspected criminals.

<sup>19</sup> Please refer to the **Glossary** in **Appendix A** for a definition of 'cuckoo smurfing'.

## CASH-INTENSIVE ACTIVITY

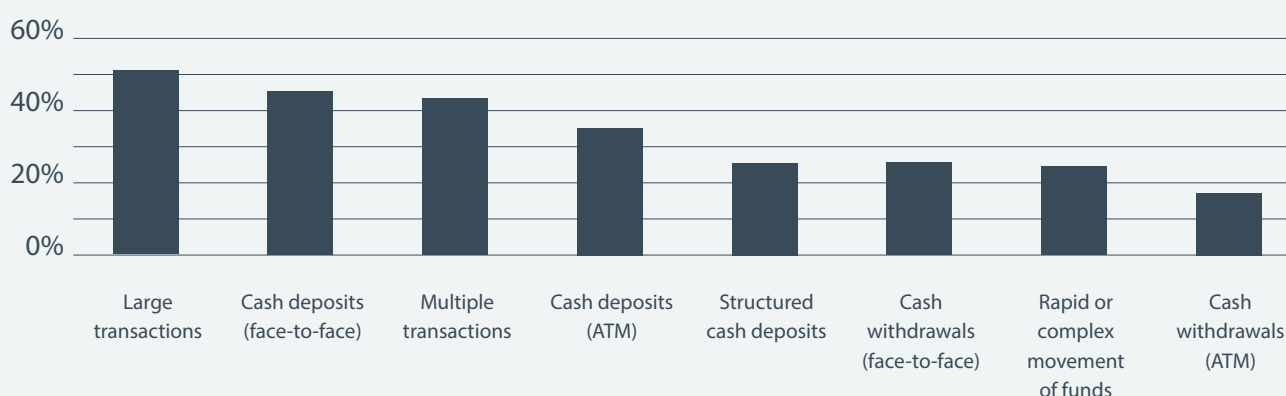
While cash use is declining in Australia, major banks continue to be exposed to a high volume of suspicious cash activity. Suspicious cash transactions were identified in 79 per cent of money laundering-related SMRs and nearly all money laundering-related intelligence reports (93 per cent), although the proportion of SMRs that contain suspicious cash transactions is declining (see **Use of cash** on page 51). Partner agencies and reporting entities consider cash transactions to be one of the most significant money laundering-related risks to major banks.

Criminals exploit the subsector's extensive national network of branches, ATMs and other deposit facilities to place and layer illicit cash (see **Level of customer contact** on page 58). These activities are undertaken by both sophisticated and unsophisticated criminals and – while present across Australia – are concentrated in urban and suburban areas.<sup>20</sup> There is no evidence to suggest criminals target specific banks for any reason other than convenience. For example, individuals involved in cash-intensive criminal activity are more likely to use banks that have large branch and intelligent deposit machine (IDM) networks in their local area, while others may spread their offending across multiple banks to try to obscure the source of funds.<sup>21</sup>

The SMR sample identified that individuals suspected of money laundering frequently combined multiple methodologies to avoid detection and obscure the source or destination of funds. For example, ATM cash deposits were often combined with rapid or complex transfers – sometimes to money mules or other third parties and often to accounts held at different banks.

Suspicious cash deposits were slightly more likely to be conducted face-to-face rather than at an ATM. AUSTRAC assesses this is likely due to reporting behaviours in the subsector rather than actual levels of misuse. For example, customers are forced to conduct higher-value deposits in-branch due to deposit limits at ATMs. Higher-value deposits are more likely to trigger transaction monitoring rules and therefore result in an SMR being submitted. Face-to-face transactions also allow branch staff to observe suspicious interpersonal indicators, which may result in reporting to AUSTRAC.

## ML-RELATED SMRs: METHODS



<sup>20</sup> Of the top 30 suburbs referenced in SMRs, all were urban or suburban centres and only two were outside of New South Wales or Victoria.

<sup>21</sup> IDMs are a type of ATM that accepts cash deposits and have additional features such as cardless cash deposits and faster transactions. Some entities call these 'Smart ATMs'.

### EXPLOITATION BY SERIOUS AND ORGANISED CRIMINALS

Partner agencies report offshore professional money laundering organisations exploit the subsector's extensive cash-deposit infrastructure to place criminal proceeds – often on behalf of drug trafficking organisations.<sup>22</sup> The common money laundering typology of cuckoo smurfing is a key feature of this illicit placement activity (see case study on the right).

Partner agencies also report Australian-based drug trafficking networks deposit criminal proceeds into major banks – often exploiting ATMs that allow third-party cash deposits. There does not seem to be a discernible pattern relating to these deposits, while some groups structure their deposits, others often exceed the \$10,000 reporting threshold.

**i** Reporting entities are encouraged to consider Fintel Alliance's [Cuckoo Smurfing Financial Crime Guide](#) to detect suspicious activity.

### MONEY LAUNDERING ORGANISATIONS EXPLOIT THIRD-PARTY ATM CASH DEPOSITS

In August 2019, AUSTRAC's public-private partnership Fintel Alliance, with support of the major banks, assisted a law enforcement operation that identified and disrupted a money laundering syndicate operating in Australia. Using a detection methodology developed by a major bank, the syndicate was detected conducting more than \$5 million in third-party cash deposits through major bank ATMs over a six-week period.

The money laundering syndicate employed the cuckoo smurfing methodology, where illicit funds are deposited into the accounts of unwitting individuals who are expecting funds from a legitimate transaction (e.g. an inward remittance from a family member). Cuckoo smurfing generally relies on remittance service providers in the originating jurisdiction notifying criminal entities of high-value transactions.

A number of indicators were used to identify the organisation's behaviour:

- successive cash deposits at ATMs within a short timeframe
- successive cash deposits at ATMs to the same account by different individuals
- use of the same mobile number for verifying deposits to multiple beneficiaries.

Fintel Alliance's work led to the arrest of five people, seizures of cash, drugs, firearms, and a community awareness campaign educating the public on the risks of third-party deposits.

<sup>22</sup> Offshore professional money laundering organisations are sophisticated criminal organisations that offer money laundering services to organised crime.

## COMPLEX COMPANY STRUCTURES AND ASSOCIATED BANKING ARRANGEMENTS

The exploitation of companies, trusts and other legal structures was identified in 40 per cent of money laundering-related intelligence reports involving major banks. Common themes of these include:

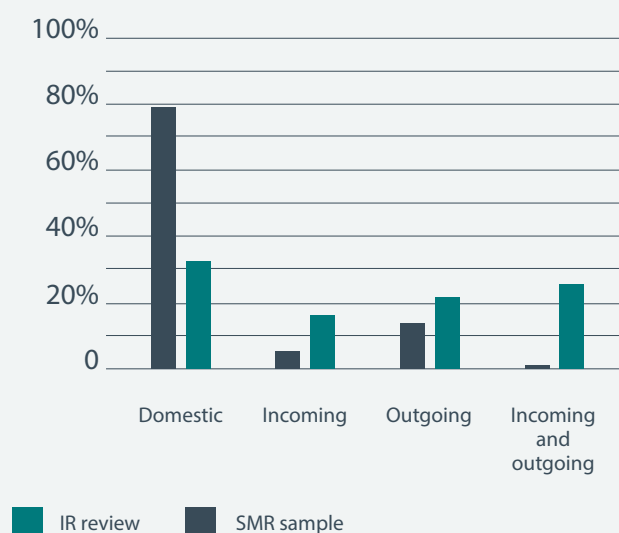
- the layering of funds between multiple entities, often under the control of a small group of individuals
- the use of shell companies (companies with no legitimate business operations)
- an offshore nexus – most of these involved transactions to higher-risk jurisdictions, including tax secrecy jurisdictions<sup>23</sup>
- multiple banks were used to conduct suspicious transactions, obscuring visibility of the destination or source of funds
- entities sometimes operated in higher-risk sectors, such as property development or natural resource extraction<sup>24</sup>
- professional facilitators were sometimes identified receiving suspicious cash or international payments, particularly lawyers.

Criminals will continue to exploit complex company structures to insulate and obfuscate their illicit financial activity. These structures are used by relatively unsophisticated criminals, as well as more sophisticated actors like transnational, serious and organised crime groups.

## ML-RELATED REPORTS: CUSTOMER TYPES



## ML-RELATED REPORTS: DIRECTION OF FUNDS



<sup>23</sup> For more information on higher-risk jurisdictions see page 66.

<sup>24</sup> 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](https://www.fatf-gafi.org/media/fatf/documents/recommendations/BPP-Use-of-FATF-Recs-Corruption.pdf).



### **SHELL COMPANY USED TO LAUNDER FUNDS IN A 'FLOW-THROUGH' SCHEME**

An AUSTRAC intelligence report identified two associated foreign nationals (Individual A and Individual B) exploiting multiple major banks and a shell company in a flow-through scheme likely designed to launder funds linked to corporate tax evasion in an offshore jurisdiction (Jurisdiction 1).

Both individuals entered Australia on a temporary visitor visa. Individual A owns a company (Company A) in Jurisdiction 1, while Individual B manages another company (Company B) in this jurisdiction. It is unknown whether a link exists between these two companies.

Once onshore, both established separate personal accounts with multiple major banks and registered an Australian company (Company C), also establishing a bank account for this company.

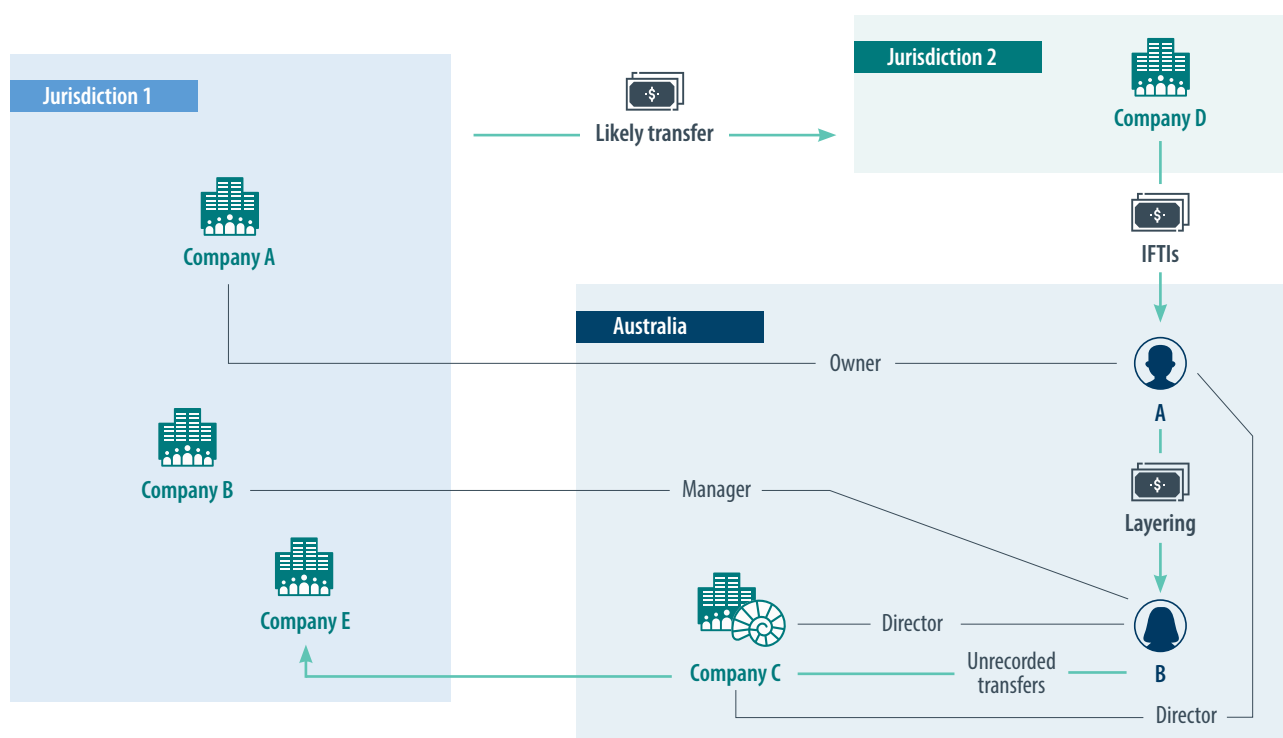
Over five months, the individuals' personal accounts received approximately \$10 million in multiple high-value international transfers from a personal account in Jurisdiction 1 and a company (Company D) domiciled in another offshore jurisdiction (Jurisdiction 2) – both of which are considered higher-risk jurisdictions for money laundering.

It is likely the funds from Jurisdiction 2 were originally sourced from Jurisdiction 1. These transactions were subject to SMRs from multiple major banks, as well as a non-major bank.

Once in their Australian bank accounts, the individuals layered the funds through a variety of methods, including:

- electronic transfers between personal accounts held with various major banks
- very large cash withdrawals by Individual A followed by corresponding deposits into Individual B's account
- multiple large transfers to a lawyer's trust account
- purchasing a bank cheque.

Less than three months after being registered, Company C conducted two very large outgoing transfers to a fourth company (Company E) in Jurisdiction 1. It is highly likely these transfers were funded by the incoming international transfers received by Individual A and Individual B, although it is unknown how the funds were moved into the company's account. Company C was deregistered very shortly after, and was almost certainly a shell company established to launder funds.



## TRADE-BASED MONEY LAUNDERING

While less than one per cent of the SMR sample identified suspected TBML, partner agencies and industry representatives report that TBML is likely to be under-represented in reporting due to challenges relating to detection.

Major banks are exposed to TBML because they sit at the centre of Australia's financial system and serve as a key conduit for financial flows into and out of the country. Major banks also offer a comprehensive range of trade finance products and service a high number of corporate customers – both factors that increase the subsector's exposure to TBML.

### INDICATORS OF TBML AND TRADE FINANCE-BASED MONEY LAUNDERING

In December 2020, the FATF and Egmont Group published *Trade-based Money Laundering: Trends and Developments* which identifies new and emerging TBML risks. The report describes the two most common trade processes exploited for TBML as open account trade and documentary trade, a form of which is documentary collection.

In open account trade, goods are shipped and delivered before payment is made. The bank's role is generally confined to processing a transaction, with little or no knowledge about the underlying contract. Because of their limited knowledge of the transaction, banks have limited ability to detect TBML, making open account trade more vulnerable to TBML.

Documentary collection is a method of trade finance where banks act as intermediaries between the exporter and importer to facilitate the transaction, which may involve the bank providing a guarantee of payment. When acting in this way, banks may review the documentation provided about the trade transaction from the parties. This documentation allows the banks to identify irregularities with the transaction, the parties or their relationships.

Common indicators of TBML include:

- evidence of over- or under-invoicing
- companies trading in higher-risk sectors or goods where prices may be highly subjective, such as natural resources, electronics, luxury goods, vehicles, textiles and scrap or precious metals (including bullion)
- trading activity inconsistent with a customer's profile, inconsistent with global market trends, or via relationships that do not make economic sense
- overly complex company or directorship structures
- upon receiving an incoming international transaction, funds are immediately:
  - split and transferred to multiple domestic company bank accounts; or
  - sent back overseas, often to the ordering company or country (u-turn activity or carouseling)
- funds received from, or exports sent to or through, higher-risk jurisdictions
- significant domestic transfers or cash transactions that exceed expectations for that business
- companies operating in porous border regions close to higher-risk jurisdictions.

The subsector is also exposed to trade finance-based money laundering because major banks offer trade finance products. Trade finance can be exploited by criminals to make otherwise suspicious trade transactions look more legitimate. Additional indicators of trade finance-based money laundering include:

- use of trade finance products that appears inconsistent with received funds or export history
- discrepancies in the documents supplied to support trade finance, such as:
  - variations in the quantity of shipping containers noted in different documents
  - unusual shipping routes
  - significant gaps between actual shipment dates and payment dates.

### FINTEL ALLIANCE TBML WORKING GROUP

In 2020, the Fintel Alliance established a dedicated working group on TBML. This involved representatives from public and private Fintel Alliance members, including major banks, who convened monthly to focus on priority issues. The working group fosters knowledge exchange among Fintel Alliance members. For example, a major bank ran a session targeted at AUSTRAC and its partner agencies to share specialist knowledge about trade finance, and how it detects and mitigates against TBML. In 2020, the working group supported international efforts to better understand TBML by facilitating significant input from industry members into the *Trade-based Money Laundering: Trends and Developments* report published by the FATF and the Egmont Group. The working group has also supported efforts to target high-risk entities impacting the Australian financial system.

### PURCHASE OF HIGH-VALUE ASSETS

The purchase of high-value assets is considered a significant money laundering risk in Australia. Purchasing goods such as real estate, jewellery, boats, artwork, antiques, and precious metals and stones can help criminals reinvest or conceal criminal proceeds. Many of these high-value assets are attractive to money launderers because they are easy to hide and transport across borders and convert back into legitimate funds. Australian-based criminals use this form of money laundering to hide value in Australia and overseas. Overseas-based criminals use this method to conceal assets from authorities in their home jurisdictions.

AUSTRAC assesses that major banks are more exposed to money laundering through high-value assets than any other financial sector. This is partly due to their dominance of Australia's home loan market coupled with the fact that real estate remains an attractive destination for criminal proceeds.<sup>25</sup> Serious and organised crime groups can use real estate as an investment or as a lifestyle benefit to integrate the proceeds of crime into the legitimate economy. The sale and purchase of real estate presents particular appeal to money launderers looking to conceal large sums of money in few transactions, or who use corporate vehicles and trusts to disguise beneficial ownership. Real estate purchases made with loan products may also offer protection from losses in the event of law enforcement confiscation proceedings. For example, if a partner agency restrains a property encumbered by a loan, criminals only stand to lose the value of the deposit, interest and loan repayments made.

Major banks are also exposed to the purchase of high-value assets because they dominate the provision of products to professions that facilitate the purchase of such assets. Major banks submitted 90 per cent of all SMRs where an accountant, real estate agent or lawyer was referenced.<sup>26</sup>

<sup>25</sup> Major banks hold more than three quarters of the ADI home loan market. APRA, *Monthly authorised deposit-taking institution statistics backseries: July 2020*, [apra.gov.au/monthly-authorised-deposit-taking-institution-statistics](https://www.apra.gov.au/monthly-authorised-deposit-taking-institution-statistics).

<sup>26</sup> Determined by analysing the 'Industry/Occupation' field reported in major bank SMRs vis-à-vis the entire reporting population.

Money launderers often exploit these professionals to acquire specialist advice or services to launder criminal proceeds. ML/TF vulnerabilities associated with these entities is discussed further in **Higher-risk customers** on page 41.

### HIGH-VALUE ASSET DEALERS FACILITATING MONEY LAUNDERING

In 2018, a partner agency report identified a real estate agency that received more than \$400,000 in proceeds of crime from known criminals with a transaction description of 'loan'. The funds were then used by the real estate agency to invest in property development. In return, the real estate agency paid the criminals a weekly 'consultancy fee', thus legitimising the proceeds of crime.

A similar scheme was identified in which an individual was providing illicit funds to a luxury car dealer disguised as a loan. These funds would be used to purchase luxury vehicles at wholesale prices. The vehicles were sold for a profit, which would be paid back to the criminal.

In the SMR sample, one per cent of money laundering-related reports involved the suspicious purchase of a high-value asset. While this is low relative to other money laundering methods, the nature of these transactions mean they are infrequent but very high in value. SMRs related to high-value asset purchases were, on average, five times higher in dollar value than all other SMRs. Real estate transactions were most common, followed by luxury vehicles and precious metals or stones. Common themes included:

- suspicious cash deposits into a major bank product (40 per cent)
- international funds transfers (48 per cent), almost all of which were incoming (95 per cent) and involved a higher-risk jurisdiction (92 per cent)
- the involvement of a student or visitor visa holder (10 per cent).

In addition, partner agencies report known cases where:

- illicit funds are used to purchase an asset outright, generally in cash
- illicit funds are used to repay a loan
- real estate agents, mortgage brokers and luxury car dealers willingly help entities to launder criminal proceeds
- complicit real estate agents under- or over-value a property, which is then sold to an accomplice as a means of transferring value between individuals.

## TERRORISM FINANCING

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

This assessment is based on the number of terrorism financing-related SMRs submitted by major banks, findings from the IR review and feedback from partner agencies. The data-matching exercise also suggests major banks are highly exposed to suspected terrorist actors, although actual exploitation is likely to be more limited.<sup>27</sup>

This assessment is lower than determined in previous AUSTRAC assessments and reflects shifting terrorism financing behaviour. While historically major banks have been used to store and send funds to support terrorist 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.

<sup>27</sup> AUSTRAC assesses that major banks do not knowingly provide products or services to known or suspected criminals. See page 42 for a detailed overview of higher-risk customer data-matching exercise results.



Despite shifts in the terrorism financing environment, major banks are still exposed to terrorism financing. For example:

- Major banks submitted 74 per cent of all terrorism financing-related SMRs received in the reporting period.<sup>28</sup>
- Major banks were identified in 46 per cent of all terrorism financing-related intelligence reports analysed for this assessment.
- More than half of the entities charged with a Commonwealth terror offence between 2014 and 2018 were identified in reports submitted by major banks as part of the data-matching exercise. Although these individuals were not always major bank customers, their appearance in reports from the subsector exposes it to a high risk of terrorism financing. For an assessment of known or suspected terrorists that are major bank customers see page 42.

Despite their exposure to suspected terrorism financing activity, associated values in the SMR sample were low, while values associated with intelligence reports were moderate. Identified terrorism financing methods were largely unsophisticated and unvaried. In most identified cases, little effort was made to obfuscate the source or destination of funds, and basic retail banking products were almost always used.

Common themes of the SMR sample include:

- lack of sophistication in products and methods used
- suspicions were triggered by a law enforcement enquiry or adverse media reports
- use of transaction accounts to raise and store funds
- international funds transfers, often to jurisdictions in the Middle East or South Asia
- use of cash
- informal fundraising, where individual customer accounts are used to collect funds disguised as charitable donations, followed by an

international funds transfer or cash withdrawals for transport offshore.

**i** Major 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.

<sup>28</sup> Determined by keyword analysis of all AUSTRAC SMRs submitted between 1 April 2018 to 31 March 2019. Notably however, many of these SMRs were triggered by adverse media, rather than suspicious transactions, and therefore do not necessarily represent actual exploitation of the subsector. The high level of SMR reporting among major banks also contributes to this number.

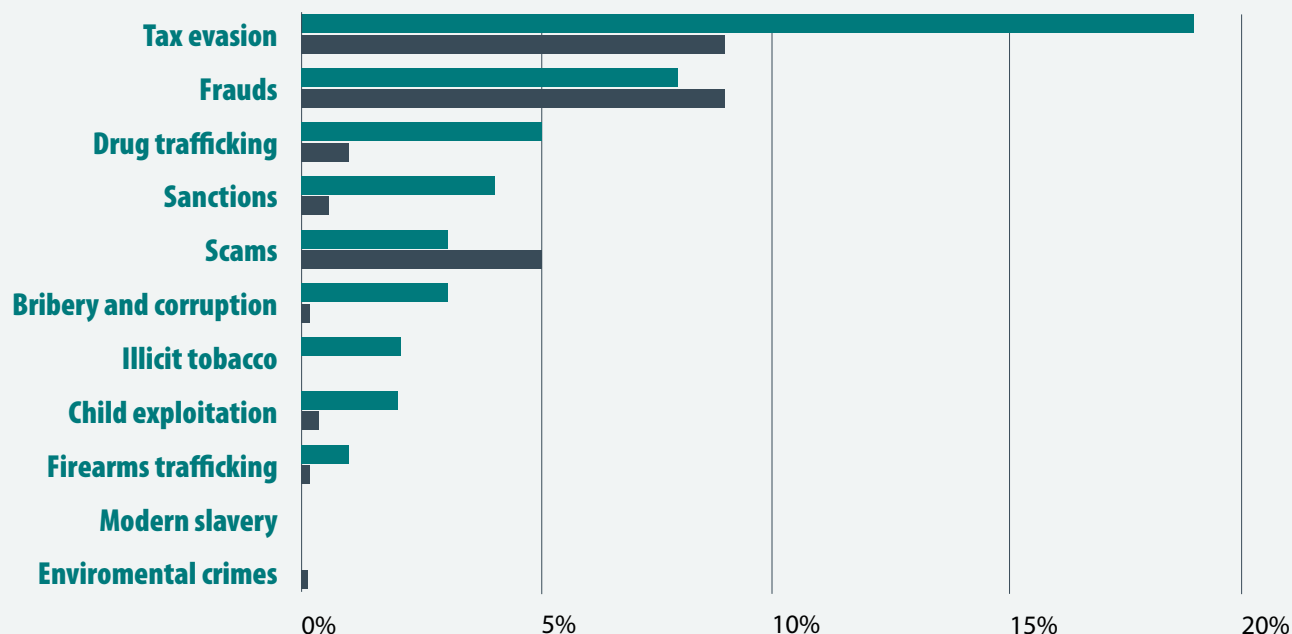
## PREDICATE OFFENCES

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

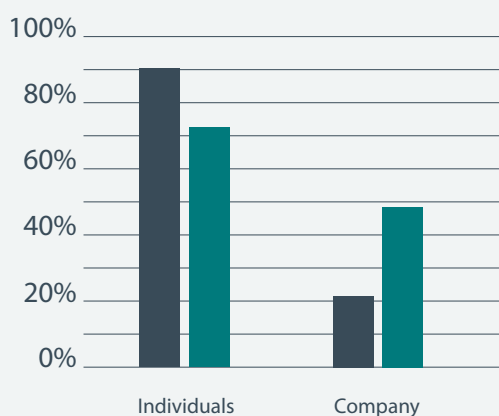
This assessment is based on consultations with partner agencies, and findings from the SMR sample and IR review.

Major banks were the most commonly misused banking subsector in intelligence reports where a predicate offence was identified.

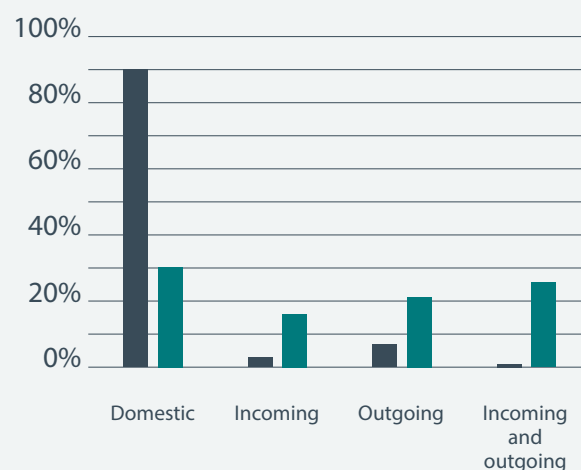
Key predicate offences include tax evasion, drug trafficking, frauds and scams. To a lesser extent, the subsector is also exposed to high-impact offences, particularly sanctions violations, bribery and corruption, child exploitation, firearms trafficking, modern slavery and environmental crimes.



### PREDICATE REPORTS: CUSTOMER TYPE



### PREDICATE REPORTS: DIRECTION OF FUNDS



■ SMR sample ■ IR review

## IDENTIFYING PREDICATE OFFENCES – A CHALLENGE FOR REPORTING ENTITIES

The actual extent of predicate offences involving major banks is almost certainly higher than is represented in the SMR sample (24 per cent). One-third of all SMRs reviewed did not identify a discernible criminal offence – these were largely submitted because of suspicious transactional activity. Similarly, nearly half of all money laundering-related SMRs did not identify a predicate offence.

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

### TAX EVASION

Tax evasion was the most common predicate offence impacting major banks identified in the IR review (19 per cent) and the second most common in the SMR sample (nine per cent). Of all tax evasion-related intelligence reports analysed, major banks were identified in almost three-quarters (73 per cent). This is likely to be driven by the subsector's exposure to cash transactions and its large number of corporate customers – some of which operate across borders.

### Corporate tax evasion

Corporate tax evasion appeared in roughly half of all tax-related SMRs. The extent of suspected corporate tax evasion is largely comparable with other tax evasion-related offences. However, the average SMR value in instances of corporate tax evasion was nearly double that of other tax evasion activities. Therefore the associated harm of corporate tax evasion through the subsector is likely higher.

Methodologies 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 corporate tax evasion indicators included:

- transactions involving foreign jurisdictions, particularly known tax secrecy jurisdictions and global financial centres<sup>29</sup>
- phoenixing<sup>30</sup>
- the use of complex corporate or legal structures to place, layer and conceal wealth
- the use of professional facilitators in Australia and overseas.

29 This report considers the following jurisdictions as global financial centres: Hong Kong SAR, Singapore, UK and USA. This is in line with the Global Financial Centres Index 26, Z/Yen and China Development Institute, 2019, [longfinance.net/media/documents/GFCI\\_26\\_Report\\_2019.09.19\\_v1.4.pdf](https://longfinance.net/media/documents/GFCI_26_Report_2019.09.19_v1.4.pdf).

30 For in-depth information of illegal phoenix activity, including financial indicators, see Fintel Alliance's illegal phoenix activity indicators: [austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/illegal-phoenix-activity-indicators-report](https://austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/illegal-phoenix-activity-indicators-report).

## HOW A GLOBAL NETWORK OF COMPANIES USING BACK-TO-BACK LOAN ARRANGEMENTS CAN EVADE TAX

An Australian company (Company A) was reported by a major bank for making a series of international transactions to an account in a global financial centre. This account was ultimately owned by a company domiciled in a tax secrecy jurisdiction (Company X).

AUSTRAC analysis identified financial transactions from Company A and two related Australian companies (Company B and Company C) which indicated they were exploiting a back-to-back loan scheme to evade corporate tax. In this scheme, the Australian companies would receive a transfer from Company X characterised as a 'loan'. Companies A, B and C were ultimately observed transferring funds to Company X to repay the 'loan' with income earned in Australia, thereby reducing their taxable income and likely evading Australian corporate tax. Between 2016 and 2018, Companies A, B and C sent more than \$95 million offshore to Company X.

Notably Companies A, B and C were part of complex offshore company structures – Companies A and B are owned by the same offshore company and Company C is owned by another company which is registered at the same address. The three companies also shared two directors – one of whom was observed making a \$9 million cash deposit into the account of Company A. While unconfirmed, it is hypothesised that the three companies share beneficial owners.

## Personal tax evasion

Cash transactions appeared in the overwhelming majority of SMRs submitted on suspicion of personal tax evasion (91 per cent). Approximately two-thirds of these reports identified suspicious cash deposits, which were often structured, while just over one-third featured suspicious withdrawals. A small proportion of cash-related personal tax evasion SMRs identified both deposits and withdrawals (10 per cent). This cash activity generally represented relatively simple tax evasion methodologies.

However, more complex tax evasion methodologies were also present. These generally involved:

- international transactions, often to or from tax secrecy jurisdictions
- transactions between multiple domestic accounts, often held with other reporting entities
- the use of a DNFBP, third party or other agent
- transfers to or from business accounts in an attempt to obfuscate the source or destination of funds.

## DRUG TRAFFICKING

Drug trafficking was identified in five per cent of the IR review and one per cent of the SMR sample. However, major banks were identified in almost one-third of all drug trafficking-related intelligence reports analysed. Most partner agencies consulted for this report ranked drug trafficking as the top predicate offence facing the subsector.

While relatively few SMRs directly link major banks to drug trafficking proceeds, the actual value of drug proceeds laundered through the subsector is likely significant. 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.<sup>31</sup> AUSTRAC assesses a sizeable portion of these funds are laundered through the banking system.

31 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).

Given the scale of major banks, it is likely these funds will enter the subsector at either placement, layering or integration. This finding is supported by partner agency intelligence, which suggests money laundering organisations and drug trafficking organisations exploit major banks to launder drug proceeds.

The data-matching exercise identified approximately \$138 million in transactions through major 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 a major bank. 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 major banks with a direct link to drug activity. SMRs that had a direct link to drug activity were usually 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 43 per cent of SMRs that identified money laundering as the only threat are linked to drug proceeds.

## ILLICIT TOBACCO

Illicit tobacco trade was identified as a threat in two per cent of the IR review and less than one per cent of SMRs submitted by major banks.

In July 2018, the Commonwealth established the Illicit Tobacco Taskforce led by the Australian Border Force to combat serious organised crime syndicates that deal in illicit tobacco. Since then, the taskforce has seized in excess of 262 tonnes of smuggled tobacco, with an estimated excise value of \$270 million.<sup>32</sup>

Some transnational, serious and organised crime groups are involved in the importation of illicit tobacco, and some operate exclusively in this area as it is perceived as lower risk than drug importation. Less established criminals are also involved in illicit tobacco as a means to raise funds to finance more lucrative drug importations.

Since 2019, major banks have developed an understanding of the illicit tobacco trade through collaboration with law enforcement investigations. While this has resulted in additional high-quality SMRs, identifying tobacco-related transactions without external intelligence is still a challenge. For this reason, proactively generated SMRs on illicit tobacco almost always relate to entities and businesses at least nominally involved in the legitimate tobacco trade.

Common financial indicators of illicit tobacco activity include:

- large or frequent cash deposits into a tobacconist's account or the accounts of individuals linked to a tobacconist business
- outgoing international transactions to pay for illicit tobacco, often conducted via third parties
- international transactions by a tobacconist or individuals linked to a tobacconist sent without apparent business reasons
- transactions with key source countries for illicit tobacco, such as China, Indonesia and the UAE, particularly where there appears to be no link with other business activity.

32 ATO, *Illicit Tobacco Taskforce detects more than 262 tonnes of tobacco*, 14 October 2019. Viewed: 9 November 2020, [ato.gov.au/Media-centre/Media-releases/Illicit-Tobacco-Taskforce-detects-more-than-262-tonnes-of-tobacco/](https://ato.gov.au/Media-centre/Media-releases/Illicit-Tobacco-Taskforce-detects-more-than-262-tonnes-of-tobacco/).

## FRAUDS

Frauds were the second most common predicate offence identified in intelligence reporting (eight per cent) and equal most common in SMRs submitted by the subsector (nine per cent). Overall, 55 per cent of all fraud-related intelligence reports analysed involved a major bank.

AUSTRAC notes the extent of fraud activities in the subsector is probably under-represented in the SMR sample. Compared to other banking subsectors, the proportion of SMRs submitted by major banks relating to fraud is significantly lower. This is likely because major banks:

- may have a higher threshold of reporting suspected fraudulent activity – e.g. SMRs may not be submitted on high-frequency, low-impact frauds like card-not-present fraud.
- facilitate more cash transactions than other subsectors. These transactions are more likely to be subject to an SMR. Therefore, the proportion of fraud SMRs may be lower.
- have more sophisticated transaction monitoring systems that identify more types of ML/TF activity, and therefore the proportion of fraud SMRs may be lower.

While most cases of fraud were relatively simple in nature, a small number were more sophisticated and had potentially significant consequences. Identity fraud was most commonly reported, followed by loan application fraud and cheque fraud. The exact nature of a number of fraud SMRs was sometimes difficult to determine or did not fit a pre-determined category used during the SMR labelling exercise undertaken by AUSTRAC for this report. 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.

Major banks are exposed to identity crime through their online product delivery arrangements. Common themes of identity fraud-related SMRs include:

- the use of stolen identity documents to establish a banking profile and open new

accounts – criminals then use these accounts for money mule purposes

- the use of stolen identity documents to gain access to existing bank accounts followed by theft of funds
- cyber-enabled activity, particularly relating to fraudulent account openings and loan and credit card applications
- use of the same personal details such as mobile numbers, email addresses or IP addresses to open multiple fraudulent accounts, sometimes over long periods of time
- providing an address linked to a vacant property
- use of specific email domains that have fewer security features.

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

## REPORTED CASES OF FRAUD ENABLED BY MORTGAGE BROKERS

In one instance, a syndicate of lending managers and mortgage brokers was suspected of altering information provided by home loan applicants across the banking sector. This resulted in hundreds of fraudulent loans, most of which were held with major banks.

In another instance, partner agencies identified a large-scale loan application fraud operation that was enabled by a number of mortgage brokers. This operation involved high-level document forgery and was believed to be orchestrated by a serious and organised crime group.

During consultations, another partner agency told AUSTRAC that it had identified a number of mortgage brokers helping known criminals obtain home loans. The brokers knowingly allowed the loans to be repaid with illicit funds. In some instances, brokers even deposited illicit cash for these customers.



## SCAMS

Scams were identified in three per cent of the IR review and five per cent of the SMR sample; however, 60 per cent of scam-related intelligence reports analysed involved a major bank. While many typologies were reported, the most common was phishing or remote access scams.<sup>33,34</sup> Common themes from SMRs that identified this typology included:

- stolen funds sent to a third-party account, generally at another domestic financial institution
- the exploitation of transaction accounts
- the use of public domain email addresses or malware
- cash withdrawals, often immediately following the receipt of scam funds.

While some remote access scams resulted in financial losses for the customer, other attempts were identified and prevented by AML/CTF systems and controls.

Romance scams were also prominent in the SMR sample.<sup>35</sup> Common themes included:

- outgoing international funds transfers, usually to higher-risk jurisdictions including global financial centres
- transaction accounts were the most common product identified and were often exploited for money mule purposes.

While major banks often advised their customer that they were being targeted in a romance scam, the advice was often ignored. In some instances, customers responded by trying to obscure their transactions from the bank by withdrawing funds in cash or transferring funds to other external accounts – behaviour that raised further red flags for reporting entities.

Although customers of major banks were usually victims of scams, in some instances transaction accounts were used to facilitate a scam or launder scam proceeds.

**i AUSTRAC acknowledges that fraud and scam threats are continually evolving. Major banks should remain vigilant of 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 scam-related activity in SMRs.

33 Phishing involves scammers contacting victims and pretending to be from a legitimate business – such as a bank – in an attempt to obtain personal information. The information is then used to fraudulently gain access to a banking product, commonly a transaction account or credit card.

34 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.

35 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.

## **PROTECTING VULNERABLE AUSTRALIANS THROUGH FINTEL ALLIANCE**

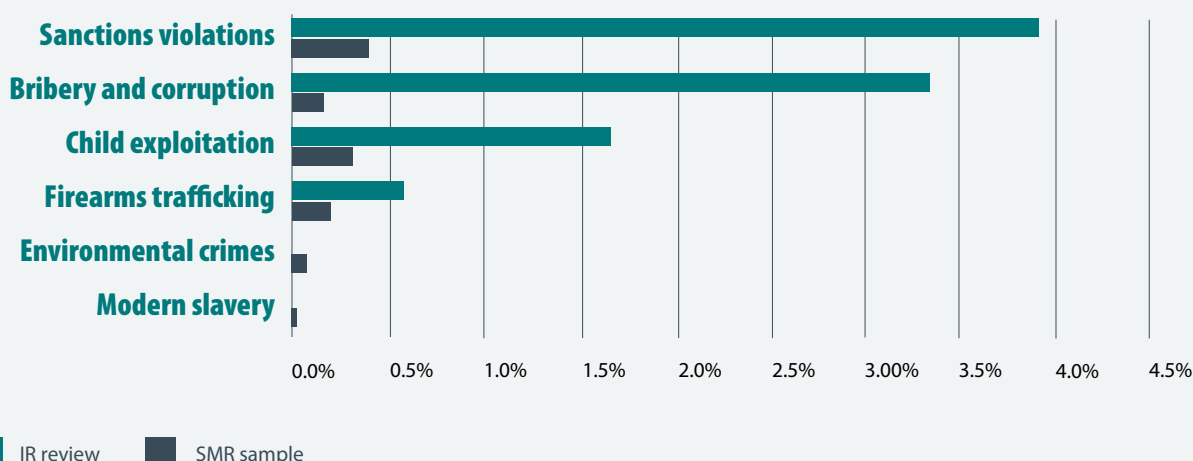
In early 2019, the Fintel Alliance established a scams working group to share information on emerging and complex scams to disrupt this crime. Through the working group, Fintel Alliance banking partners worked closely with the New South Wales Police Force to investigate a criminal syndicate targeting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

## OTHER HIGH-IMPACT PREDICATE OFFENCES

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



**i** Despite low levels of suspected or detected instances of misuse, 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.

### SANCTIONS VIOLATIONS

Suspected or attempted sanctions violations were identified in four per cent of the IR review and less than one per cent of the SMR sample. However, major banks were identified in two-thirds of all sanctions-related intelligence reports analysed. This is unsurprising given sanctions violations generally involve transactions with foreign entities, and major banks process roughly two-thirds of Australia's international transactions by value.

Common themes in sanctions-related SMRs and intelligence reports include:

- transactions with a proscribed or sanctioned entity, their family members or associates
- transactions with at least one higher-risk jurisdiction
- the use of offshore companies or other legal structures
- companies often operating in higher-risk industries, particularly natural resources and electronics.

Major banks generally blocked instances of attempted transactions with known sanctioned entities. However, AUSTRAC intelligence also identified a small number of instances where the subsector was exploited by associates, intermediaries or agents of sanctioned entities.

While the overall number of suspected or attempted sanctions violations was low relative to other predicate offences, the potential consequences to national and international security, and the reputation of Australia's financial system, are very high.

### **BRIBERY AND CORRUPTION**

Suspected bribery and corruption was identified in three per cent of the IR review and less than one per cent of the SMR sample. However, major banks were identified in over two-thirds of bribery and corruption-related intelligence reports analysed for this risk assessment. Most of these intelligence reports related to transactions with links to suspected offshore corruption, all of which involved higher-risk jurisdictions. Foreign PEPs were commonly identified in relation to these transactions and, in some instances, were observed exploiting bank accounts held by family members.

Despite relatively low levels of detection to date, major banks are widely exposed to bribery and corruption threats because they sit at the centre of Australia's financial services industry and are highly exposed to foreign jurisdiction risk. 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.<sup>36,37</sup>

### **CHILD EXPLOITATION**

Child exploitation was identified in approximately two per cent of the IR review and less than one per cent of the SMR sample. Although the volume of suspicious transactions was relatively low, the harm inflicted by child exploitation is very high. Intelligence from AUSTRAC and partner agencies confirms that major banks are used to facilitate payments for access to child exploitation material, as well as to facilitate 'grooming' and child sex tourism.

While major banks submit more child exploitation-related SMRs than any other financial sector,<sup>38</sup> this is unlikely to be an accurate representation of the actual level of threat. Rather, the high proportion of reporting by major banks likely reflects a greater awareness and proactive targeting efforts by the subsector in recent years – particularly through Fintel Alliance operations.

There has been a 945 per cent increase in reporting of suspected child-related offending since the establishment of Fintel Alliance. Actionable financial intelligence developed under a Fintel Alliance-led project has directly led to the arrest of individuals in Australia and the rescue of children from harm overseas. A number of targets identified through the project remain under active investigation by law enforcement agencies in Australia and overseas.

Partner agency and AUSTRAC investigations demonstrate that offenders often use various reporting entities across the banking and remittance sectors to facilitate offshore payments in an attempt to avoid detection.

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

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

38 Keyword analysis indicates that major banks submitted 78 per cent of all child exploitation-related SMRs in the reporting period.

### 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.

### FIREARMS TRAFFICKING

While the exact value of the illicit firearms market cannot be determined, the ACIC estimates there are approximately 260,000 illicit firearms in Australia.<sup>39</sup> 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.<sup>40</sup> 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.

Reports relating to illicit firearms were uncommon in both the SMR sample and IR review.

Approximately half of SMRs relating to illicit firearms were triggered by references to guns or ammunition in transaction descriptions.

Financial intelligence provided by reporting entities provides AUSTRAC and its partner agencies with the ability to investigate firearms trafficking and mitigate any potential harm.

### ENVIRONMENTAL CRIMES

Environmental crimes incorporate an array of offences, including wildlife trafficking, logging and the dumping of illegal waste. These offences can generate significant illicit profits and attract lower criminal penalties than other crimes, making them appealing to 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.<sup>41</sup>

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.

While major banks' exposure to environmental crimes is almost certainly low relative to other predicate offences, it is likely that a portion of related proceeds will have a nexus to major banks due to the scale of their customer base and extent of product offerings.

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

<sup>39</sup> ACIC, *Illicit firearms in Australia*, 2018, page 7, [acic.gov.au/sites/default/files/2020-08/illicit\\_firearms\\_in\\_australia.pdf](https://www.acic.gov.au/sites/default/files/2020-08/illicit_firearms_in_australia.pdf).

<sup>40</sup> 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/sites/default/files/2020-08/illicit\\_firearms\\_in\\_australia.pdf](https://www.acic.gov.au/sites/default/files/2020-08/illicit_firearms_in_australia.pdf).

<sup>41</sup> 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](https://www.interpol.int/en/News-and-Events/News/2016/UNEP-INTERPOL-report-value-of-environmental-crime-up-26).

## 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.<sup>42</sup> 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.<sup>43</sup>

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.<sup>44</sup> 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.<sup>45</sup>

Financial information provided by reporting entities plays a key role in combating modern slavery. For example, analysis of AUSTRAC data led to the conviction of an individual running a business involving sexual servitude in July 2019. In a separate instance, AUSTRAC intelligence identified a syndicate using a major bank to send more than \$1 million to a jurisdiction of interest over a 12-year period to facilitate human trafficking for the purposes of sexual services.

<sup>42</sup> For more see: [homeaffairs.gov.au/criminal-justice/Pages/modern-slavery.aspx](https://homeaffairs.gov.au/criminal-justice/Pages/modern-slavery.aspx).

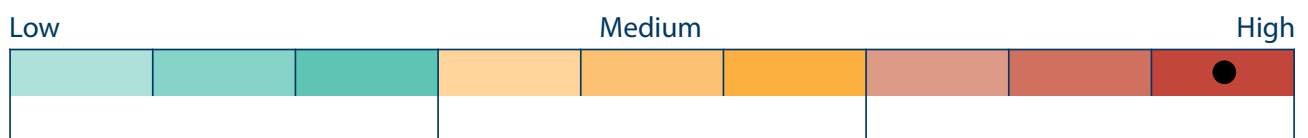
<sup>43</sup> Lyneham S, Dowling C & Bricknell S, *Estimating the dark figure of human trafficking and slavery victimisation in Australia*, Australian Institute of Criminology (AIC), 2019, page 6, [aic.gov.au/publications/sb/sb16](https://aic.gov.au/publications/sb/sb16).

<sup>44</sup> International Labour Organization, *Profits and poverty: The economics of forced labour*, 2014, page 13, [ilo.org/global/publications/ilobookstore/order-online/books/WCMS\\_243391/lang--en/index.htm](https://ilo.org/global/publications/ilobookstore/order-online/books/WCMS_243391/lang--en/index.htm).

<sup>45</sup> 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](https://aph.gov.au/Parliamentary_Business/Committees/Joint/Foreign_Affairs_Defence_and_Trade/ModernSlavery/Final_report).



# 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 major 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 major banks' customer base presents a **high** level of inherent ML/TF vulnerability.

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

### SIZE OF THE CUSTOMER BASE

Australia's major banks comprise the largest financial industry in the country. Combined, they provide services to approximately 47 million customers, and hold \$1.7 trillion in deposits and \$3.4 trillion in assets.<sup>46</sup> The vast size of the customer base increases the subsector's exposure to criminal entities and makes it difficult to proactively detect criminal misuse.

While the customer base is dominated by individuals, major banks service a significant number of non-individual customers including companies, trusts and other legal entities. 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 does not expect the size of the subsector's customer base to change significantly in the coming years. While some customers may exit major banks in favour of other domestic banks due to increased competition facilitated by Open Banking, major banks will likely attract new customers as Australia's population grows.

### HIGHER-RISK CUSTOMERS

Major 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.

The subsector reports having more high-risk customers than all other AUSTRAC reporting entities combined.<sup>47</sup>

AUSTRAC assesses that the subsector also has a high number of higher-risk customer categories, which can include:

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

<sup>46</sup> APRA, *Monthly authorised deposit-taking institution statistics backseries: July 2020*, [apra.gov.au/monthly-authorised-deposit-taking-institution-statistics](https://apra.gov.au/monthly-authorised-deposit-taking-institution-statistics).




<sup>47</sup> This finding refers to customers that each reporting entity assesses as 'high-risk'.

## HIGH-RISK CUSTOMERS IN CONTEXT

The subsector's exposure to high-risk customers and higher-risk customer categories is primarily a result of its very large customer base, which is larger than any other sector regulated by AUSTRAC. This is due to major banks' established market presence, extensive network of physical outlets, wide range of products and services, sophisticated online delivery channels and exposure to foreign jurisdictions. AUSTRAC assesses that, while major banks have the most high-risk customers in absolute terms, their exposure to high-risk customers is generally proportional to the size of their customer base.

### KNOWN OR SUSPECTED CRIMINALS

## LINKS TO KNOWN AND SUSPECTED CRIMINALS: RESULTS OF AUSTRAC DATA-MATCHING

| 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 |
|  | \$\$\$                |  | \$\$\$                |  | \$                    |
| <b>LEGEND</b> \$ = Low      \$\$ = Medium      \$\$\$ = High                        |                       |   |                       |   |                       |

AUSTRAC assesses major banks have a high exposure to known or suspected criminal customers, presenting 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:<sup>48</sup>

- 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 2018<sup>49</sup>
- charged with a terrorism-related offence between 1 January 2014 and 31 December 2018.<sup>50</sup>

SMRs accounted for two-thirds of the value of all reports that matched to these entities, suggesting transaction monitoring systems used by major banks were effective at identifying transactions conducted by known or suspected criminals. Where an international funds transfer was matched to these individuals, the most common source or destination jurisdictions were Hong Kong Special Administrative Region of the People's Republic of China (Hong Kong SAR), USA, New Zealand, UK and Thailand. While the proportion of known or suspected criminals that are customers of major banks is high, the overall number of these entities is low relative to the size of the subsector's customer base. Despite this, these customers present a very high ML/TF risk to the subsector.

<sup>48</sup> This analysis was completed on IFTIs, TTRs and SMRs submitted by major 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).

<sup>49</sup> 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).

<sup>50</sup> 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).

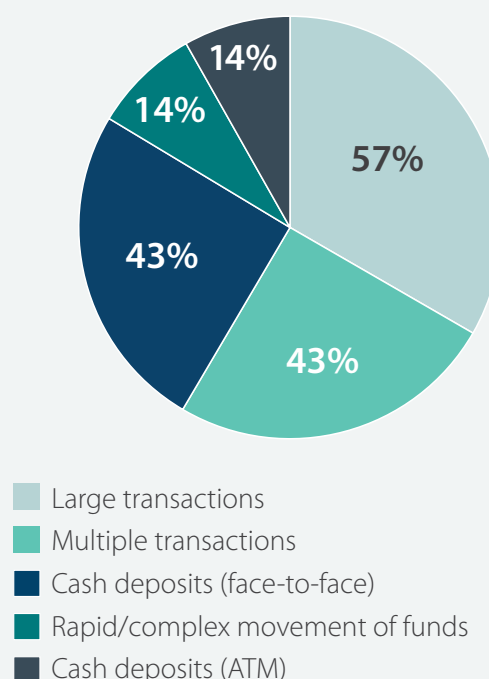
### POLITICALLY EXPOSED PERSONS

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.<sup>51</sup> 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.

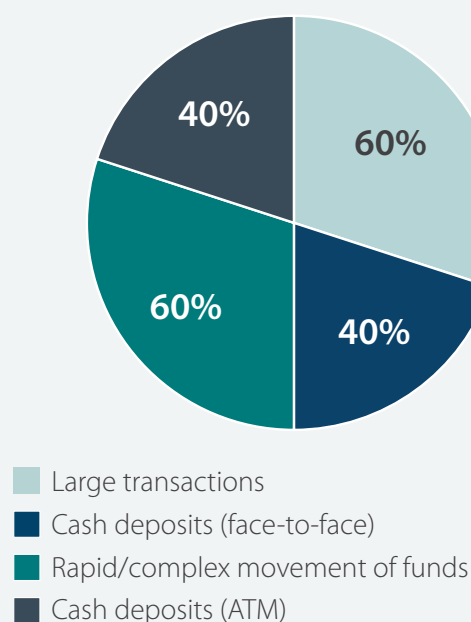
Major banks have a very high overall number of PEP customers, although this is proportionate to the size of the subsector's customer base. PEPs featured in less than one per cent of the SMR sample. Most reports related to foreign PEPs, often with links to a higher-risk jurisdiction. Incoming international funds transfers, cash deposits and large transactions were commonly identified. In known and suspected instances of misuse, partner agencies identified international funds transfers into accounts held by family members of PEPs. These funds were often used to purchase real estate or fund gambling activity.

While the number of PEP customers is generally proportionate to the subsector's customer base, AUSTRAC assesses the overall number of PEP customers will continue to present a high ML/TF risk to major banks.

### SUSPICIOUS TRANSACTIONS LINKED TO FOREIGN PEPs IN SMR SAMPLE



### SUSPICIOUS TRANSACTIONS LINKED TO DOMESTIC PEPs IN SMR SAMPLE



<sup>51</sup> 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.

Major banks service a large number of companies, trusts and other legal entities.<sup>52</sup> These customers were identified in 15 per cent of the SMR sample, most of which were linked to money laundering or corporate tax evasion activities.

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 (see case study below).<sup>53</sup>

- 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 (see page 23).
- 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.

52 In the first quarter of 2019, just under half of all deposits received by major banks were from non-individuals (APRA Monthly Banking Statistics: March 31, 2019); and data from the latest annual reports of major banks suggests approximately 40 to 50 per cent of revenue is derived from these customers.

53 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.

## EXPLOITATION OF COMPANIES BY KNOWN CRIMINALS

AUSTRAC identified a network of at least 16 companies and six trusts linked to a convicted criminal with links to domestic and transnational serious organised crime. Some entities were directly owned and controlled by the individual (operating under an alias), and the other entities were owned and controlled by the individual's relative. Many of the entities held accounts with multiple major banks.

All companies purported to operate in the property, construction and energy sectors and exhibited signs they were shell companies. In particular, six of the entities were established within a short period and shared an address that corresponded to the office of a DNFBP. Two companies were deregistered very shortly after other companies in the network were registered.

AUSTRAC intelligence identified the network of companies and trusts conducting:

- Hundreds of structured cash withdrawals, often by cheque.
- Layering between entities in the network, as well as between business and personal accounts. In one instance, funds were used to purchase large bank cheques made payable to the known criminal. Funds were then deposited into a personal account and used to fund outgoing international transfers to a higher-risk jurisdiction.
- Large transactions to and from casino accounts, often funded by large bank cheques.
- Large transfers to the trust accounts of multiple legal firms. In one instance, funds were transferred from the trust to third parties – likely in an attempt to obscure the source of funds.
- Large international transfers to foreign jurisdictions considered higher risk for money laundering.

**i** 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 by law enforcement and financial regulators as potentially attractive to 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.

Major banks are widely exposed to DNFBPs – in particular accountants, real estate agents and lawyers – because they offer specific products such as statutory trust accounts to these professions. Across the entire reporting population, major banks submitted 95 per cent of TTRs and 90 per cent of SMRs where an accountant, real estate agent or lawyer was referenced.

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.

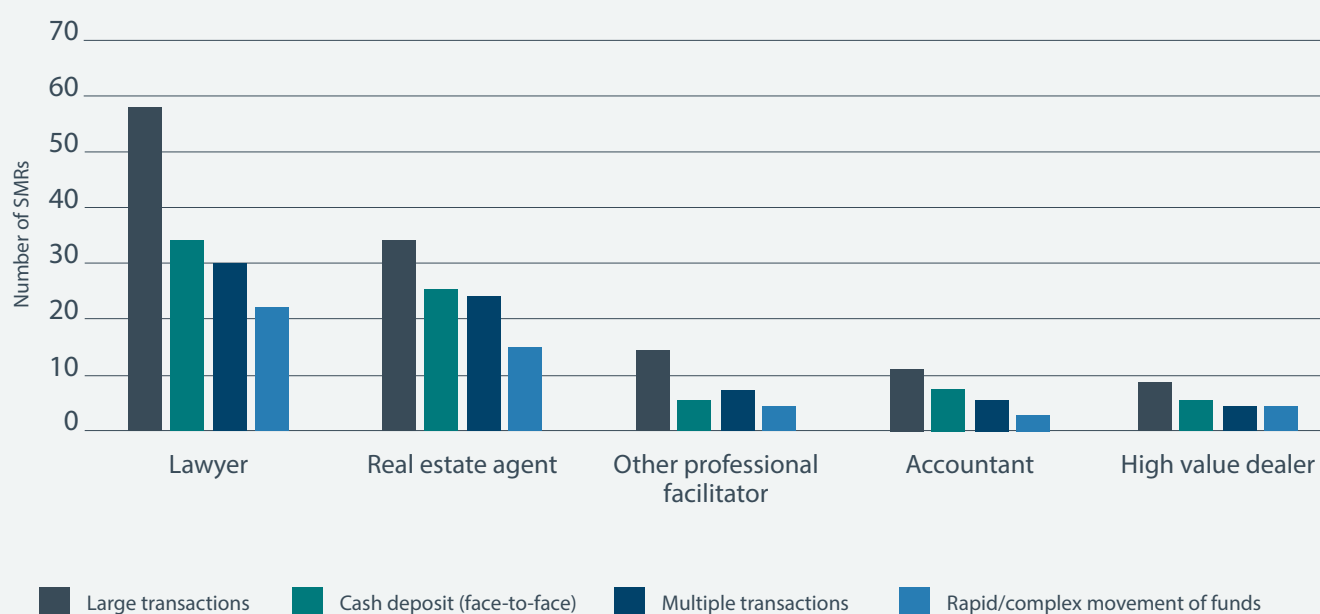
Real estate agents are also exploited by criminals, particularly in the layering and integration phases of money laundering. Criminals might seek to purchase real estate with large amounts of cash, which may

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 a small number of high-risk DNFBPs will present ongoing ML/TF risks to major banks. This assessment is based on the SMR sample, and partner agency information, which confirms DNFBPs are often identified in criminal investigations involving misuse of the subsector. In the reporting period, two per cent of SMRs involved a DNFBP. Common themes included:

- suspected money laundering activity
- large transactions
- incoming international funds transfers
- cash transactions.

### SUSPICIOUS TRANSACTIONS LINKED TO DNFBPs IN SMR SAMPLE



## 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 entities seeking to disguise their criminal activity, including 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 major banks to facilitate tax evasion and the movement of funds internationally. AUSTRAC expects major banks to report any suspicions of professional facilitators or enabling parties to illicit activity, and encourages mature risk mitigation strategies for limiting insider threats.

**i AUSTRAC encourages major banks to remain aware of enduring ML/TF risks posed by DNFBPs and continue reporting detailed SMRs when a suspicion is formed.**

## TEMPORARY VISA HOLDERS

AUSTRAC assesses a small number of visitor visa holders who become customers of major banks present a high ML/TF risk. Partner agencies report known and suspected instances of criminal exploitation by visitor visa holders. Some examples include:

- An onshore criminal entity used a network of fly-in fly-out money mules on visitor visas to launder more than \$2 million of proceeds from investment scams. The visitor visa holders registered companies and opened multiple bank accounts, which were used to receive scam proceeds via domestic transfers from Australian victims. Control of the accounts was then turned over to the onshore controller, who sent funds overseas or withdrew it as cash.
- A network of visitor visa holders were appointed as directors of separate shell companies and then opened personal and business bank accounts with two major banks. These accounts were used to acquire EFTPOS machines used to perpetrate a credit card fraud scheme. Subsequently five visitor visa holders were convicted of money laundering.
- An individual arrived in Australia on a visitor visa and opened a transaction account with a major bank. Soon after, they began making large cash deposits. Within a one-month period, they deposited \$780,000 and then transferred these funds to multiple third parties. After making a final deposit, the individual left the country the next day. Most of the funds were ultimately used by a third party to fund bank cheques to purchase real estate.
- An individual overstayed their visitor visa but continued to make transactions in person at a major bank. They made multiple large cash withdrawals worth \$3.8 million from their transaction account in the name of their Australian-registered company. The funds came from multiple transfers from accounts linked to other Australian companies controlled by the individual.

At least two per cent of the SMR sample involved a customer who held a visitor visa.<sup>54</sup> Most reports were submitted on suspicion of money laundering, with half involving suspicious cash deposits and more than 20 per cent involving cash deposits followed by outgoing domestic transfers.

Indicators of suspicious activity by visitor visa holders include:

- establishing a banking profile shortly after arriving in Australia
- 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.

#### STUDENT VISA HOLDERS

AUSTRAC assesses a small number of student visa holders who become customers of major banks present a high ML/TF risk. While not isolated to major banks, partner agencies report known and suspected instances of criminal exploitation by these individuals. Approximately two per cent of the SMR sample identified at least one student visa holder.<sup>55</sup>

Common money laundering methodologies associated with student visa holders include:

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

#### MITIGATING EXPLOITATION BY TEMPORARY VISA HOLDERS

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 visitor visa.

Representatives from a non-major bank told AUSTRAC their company policy requires staff to be satisfied that an individual has a significant connection to Australia before being onboarded. Subsequent customer due diligence (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 mandated enhanced customer due diligence (ECDD) be conducted if an individual held what this reporting entity considered a high-risk visa.

<sup>54</sup> This information only reflects instances where visa information has been included in an SMR, and AUSTRAC is aware of situations where this has not been the case. For example, a known visitor visa holder was subject to eight SMRs in a seven-month period but no visa information was included. Therefore, the true extent of suspicious transactions conducted by individuals on short-term visas is unknown.

<sup>55</sup> *ibid.*

**HIGH NET-WORTH INDIVIDUALS**

High net-worth individuals can pose a higher ML/TF risk to major banks, particularly through their private banking or wealth management operations. This is because the provision of personalised and complex financial advice to high net-worth individuals, including the delivery of bespoke financial products, can obscure beneficial ownership. Factors that increase ML/TF vulnerabilities associated with high net-worth individuals include:

- very high-value transactions
- the use of complex banking products and services and interactions with other financial sectors, such as securities and derivatives
- a lack of transparency around the source of funds
- the use of complex legal structures that obscure beneficial ownership
- a higher exposure to foreign jurisdiction risk, including:
  - accounts for non-residents located in jurisdictions with weak AML/CTF regimes
  - the use of private investment companies (or shell companies) established in secrecy jurisdictions
- accounts with third-party power of attorney operation, including the involvement of asset managers, accountants or lawyers acting on behalf of clients.

**i** While AUSTRAC acknowledges some major banks have plans to demerge or otherwise restructure their wealth management businesses, the subsector should ensure it maintains the integrity and high standards of business practices within these units. For example, reporting entities should put in place measures to ensure the pressure for private

**bankers to attract and retain clients is not at the expense of complying with their AML program, and does not create a permissible environment for criminal exploitation.**

**FINANCIAL INSTITUTIONS**

While limited in number, financial institution customers may pose a higher ML/TF vulnerability to major banks.<sup>56</sup> This is because financial institutions have many hundreds or thousands of customers of their own (underlying customers). This means providing services to a single financial institution exposes a major bank to many underlying customers. Major 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 major banks to a high volume of cash transactions, particularly if they allow their underlying customers to make deposits into an account held by a major bank.

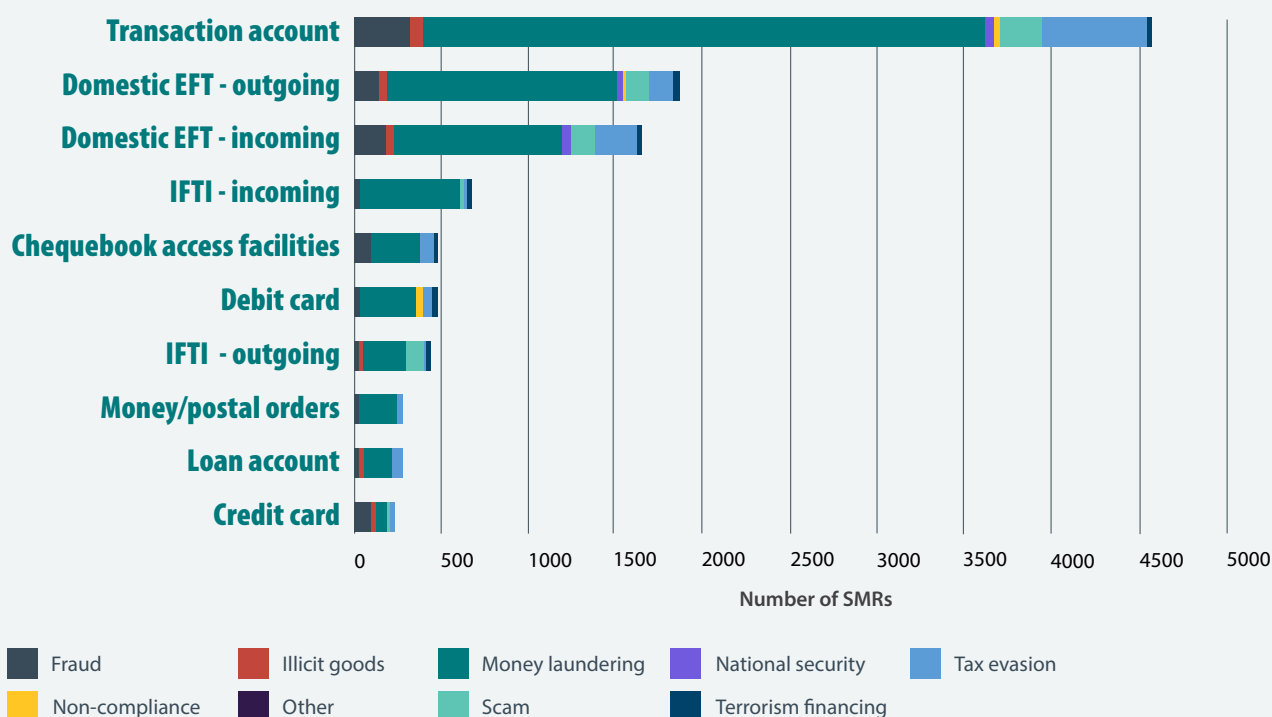
Risks posed by a financial institution customer highly depend on factors such as the types of products or services it offers, the composition of its customer base and the jurisdictions it operates in.

Major banks also count some offshore financial institutions as customers by providing them with correspondent banking services, which is discussed further on page 56.

<sup>56</sup> Please refer to the **Glossary** in **Appendix A** for a definition of 'financial institutions'.

## 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 major banks pose a **high** inherent ML/TF vulnerability.

Major banks have a very high exposure to cash transactions – due in part to their extensive cash deposit and withdrawal infrastructure. While dealing with cash transactions is an inherent part of banking operations, it also increases the industry's exposure to the proceeds of crime, which are often derived in cash making them very difficult to trace. 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.

Major banks also offer a large number of products and services that can be used to store and move illicit funds in and out of the subsector. Products most vulnerable to ML/TF include transaction accounts, credit cards, bank cheques, trust accounts and correspondent banking relationships.

## USE OF CASH

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

- Total number of TTRs submitted to AUSTRAC: **2,293,919**
- Total cash value of TTRs: **\$42.9 billion**
- Largest cash deposit: **\$2,575,990**
- Largest cash withdrawal: **\$2,200,000**
- Total number of cash-related SMRs: **103,337**
- Total value of cash-related SMRs: **\$6.2 billion**
- **59%** of the SMR sample identified at least one suspicious cash transaction.
- **86%** of the IR review identified at least one suspicious cash transaction.

Major banks have the most extensive cash transaction facilities in Australia and are therefore exposed to a very high volume of cash. These serve a critical function in the national economy, providing convenience and access to the financial system for various segments of the Australian community – particularly businesses, the elderly and culturally or linguistically diverse communities.

Criminals are also attracted to banking infrastructure that facilitate cash transactions. While 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.

In the reporting period, major banks submitted approximately 2.3 million TTRs with a cash value of \$42.9 billion. This accounts for more than two-thirds of all TTRs submitted to AUSTRAC during the reporting period.<sup>57</sup> While the size of this figure is largely attributable to the very large size of the subsector's customer base, major banks also process three times the value of cash transactions per customer (\$913) compared to all other Australian ADIs (\$378).<sup>58</sup> This is likely because the subsector services many larger corporate customers, which tend to conduct higher-value transactions.

The subsector's very high exposure to cash can also be attributed to its network of 3,400 branches and 8,900 ATMs and extensive network of business express deposit facilities – which make it easier to deposit and withdraw cash.<sup>59</sup> Since 2012, major banks have replaced more than half of regular ATMs with IDMs. As well as providing standard ATM functions, IDMs also accept cash deposits and credit a customer's account in real-time, further increasing the convenience of transacting in cash (IDMs are discussed further on page 59).

Suspicious cash transactions were identified in 59 per cent of the SMR sample. Key themes include:

- three-quarters involved cash deposits
- a quarter identified structured deposits – face-to-face deposits (75 per cent) were more common than ATM deposits (58 per cent)
- 22 per cent included a cash deposit followed by layering activity
- 10 per cent involved at least one international funds transfer. The top five jurisdictions were China, Hong Kong SAR, Malaysia, Vietnam and the USA.

<sup>57</sup> This figure only includes transactions of \$10,000 and above; the real value of cash transactions processed by major banks is far greater.

<sup>58</sup> This was determined by analysing the total cash amount of TTRs submitted by each subsector as a proportion of its customer numbers.

<sup>59</sup> *Authorised deposit-taking institutions points of presence June 2019*, APRA.



## PUSH AND PULL FACTORS ON CASH USE

As electronic payments become more popular, cash use is in steady decline in Australia.<sup>60</sup> 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 major bank SMRs containing a suspicious cash transaction have also declined, from 83 per cent in 2013-14 to 59 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".<sup>61</sup> Overall, the Reserve Bank noted a "substantial increase in high-value cash withdrawals at branches" in the first half of 2020.<sup>62</sup>

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

## 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, major banks offer thousands of products and services. The subsector's highly extensive and diverse 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
- credit card accounts
- bank cheques
- trust accounts
- correspondent banking services.

Known cases of criminal misuse of trade finance facilities and investment products in the subsector are low. However, some reporting entities and industry representatives note these products are highly vulnerable to ML/TF, and the potential impacts from criminal misuse can be significant given the often large associated values. These products are not discussed in-depth below, as they did not rate 'high' on the Product Risk Matrix. However, reporting entities who offer these services should apply appropriate enhanced customer and transaction due diligence and post-transaction monitoring processes to detect suspicious or unusual activity.

Indicators of TBML and trade finance-based money laundering are discussed on page 24. Reporting entities can also review [AUSTRAC's ML/TF risk assessment of Australia's securities and derivatives sector](#). This report provides an in-depth analysis of ML/TF vulnerability associated with these investment products.

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

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

62 L Delaney, N McClure and R Finlay, *Cash Use in Australia: Results from the 2019 Consumer Payments Survey*, Reserve Bank of Australia, 2020, [rba.gov.au/publications/bulletin/2020/jun/pdf/cash-use-in-australia-results-from-the-2019-consumer-payments-survey.pdf](https://rba.gov.au/publications/bulletin/2020/jun/pdf/cash-use-in-australia-results-from-the-2019-consumer-payments-survey.pdf).

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

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

**i** 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 major bank 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 major 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 major banks.

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

Further discussion is then provided on product and service categories that received an overall rating of 'high' only.

Discussion is not provided on products or service categories that received an overall rating of 'medium' or 'low'.

## PRODUCT AND SERVICE VULNERABILITY RATINGS

| PRODUCT/SERVICE                    | VULNERABILITY PERCEPTION RATING | DETECTED EXPLOITATION | VALUE OF MEDIAN TRANSACTION | TRANSACTION VOLUME | OVERALL RATING |
|------------------------------------|---------------------------------|-----------------------|-----------------------------|--------------------|----------------|
| Transaction accounts               |                                 | High                  | \$                          | Extreme            |                |
| Credit card accounts               |                                 | High                  | \$                          | Very High          |                |
| Bank cheques                       |                                 | High                  | \$ \$                       | Medium             |                |
| Trust accounts                     |                                 | High                  | \$                          | Medium             |                |
| Correspondent banking (Vostro)     |                                 | High                  | \$ \$                       | Medium             |                |
| Savings accounts                   |                                 | Low                   | \$                          | High               |                |
| Home loans                         |                                 | High                  | \$                          | Medium             |                |
| Business loans                     |                                 | Medium                | \$ \$ \$                    | Low                |                |
| Stored value cards                 |                                 | High                  | \$                          | Medium             |                |
| Merchant services                  |                                 | Low                   | \$                          | Extreme            |                |
| Trade finance                      |                                 | Medium                | \$ \$ \$                    | Low                |                |
| Super and approved deposit funds   |                                 | Medium                | \$ \$                       | Low                |                |
| Institutional lending              |                                 | Low                   | \$ \$ \$                    | Low                |                |
| Personal loans                     |                                 | Medium                | \$                          | Medium             |                |
| Investment accounts and services   |                                 | Low                   | \$ \$                       | Low                |                |
| Pensions and annuities             |                                 | Low                   | \$ \$                       | Low                |                |
| Term deposits                      |                                 | Low                   | \$ \$                       | Low                |                |
| Foreign currency exchange services |                                 | Medium                | \$                          | Low                |                |
| Foreign currency accounts          |                                 | Low                   | \$                          | Low                |                |
| Asset financing                    |                                 | Low                   | \$                          | Low                |                |

### TRANSACTION ACCOUNTS

Transaction accounts are by far the most common and versatile products offered by major banks. They are also the most commonly misused product – at least two-thirds of SMRs reviewed identified the exploitation of transaction accounts. These accounts enable fast and effective storage and movement of funds domestically and internationally, exposing the product to foreign jurisdiction risk. Higher risk international funds flows are further discussed in the **Foreign jurisdictions** section on page 65. 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. Extremely 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 major banks – and because their provision poses almost no credit 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 to place or layer criminal proceeds.

### SMR SAMPLE: SUSPICIOUS FINANCIAL ACTIVITY INVOLVING A TRANSACTION ACCOUNT

| TRANSACTION TYPE                                  | % OF SMRs |
|---|-----------|
| Cash deposit                                      | 56        |
| Cash withdrawal                                   | 32        |
| Domestic electronic funds transfer out of account | 22        |
| Domestic electronic funds transfer into account   | 18        |
| International funds transfer into Australia       | 7         |
| International funds transfer out of Australia     | 4         |

### CREDIT CARD ACCOUNTS

Credit card accounts operate much like transaction accounts. They allow for the purchase of goods, withdrawal of cash, acceptance of transfers, including the ability to go into credit and the ability to accept third-party biller payments. In some instances, credit card accounts can be used to transfer funds to connected transaction accounts. These accounts have some additional limitations, such as credit limits, high fees to withdraw cash and limited ability to make outgoing transfers in some instances.

Key ML/TF vulnerabilities associated with credit card accounts include:

- The ability to deposit cash directly into a credit card account. This allows placement of illicit cash, including by third parties. In the SMR sample, more than 40 per cent of reports relating to a credit card account involved a suspicious cash transaction.
- Access to online application and approval with no face-to-face contact. This significantly increases the risk of fraudulent account openings including using stolen identity documents. In the SMR sample, more than 25 per cent of reports relating to suspected identity fraud involved a credit card account.
- Allowing international transactions, including offshore cash withdrawals, which can be funded by onshore third-party cash deposits.

### BANK CHEQUES

Bank cheques allow for the movement of large amounts of funds with a single piece of paper, making them easy to move and conceal. Unlike regular cheques, bank cheques provide the holder with assurance that the cheque will be honoured. Bank cheques are frequently associated with the purchase of property and vehicles, which are common methods for integrating illicit funds.

Industry consultations revealed some reporting entities let non-customers pay for bank cheques in cash. While the customer's details are recorded, ML/TF vulnerability is higher as the source of funds cannot be confirmed.

In recent years, some major banks have also introduced the ability to deposit bank cheques through mobile apps. This feature may be attractive for money launderers as illicit funds can be rapidly placed and layered.

Reporting entities and findings from the IR review suggest bank cheques are vulnerable to ML/TF misuse. Bank cheque-related SMRs were less common (five per cent) but more valuable – the average value of bank cheque-related SMRs was four times larger than the value of the average SMR. When identified, reports often related to suspected money laundering. While the use of bank cheques is declining as customers shift to electronic reconciliation methods, such as PEXA, they will likely remain attractive for criminal misuse.<sup>63</sup>

### TRUST ACCOUNTS

Trust accounts are used by some DNFBPs such as lawyers, accountants and real estate agents, to hold client money under trust for a specific purpose. These professionals offer services sought out 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).

While most transactions involving a trust account are low value, these products also receive very high-value transactions (e.g. for the purchase of real estate).

Reporting entities and partner agencies consider trust accounts highly vulnerable to ML/TF. Although they appeared relatively infrequently in the SMR sample (one per cent) and IR review (one per cent), the average value of trust account-related SMRs was seven times larger than the average SMR value.

### CORRESPONDENT BANKING SERVICES

Correspondent banking is the provision of banking services by one bank (the correspondent bank) to another bank (the respondent bank). Major banks have extensive correspondent banking relationships. Combined they operate approximately 2,000 vostro accounts and 200 nostro accounts (see definitions below).<sup>64</sup>

Correspondent banking is vulnerable to criminal misuse because the reporting entity is reliant upon the effectiveness of the respondent bank's AML/CTF controls because it does not have a direct relationship with the underlying parties to a transaction. The correspondent bank provides services to individuals or entities for which it has neither verified identities nor obtained any firsthand knowledge. Correspondent banks are reliant on the quality of CDD conducted by the respondent bank, and ML/TF risk exposure can increase significantly if a respondent bank has weak AML/CTF controls.

In addition, correspondent banking is designed to enable the movement of funds internationally, therefore exposing reporting entities to foreign jurisdiction risk. Moving funds across borders can also complicate efforts to confirm the legitimacy of funds, the sender's identity and the ultimate beneficiary – factors criminals actively exploit.

Reporting entities, external auditors and partner agencies identified vostro accounts – where a bank holds funds on behalf of a respondent bank – as particularly vulnerable to ML/TF exploitation. Major banks hold the vast majority of vostro accounts in Australia and act as a key conduit for international funds transfers for some other domestic banks. This exposes the subsector to high ML/TF vulnerabilities relating to correspondent banking.

63 PEXA or Property Exchange Australia is a digital platform that enables the settlement of property transactions via electronic means.

64 Based on survey of ADIs conducted by AUSTRAC in 2016.

Additional ML/TF risks posed by correspondent banking services include:

- Nesting – a practice where the respondent bank provides downstream services to another financial institution and processes these transactions through its own correspondent account. This means the correspondent bank is even further removed from knowing the identities or business activity of the actual customer, or even the types of financial services provided.
- Payable-through accounts – in some correspondent relationships, the respondent bank's customers can conduct their own transactions through the respondent bank's correspondent account without first clearing the transaction through the respondent bank. In this scenario, the respondent bank is not provided oversight prior to the transaction and the customer has direct control of funds at the correspondent bank. The AML/CTF Act does not permit the use of payable-through accounts.

### Due diligence relating to correspondent banking

Under the AML/CTF Act, reporting entities have an obligation to conduct due diligence on a respondent bank to ensure adequate AML/CTF controls prior to entering into a correspondent banking relationship with the respondent bank. Reporting entities are not required to conduct due diligence on customers of the respondent bank.<sup>65</sup>

There are two types of accounts associated with correspondent banking:

- nostro account – an account that a bank holds, usually in a foreign currency, in another bank
- vostro account – an account that other banks have with the bank, usually in the the latter bank's domestic currency.

Due diligence requirements apply to vostro accounts only.

These requirements are consistent with the FATF's international standards and international banking practice. Due diligence requirements are outlined in Part 8 of the AML/CTF Act and Chapter 3 of the AML/CTF Rules.

Legislation under the Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Act 2020 strengthen protections on correspondent banking. The new measures prohibit financial institutions from entering into a correspondent banking relationship with another financial institution that permits its accounts to be used by a shell bank, and require banks to conduct due diligence assessments before entering, and during, all correspondent banking relationships. These changes are consistent with international banking practice.

<sup>65</sup> The FATF Recommendations and Australia's AML/CTF framework do not require financial institutions to conduct 'know your customer' checks on customers of the respondent bank.



## DELIVERY CHANNELS

AUSTRAC assesses the delivery channels through which major 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 and ATMs. These channels give criminals anonymity, which can be exploited to perpetrate financial crimes, and make it harder to detect suspicious transactions.

Major banks are also exposed to ML/TF vulnerabilities related to the use of outsourced product delivery arrangements, particularly agent banking arrangements. While the associated ML/TF risks are generally high, customers of major banks are less reliant on these arrangements due to the subsector's extensive branch and ATM networks.

### LEVEL OF CUSTOMER CONTACT

Major banks use the full spectrum of delivery channels to provide their products and services to customers. This includes in-branch, ATMs and other non-face-to-face physical outlets, phone, online and through third-party relationships. Despite maintaining substantial national branch networks, major banks report a sharp 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 thousands 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, major banks have implemented measures to reduce face-to-face contact with customers where possible. For example, major 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. The subsector has also introduced additional guidance to help customers register for online banking for the first time. One major bank reported that a large number of customers that previously used traditional means of banking have moved to using bank cards and online facilities during the pandemic.

It is likely these changes will accelerate the trend away from face-to-face product delivery and towards online banking. One major bank suggested that some of these changes may be sustained over the medium to long-term, driven by customer demand and operational factors.

to replace traditional ATMs with IDMs the number of machines that accept cash deposits has increased over this period. Analysis of SMRs show suspicious cash deposits at ATMs have increased over this period, while suspicious cash deposits in branches have decreased slightly. In response to the changing environment, major banks have tightened limits on the amount of cash that can be deposited and withdrawn at ATMs and continue to review and modify these limits.

ATM transactions were identified in 38 per cent of the SMR sample. Of these reports:

- deposits were most common (73 per cent of ATM-related SMRs)
- suspected money laundering activity was the primary threat (57 per cent)
- personal or corporate income tax evasion were relatively common
- a quarter involved both deposits and withdrawals
- structuring appeared in about one-third of ATM deposit-related SMRs
- most were concentrated in urban or suburban centres.

### ATMs

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. Intelligent deposit machines are a type of ATM that accept cash deposits and have additional features.

Major banks have more than three times as many ATMs than all other ADIs combined, although the number of ATMs has decreased by 14 per cent since 2017.<sup>66</sup> However, as major banks continue

### 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 each major bank now operates extensive national networks of these machines. Since the wide scale rollout of IDMs, major banks report significant growth in cash deposits conducted at ATMs and declining in-branch transactions.<sup>67</sup>

While IDMs provide convenience for both the bank and the customer, they also expose major banks to unique ML/TF vulnerabilities compared to in-branch deposits and their use can make it

<sup>66</sup> Major bank customers can also make withdrawals (but not deposits) from ATMs owned by other ADIs, both domestically and internationally (for more on this see **Agent banking relationships** on page 62).

<sup>67</sup> One major bank reported that less than 10 per cent of transactions occurred in-branch in 2019, down from more than half of transactions 15 years ago.


harder to identify criminal proceeds. For example, IDMs allow cardless cash deposits to be made by third parties, sometimes anonymously (see case study right). 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.<sup>68</sup>

Professional money laundering organisations and other serious organised crime groups exploit the increased anonymity provided by cardless deposits to distance themselves from illicit funds (see page 21 for more details).

### **DRUG PROCEEDS PLACED INTO MAJOR BANKS THROUGH ATMs**

In 2019, AUSTRAC identified suspected drug proceeds being placed into multiple transaction accounts via structured third-party ATM deposits. Some accounts were held by a shell company, while others were held by directors of the shell company. Almost all of the deposits were made by third parties, some of which used cards linked to other major banks, while others used cardless deposits. No information about the suspicious cardless deposits was provided by the reporting entity and the depositors could not be identified.

The funds were subsequently layered through a variety of accounts held by multiple shell companies, as well as used for u-turn international transactions, transferred to online betting accounts and withdrawn via ATMs. The individuals that controlled the drug trafficking network were subsequently observed purchasing high-end real estate, although a direct link between the drug proceeds placed with major banks and the purchase of the real estate could not be made at the time of reporting.

 **AUSTRAC asks reporting entities to provide as much information as possible about the identity of a person conducting suspicious cardless deposits to assist law enforcement investigations.**

<sup>68</sup> The New Payments Platform is discussed on page 63.

### **BUSINESS EXPRESS DEPOSIT BOXES AND NIGHT SAFES**

Business express deposit boxes and night safes (BED facilities) enable large amounts of cash, as well as cheques, to be deposited at any time without face-to-face contact. In the reporting period, they accounted for one-third of all large cash deposits, with a total value of \$9.8 billion.

Several factors make BED facilities highly vulnerable to ML/TF exploitation:

- Some major banks do not require customer registration to use the facilities.
- Generally, there are no processes in place to identify the agent making the deposit, which is 'dropped' into a chute or receptacle and manually processed at a later time.
- While BED facilities are primarily marketed to business customers, some major banks have no controls to prevent individuals using this channel to accept large sums of cash into their personal accounts.
- Most BED facilities are available 24/7.

A 2015 AUSTRAC typology report highlighted the exploitation of BED facilities by serious and organised crime groups, including visitor visa holders.<sup>69</sup> Findings from the IR review indicate that low-level exploitation continues. AUSTRAC assesses the tightening of AML/CTF controls around IDMs will possibly displace illicit activity towards BED facilities.

### **THIRD-PARTY CASH DEPOSITS**

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 or BED facilities. Major banks employ few authentication measures to identify depositors. For example, where reporting entities require mobile numbers, they are often not verified.

During consultations for this assessment, major banks acknowledged the vulnerabilities associated with anonymous cash channels as one of their highest ML/TF risks. The subsector has introduced a range of limits on cash deposits, which are often subject to internal review and modification to mitigate some of these risks.

Despite this, a review of partner agency information and AUSTRAC intelligence confirms that criminal entities continue to exploit the anonymity provided by third-party cash deposits to place illicit funds into major banks.

### **ONLINE BANKING**

The vast majority of transactions facilitated by major banks originate online – either through banking apps or through websites. A large and increasing number of products can also be applied for online. One major bank reports that almost 20 per cent of its products can be applied for online and that the time required to open regular transaction accounts has reduced from days to minutes in recent years.

While this trend is driven by consumer demand for faster, more convenient banking options, the increasingly online nature of bank transactions introduces 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.

<sup>69</sup> AUSTRAC, *Strategic analysis brief: Use of business express deposit boxes to avoid reporting requirements*, 2015, [austrac.gov.au/sites/default/files/2019-06/sa-brief-express-deposit-boxes.pdf](https://austrac.gov.au/sites/default/files/2019-06/sa-brief-express-deposit-boxes.pdf).

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

While major banks have invested significantly in the security of their digital assets, 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. Partner agencies have identified criminals who spend hours testing new versions of mobile apps deployed by major banks to discover and exploit features to perpetrate crimes faster and more anonymously.

**i Reporting entities should carefully consider the financial crime implications of introducing new features into banking apps – even minor updates can be exploited by criminals. One recent example of this was the misuse of a major bank mobile app to collect personal information using the NPP framework via an enumeration attack.**

## COMPLEXITY OF PRODUCT DELIVERY ARRANGEMENTS

Major banks have a relatively low level of outsourcing of product delivery channels. Their large-scale operations allow them to deliver most products and services themselves. Where used, outsourcing arrangements generally allow a major bank's customers to conduct face-to-face cash transactions or ATM withdrawals in locations where the major bank might not have a physical presence, as well as integrating third parties into the product delivery chain.

This creates an 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 RELATIONSHIPS

Each major bank allows their customers to conduct some transactions, such as cash deposits or withdrawals, through the branches or ATMs (withdrawals only) of other major banks. This process is known as agent banking. Most major banks also have agreements with non-ADI agents to facilitate certain types of transactions at non-bank locations, such as a newsagent or post office.

An agent banking arrangement consists of:

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

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

- lengthening the product delivery chain to incorporate a third party between the customer and the major bank, which may create difficulties for transaction monitoring and establishing appropriate governance frameworks to manage ML/TF risks

- limiting the ability for the major bank providing the account to ask questions about large or suspicious activity
- confusion around AUSTRAC reporting obligations, which can lead to missed reports or double reporting<sup>70</sup>
- 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.

### 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'.<sup>71</sup> 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 vulnerabilities to payments and increase the complexity of product delivery arrangements.

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

<sup>70</sup> For AUSTRAC guidance on agent banking arrangements and TTR obligations see: [austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/agent-banking-arrangements-threshold-transaction-report-ttr-obligations](https://austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/agent-banking-arrangements-threshold-transaction-report-ttr-obligations).

<sup>71</sup> 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](https://rba.gov.au/publications/bulletin/2018/sep/the-new-payments-platform-and-fast-settlement-service.html).



## 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 starting with major banks, which have already made available data relating to general retail products such as deposit accounts, credit cards and loan accounts.

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 their major bank. This disaggregation of transactions across multiple financial services providers reduces major 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.

## FOREIGN JURISDICTIONS

AUSTRAC assesses major banks have a **high** inherent ML/TF vulnerability to foreign jurisdiction risk due to substantial and ongoing exposure to foreign jurisdictions.

Major banks sit at the centre of Australia's financial system and act as important correspondents for other financial institutions. The subsector facilitates almost two-thirds of Australia's international transactions by value, and is therefore a key conduit for financial flows into and out of the country.

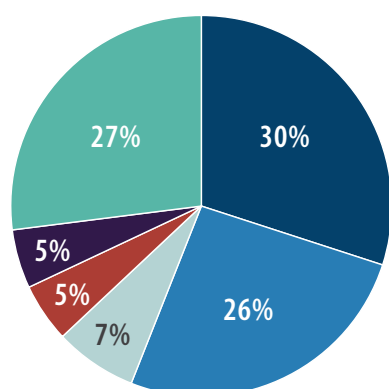
This exposes major banks to foreign jurisdiction risk, including transactions with higher-risk jurisdictions. Exposure to foreign jurisdictions poses ML/TF risk because it creates opportunities for international movement of criminal proceeds and the funding of overseas terrorist activity. Further, transactions 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

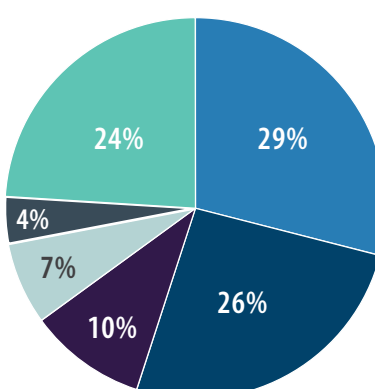
Major banks facilitate 63 per cent of Australia's international transactions by value, submitting 15 million IFTIs in the reporting period worth \$3.5 trillion.<sup>72</sup> These were evenly split between incoming and outgoing transactions.

International transactions were identified in about 20 per cent of the SMR sample and 40 per cent of the IR review. The top five jurisdictions in the SMR sample were China, Hong Kong SAR, Malaysia, USA and the Philippines. Only two of these jurisdictions (Hong Kong SAR and USA) appear in the top five source or destination IFTI jurisdictions. This suggests suspicious activity from China, Malaysia and the Philippines is over-represented relative to the volume of transactions with these jurisdictions. The main threats identified in these SMRs were money laundering, scams and personal income tax evasion.

Incoming IFTIs (\$)



Outgoing IFTIs (\$)



<sup>72</sup> 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

Major banks frequently transact with higher-risk jurisdictions, in particular a very high volume and value of funds flows through global financial centres.<sup>73</sup> In total, 84 per cent of all IFTIs submitted during the reporting period involved a higher-risk jurisdiction.<sup>74</sup> This figure drops to six 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 major 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.<sup>75</sup> 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.

As globally connected banks supporting a globally connected economy, this is reflected in the international transactions facilitated by Australia's major banks. By value, 69 per cent of IFTIs (worth \$2.4 trillion) 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 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 higher 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.

<sup>73</sup> This report considers the following jurisdictions as global financial centres: Hong Kong SAR, Singapore, UK and USA. This is in line with the *Global Financial Centres Index 26*, Z/Yen and China Development Institute, 2019, [longfinance.net/media/documents/GFCI\\_26\\_Report\\_2019.09.19\\_v1.4.pdf](https://longfinance.net/media/documents/GFCI_26_Report_2019.09.19_v1.4.pdf).

<sup>74</sup> 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.

<sup>75</sup> Z/Yen and China Development Institute, *Global Financial Centres Index 26*, 2019, [longfinance.net/media/documents/GFCI\\_26\\_Report\\_2019.09.19\\_v1.4.pdf](https://longfinance.net/media/documents/GFCI_26_Report_2019.09.19_v1.4.pdf).

## 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



49%



51%

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



49%



51%

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



44%



56%

Jurisdictions considered higher risk for tax evasion



58%



42%

Jurisdictions considered higher risk for terrorism financing



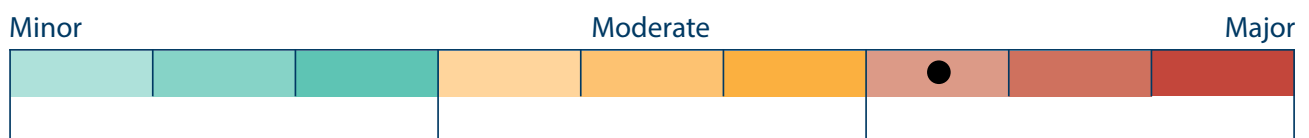
44%



56%

Jurisdictions considered higher risk for child exploitation

# CONSEQUENCES



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



AUSTRAC assesses that the consequences of criminal activity in the major banks subsector are **major**. Consequences include the potential impact or harm that ML/TF and other financial crimes may cause.

Financial crime that impacts major banks has consequences for customers, individual reporting entities, the subsector as a whole, and the broader Australian and international community. The exploitation of major banks to facilitate the financing of terrorism or serious transnational crime has consequences for national and international security.

## CUSTOMERS

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

The impacts of criminal activity on customers of major banks partly depends on the type of criminal activity. For example, reporting entities' guarantee against unauthorised transactions generally covers customers for financial losses stemming from frauds. On the other hand, victims of scams are likely to suffer unrecoverable financial losses.

The type of customer subject to exploitation also affects the scale and consequence of financial losses. Larger, more sophisticated customers such as corporations are better placed to detect and prevent exploitation by criminals or absorb the financial losses that result.

Generally, impacts of criminal activity on major bank 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 major banks has **moderate** consequences for individual reporting entities and the subsector as a whole.

Criminal activity can have a moderate impact on the major banks subsector. While high profile criminal exploitation can result in serious reputational damage for individual reporting entities and the subsector, the scale of major banks means they are well positioned to absorb the financial costs of significant criminal attacks.

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 be accentuated if the banking sector becomes more competitive, including as a result of Open Banking reforms (see **Consumer Data Right - Open Banking** on page 64).

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

Financial costs may include:

- increased costs to improve AML/CTF compliance and mitigation strategies
- financial losses directly related to criminal activity, including customer reimbursements, settlements or civil penalties
- indirect losses, such as reimbursing customers subject to frauds or increased fraud insurance premiums

- increased costs to combat criminal attacks, in particular staff and IT capability costs
- increased costs or allocation of resources to investigate criminal activity or complaints
- loss of earnings as a result of criminal exploitation (i.e. customers taking business elsewhere due to negative experience)
- negative impact on share price
- potential downgrade of business group credit rating and associated increase of funding costs.

Reputational costs may include:

- damage to brand and customer trust following an ML/TF incident that was not appropriately mitigated
- dissatisfaction or loss of investors, customers, partners or debtors
- reduced ability to attract skilled staff
- difficulty continuing or beginning relationships with other financial institutions both domestically and overseas.

Operational impacts may include:

- heightened regulatory oversight or law enforcement action
- increased risk of legal action arising from failed AML/CTF controls
- 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 major banks has **major** consequences for the Australian financial system and the community.

Major banks dominate Australia's financial system – they hold three-quarters of all assets owned by ADIs in the country and APRA has classified them as domestic systemically important banks. Both the prudential regulator and the International Monetary Fund agree that, should any of the four major banks be subject to significant or protracted distress, there would be severe repercussions for Australia's financial system and economy.<sup>76</sup> However, given the size of the major banks and the higher loss absorbency requirements imposed by APRA, the likelihood that criminal exploitation would be serious enough to create significant or protracted distress to these reporting entities is low.

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. This is particularly true given the size of the subsector's financial footprint in Australia and the significant value of transactions it facilitates. In addition, money laundering helps criminals preserve illicit assets, can finance new crimes and can lead to corruption of public officials and private enterprise.

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

- societal harm inflicted upon the community through offences such as drug trafficking and child exploitation
- reduced government revenue due to tax evasion, impacting on 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 enterprise<sup>77</sup>
- widespread or concentrated real estate purchases with the proceeds of crime, driving property prices up and pricing legitimate buyers out of the market.

<sup>76</sup> APRA, *Information Paper: Domestic systemically important banks in Australia*, 2013, [apra.gov.au/sites/default/files/information-paper-domestic-systemically-important-banks-in-australia-december-2013.pdf](https://www.apra.gov.au/sites/default/files/information-paper-domestic-systemically-important-banks-in-australia-december-2013.pdf).

<sup>77</sup> 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 major 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 major 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.

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.

The subsector has a mixed record of applying risk mitigation strategies. On one hand, major banks make significant investments to counter ML/TF risk, engage regularly with AUSTRAC on both regulatory and intelligence matters, and some entities are undergoing a significant uplift in their AML/CTF systems, controls and policies. On the other hand, there have been significant and systemic deficiencies detected in the subsector over recent years. Governance and assurance around AML/CTF compliance has been identified as a particular concern, and risk mitigation strategies are not always applied consistently across a reporting entity's various businesses.

Because of the scale of major banks' operations, failures to implement and maintain risk mitigation strategies can be amplified many times over and

expose the subsector to significant ML/TF risk. It is crucial that reporting entities are aware of the impacts that group-level changes might have downstream on other parts of their business, particularly areas that might be vulnerable to ML/TF exploitation.

## **SYSTEMS AND RESOURCES**

Major banks are uniquely well resourced to purchase, adapt and build sophisticated transaction monitoring programs and other systems to identify and disrupt financial crime. Reporting entities in the subsector have increased investment in AML/CTF systems and controls in recent years and substantially increased the size of their financial crime teams as part of a general uplift of their AML/CTF capabilities. Each entity has hundreds of staff working to combat financial crime, and additional teams working to protect their customers from fraud. While additional resourcing is a key step towards a reporting entity developing

mature AML/CTF systems and controls, these should be supplemented with commensurate changes to organisational culture, governance practices and systems where appropriate.

During consultations some reporting entities acknowledged that legacy IT systems and databases were a vulnerability. One example given was the existence of multiple customer databases being used by separate businesses within the group, resulting in inconsistencies. While major banks have built and deployed upgraded IT systems in recent years to fix or prevent some of these issues, vulnerabilities in this area remain.

## CUSTOMER DUE DILIGENCE

Major banks generally employ CDD and ECDD processes to verify customers' identities and assess the legitimacy of their wealth or business operations. However, there have been a number of failings in applying appropriate CDD and ECDD by some major banks in recent years.

During industry consultations, major banks described their customer risk rating models and the range of factors they consider when determining a customer's risk rating. These include customer-specific factors, such as legal structure or industry, and also incorporate elements such as the products being used or any relevant foreign jurisdictions.

**i** Some reporting entities provide products and services that can be geared towards 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.

Major bank representatives also described policies to determine acceptable customer risk profiles, with customers that exceed certain thresholds refused at onboarding. Some entities identified that improving internal communication of what constitutes an acceptable risk is a priority.

Major bank representatives told AUSTRAC that higher-risk customers are subject to ECDD and periodic reviews of their KYC information; depending on the outcome of these reviews, a customer's risk rating may be modified. Despite this, one reporting entity pointed out that information received from a customer is point-in-time or 'static', while real world circumstances change frequently. For example, the occupation provided by a customer when they first establish their banking profile could change within months or be falsified. This entity told AUSTRAC that it preferred to rely on what it described as 'dynamic' information, such as information acquired through transaction monitoring.

## MAJOR BANKS ADAPT CDD PROCEDURES IN RESPONSE TO COVID-19

Due to COVID-19 restrictions, major banks have adopted other ways of verifying customer identity, using new methods such as video calling. One major bank consulted for this report indicated it is likely that some of these changes will remain in place after the pandemic is over.



## 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

Transaction monitoring programs allow reporting entities to detect ML/TF exploitation by criminal entities or terrorism financiers. This is particularly important given the extremely high volume of transactions processed by major banks. While most major banks use off-the-shelf transaction monitoring systems, industry representatives told AUSTRAC that these systems were subject to a high degree of customisation. For some specific low-volume or high-risk products, reporting entities employ manual monitoring or dedicated transaction monitoring programs to better manage ML/TF risks.

During consultations, major banks 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, with collected information flowing into reporting and used to update customer risk profiles.

However, in recent years AUSTRAC has identified a number of instances where some major banks' transaction monitoring and ECDD processes were poorly designed and executed. In some instances, this contributed to a significant volume of suspected criminal exploitation of the subsector.

Along with monitoring and identifying unusual transactions for suspicious activity, major bank representatives told AUSTRAC they also use these capabilities to proactively reduce ML/TF risks. For example, one major bank described an initiative to reduce its exposure to cash by identifying business customers with high rates of cash deposits and offering them electronic merchant services.

## RISK ASSESSMENTS

During consultations, every major bank described risk assessment processes built into their AML/CTF programs. As well as the customer risk assessment 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 major 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

Major banks are the largest SMR reporters of any sector regulated by AUSTRAC. There has been a 640 per cent increase in the number of reports submitted by the subsector since 2015.

SMRs submitted by major banks are generally of a good standard, and there has been consistent improvement in the amount and quality of information included. Of the reports reviewed for this assessment, those of the highest intelligence value included detailed transaction histories, records of contact with the customer or suspicious party and relevant information uncovered from carrying out ECDD, such as a customer's source of wealth.

AUSTRAC also 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 a 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 are generally not actionable.
- **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.

## 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 major banks to review these resources and consider if their reporting could be improved.

## FINTEL ALLIANCE COOPERATION

Launched in 2017 by AUSTRAC, Fintel Alliance is a world first public-private partnership to increase the resilience of the financial sector to prevent it being exploited by criminals and support law enforcement investigations into serious crime and national security matters. It brings together experts across 29 organisations from financial institutions – including all major banks – state and commonwealth law enforcement and intelligence agencies, and academia. Fintel Alliance focuses on enhancing information sharing between intelligence agencies and the private sector, as well as developing new capabilities to fight crime.

Major bank representatives frequently reported their involvement with Fintel Alliance was an important part of their ability to proactively disrupt financial crime. Fintel Alliance facilitates the sharing of emerging financial crime indicators and typologies, as well as the ability to conduct joint financial crime detection operations. During industry consultations, major bank representatives said they particularly valued access to expertise and information from AUSTRAC partner agencies, which enhanced situational awareness on criminal activities that could feed into risk mitigation efforts.

The COVID-19 pandemic has had unprecedented impacts on the financial industry and the global criminal threat environment. In 2020, Fintel Alliance established a dedicated COVID-19 response project, which enabled government and industry partners to work together to respond rapidly to emerging risks and protect Australians from fraud, particularly against the Early Release of Superannuation and JobKeeper schemes.

AUSTRAC shared information with Fintel Alliance partners at the outset of the pandemic to provide guidance on emerging fraud methodologies. The timeliness of this information enabled industry partners to closely monitor financial activity and submit actionable and targeted SMRs. In the first six months of 2020, AUSTRAC received approximately 5,000 COVID-19 related SMRs of which approximately 40 per cent were from Fintel Alliance partners. Reports received from industry provided valuable insights into how individuals and organised crime attempted to exploit the pandemic, targeting vulnerable Australians and the government for financial gain. Enhanced reporting also identified linkages between offenders for law enforcement to target and disrupt illegal activity.

## FORUM SHOPPING

Industry consultation revealed concerns about inconsistent systems and controls across the sector, particularly in relation to customer onboarding and product and service delivery.

As a result, criminals may 'forum shop' to exploit weak points. For example, in one scenario described during a consultation, an individual was refused onboarding at one major bank because they posed an unacceptably high ML/TF risk but was quickly onboarded by another major bank.

AUSTRAC found little evidence that criminals target specific reporting entities, but partner agencies report that criminals will constantly probe products or delivery channels for gaps in systems and controls and will quickly identify and exploit a weak link.

Systems that allow products and services to be applied for and delivered online are particularly vulnerable to probing, and controls around these delivery channels need to be carefully considered and calibrated.

It is also important that reporting entities maintain comprehensive controls to harden the entire subsector against criminal abuse and test these controls to ensure their continuing effectiveness. For example, all major banks require a third party depositing cash via an IDM to provide a mobile number, but only some entities authenticate this mobile number by sending a code to it.

# APPENDIX A: GLOSSARY

| NAME   | DESCRIPTION   |
|--|---|
| <b>Authorised deposit-taking institution (ADI)</b> | 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.                            |
| <b>AML/CTF</b>                                     | Anti-money laundering and counter-terrorism financing.  |
| <b>AML/CTF program</b>                             | A document that sets out how a reporting entity meets its AML/CTF compliance obligations.   |
| <b>Beneficial owner</b>                            | An individual who owns 25 per cent or more, or otherwise controls the business of an entity.  |
| <b>Corporate and institutional banking</b>         | 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  |
|---|--|
| <b>Cuckoo smurfing</b>  | 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.   |
| <b>Customer due diligence (CDD)</b>                                 | Customer due diligence (CDD) is the process where pertinent information of a customer's profile is collected and evaluated for potential ML/TF risks.  |
| <b>Designated business group (DBG)</b>                              | 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.  |
| <b>Designated non-financial businesses and professions (DNFBPs)</b> | 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.  |
| <b>Enhanced customer due diligence (ECDD)</b>                       | Enhanced customer due diligence (ECDD) is the process of undertaking additional customer identification and verification measures in certain circumstances deemed to be high risk.   |
| <b>Financial Action Task Force (FATF)</b>                           | 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.   |
| <b>Financial institutions</b>                                       | <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"> <li>• acceptance of deposits and other repayable funds from the public</li> <li>• lending</li> <li>• financial leasing</li> <li>• money or value transfer services</li> <li>• issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money)</li> <li>• financial guarantees and commitments</li> <li>• participation in securities issues and the provision of financial services related to such issues</li> <li>• individual and collective portfolio management</li> </ul> |

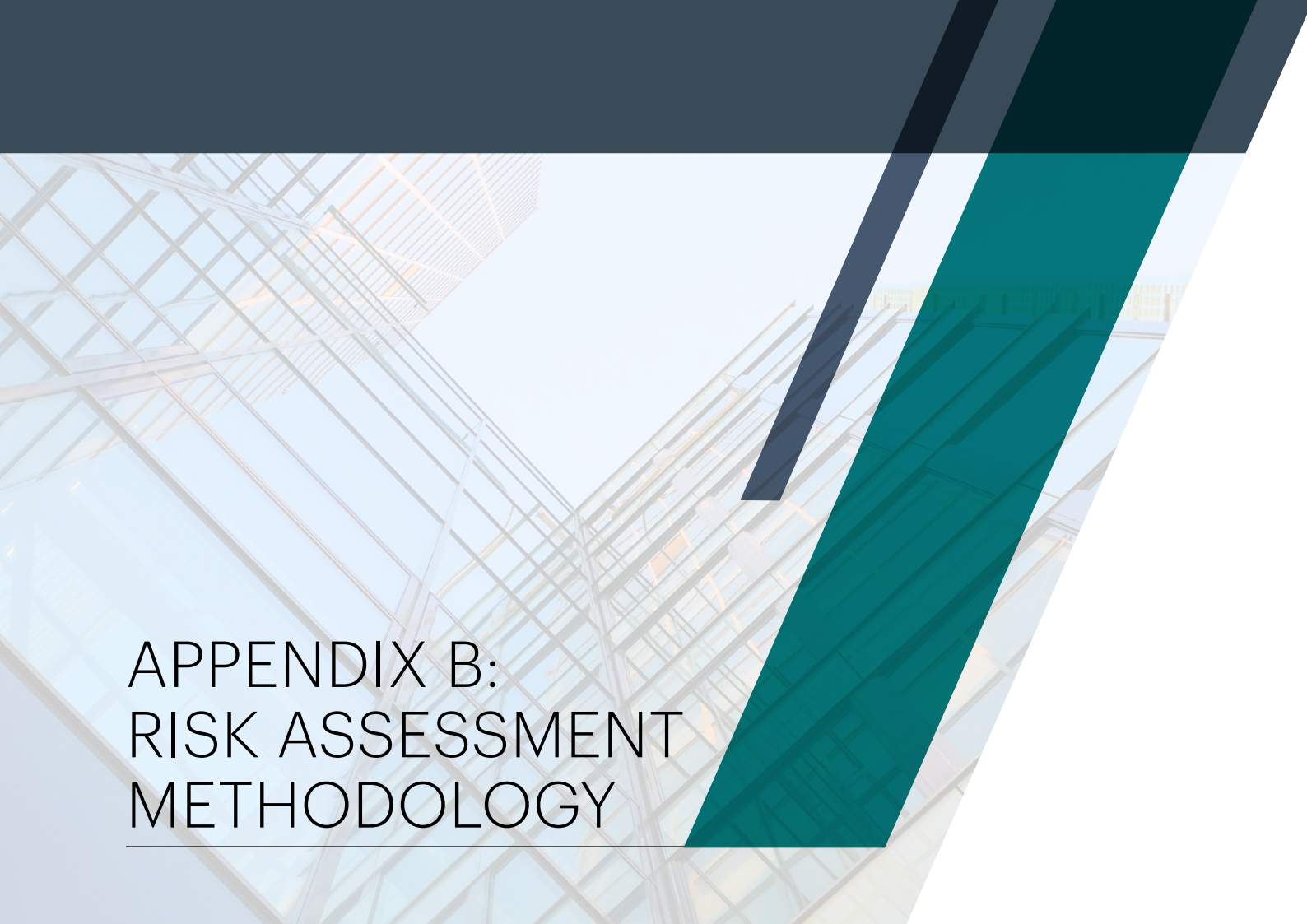
| NAME   | DESCRIPTION   |
|--|---|
| <b>Financial institutions cont.</b>                    | <ul style="list-style-type: none"> <li>• safekeeping and administration of cash or liquid securities on behalf of other persons</li> <li>• otherwise investing, administering or managing funds or money on behalf of other persons</li> <li>• underwriting and placement of life insurance and other investment related insurance</li> <li>• money and currency changing</li> <li>• trading in money market instruments, foreign exchange, exchange, interest rate and index instruments, transferable securities, commodity futures trading.</li> </ul> |
| <b>Global financial centres</b>                        | 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.   |
| <b>Inherent risk</b>                                   | Inherent risk represents the amount of risk that exists in the absence of AML/CTF controls implemented by the reporting entity.   |
| <b>Integration</b>                                     | 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.  |
| <b>Intelligent deposit machine (IDM)</b>               | 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.  |
| <b>International funds transfer instruction (IFTI)</b> | <p>An international funds transfer instruction (IFTI) involves either:</p> <ul style="list-style-type: none"> <li>• an instruction that is accepted in Australia for money or property to be made available in another country, or</li> <li>• an instruction that is accepted in another country for money or property to be made available in Australia.</li> </ul>  |
| <b>Layering</b>  | The second stage of the money laundering cycle, which involves moving, dispersing or disguising illegal funds or assets to conceal their true origin.   |
| <b>ML/TF</b>   | Money laundering/terrorism financing.   |
| <b>Phoenixing</b>                                      | Phoenixing occurs when a new company is created to continue the business of a company that has been deliberately liquidated to avoid paying its debts, including taxes, creditors and employee entitlements.  |
| <b>Placement</b>                                       | The first stage of the money laundering cycle, in which illicit funds first enter the formal financial system.  |



| NAME                                    | DESCRIPTION  |
|---|--|
| <b>Politically exposed person (PEP)</b> | <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"> <li>• Domestic PEP – someone who holds a prominent public position or role in an Australian government body.</li> <li>• Foreign PEP – someone who holds a prominent public position or role with a government body in a country other than Australia.</li> <li>• 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).</li> </ul> |
| <b>Predicate offence</b>                | For the purpose of this risk assessment, a predicate offence is any offence that generates proceeds of crime.  |
| <b>Private banking</b>                  | 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.  |
| <b>Residual risk</b>                    | Residual risk is the amount of risk that remains after a reporting entity's AML/CTF controls are accounted for.  |
| <b>Retail banking</b>                   | 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.  |
| <b>Suspicious matter report (SMR)</b>   | A report a reporting entity must submit 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.   |



| NAME   | DESCRIPTION  |
|--|--|
| <b>Structuring</b>                                       | Making or receiving a series of cash transactions intentionally structured to be below the \$10,000 reporting threshold.   |
| <b>Threshold transaction report (TTR)</b>                | 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.   |
| <b>Trade-based money laundering (TBML)</b>               | 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.   |
| <b>Transnational, serious and organised crime (TSOC)</b> | <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"> <li>• manufacture and trade of illicit commodities, including drugs and firearms</li> <li>• sexual exploitation of children</li> <li>• human trafficking and slavery</li> <li>• serious financial crime</li> <li>• cyber crime</li> </ul> <p>Key enablers of transnational, serious and organised crime include money laundering, identity crime and public sector corruption.</p> |
| <b>Trigger-based reporting</b>                           | 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.   |



## 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 higher-risk entities.  | Money laundering methodologies are moderately varied. There is a medium level of involvement by SOCGs and other higher-risk entities.                                | Money laundering methodologies are highly varied. There is a high level of involvement by SOCGs and other higher-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 utilising the subsector. | Terrorist financing methodologies are somewhat varied. There is a small number of terrorist groups, financiers, associates and facilitators utilising the subsector. | Terrorist financing methodologies are highly varied. There are several terrorist groups, financiers, associates and facilitators utilising 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/service rarely involves cash, or involves cash in small amounts.           | Provision of product/service sometimes involves cash, or involves cash in moderate amounts. | Provision of product/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/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/or value can be transferred internationally.                   | Significant amounts of funds and/or value are easily transferred internationally.    |
| Transactions rarely or never involve higher-risk jurisdictions.                                 | Transactions sometimes involve higher-risk jurisdictions.                                   | Transactions often involve higher-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 |
|--|------------|-----------|
| Major bank reports that identified ML          | 46%        | 57%       |
| <b>Top 5 suspicious transaction activities</b> |            |           |
| Large transactions                             | 51%        | N/A       |
| Cash deposits (face-to-face)                   | 46%        | N/A       |
| Multiple transactions                          | 44%        | N/A       |
| Cash deposits (ATM)                            | 36%        | N/A       |
| Structuring                                    | 25%        | N/A       |
| <b>Customer type</b>                           |            |           |
| Individual                                     | 92%        | 79%       |
| Company  | 15%        | 40%       |
| Sole trader                                    | 3%         | N/A       |
| Trust  | 2%         | N/A       |
| <b>Involved PEP</b>                            |            |           |
| Yes  | 0.3%       | 6%        |
| No   | 99.7%      | 94%       |



| ATTRIBUTE                                  | SMR SAMPLE | IR REVIEW |
|--|------------|-----------|
| <b>Involved DNFBP</b>                      |            |           |
| Yes  | 3%         | 5%        |
| No   | 97%        | 95%       |
| <b>Product used</b>                        |            |           |
| Transaction account                        | 85%        | 97%       |
| Chequebooks                                | 8%         | 5%        |
| Bank cheques                               | 6%         | 7%        |
| Loan accounts                              | 5%         | 1%        |
| Credit card accounts                       | 2%         | 1%        |
| Trust accounts                             | 1%         | 0.5%      |
| <b>Direction of funds</b>                  |            |           |
| Domestic                                   | 79%        | 32%       |
| Incoming                                   | 14%        | 22%       |
| Outgoing                                   | 6%         | 17%       |
| <b>Involved a higher-risk jurisdiction</b> |            |           |
| Yes  | 18%        | 54%       |
| No   | 82%        | 46%       |
| <b>Involved cash</b>                       |            |           |
| Yes  | 79%        | 93%       |
| No   | 21%        | 7%        |

## MONEY LAUNDERING ATTRIBUTES FROM SMR SAMPLE AND IR REVIEW

| ATTRIBUTE                                      | SMR SAMPLE | IR REVIEW |
|--|------------|-----------|
| Major bank reports that identified ML          | 46%        | 57%       |
| <b>Top 5 suspicious transaction activities</b> |            |           |
| Large transactions                             | 51%        | N/A       |
| Cash deposits (face-to-face)                   | 46%        | N/A       |
| Multiple transactions                          | 44%        | N/A       |
| Cash deposits (ATM)                            | 36%        | N/A       |
| Structuring                                    | 25%        | N/A       |
| <b>Customer type</b>                           |            |           |
| Individual                                     | 92%        | 79%       |
| Company  | 15%        | 40%       |
| Sole trader                                    | 3%         | N/A       |
| Trust  | 2%         | N/A       |
| <b>Involved PEP</b>                            |            |           |
| Yes  | 0.3%       | 6%        |
| No   | 99.7%      | 94%       |
| <b>Involved DNFBP</b>                          |            |           |
| Yes  | 3%         | 5%        |
| No   | 97%        | 95%       |

| ATTRIBUTE                                  | SMR SAMPLE | IR REVIEW |
|--|------------|-----------|
| <b>Product used</b>                        |            |           |
| Transaction account                        | 85%        | 97%       |
| Chequebooks                                | 8%         | 5%        |
| Bank cheques                               | 6%         | 7%        |
| Loan accounts                              | 5%         | 1%        |
| Credit card accounts                       | 2%         | 1%        |
| Trust accounts                             | 1%         | 0.5%      |
| <b>Direction of funds</b>                  |            |           |
| Domestic                                   | 79%        | 32%       |
| Incoming                                   | 14%        | 22%       |
| Outgoing                                   | 6%         | 17%       |
| <b>Involved a higher-risk jurisdiction</b> |            |           |
| Yes  | 18%        | 54%       |
| No   | 82%        | 46%       |
| <b>Involved cash</b>                       |            |           |
| Yes  | 79%        | 93%       |
| No   | 21%        | 7%        |

## PREDICATE OFFENCE ATTRIBUTES FROM SMR SAMPLE AND IR REVIEW

| ATTRIBUTE  | SMR SAMPLE | IR REVIEW |
|--|------------|-----------|
| Major bank reports that identified a predicate offence                   | 46%        | 57%       |
| <b>Key predicate offences (proportion of all major bank reports)</b>     |            |           |
| Tax evasion  | 9%         | 19%       |
| Drug trafficking   | 1%         | 5%        |
| Frauds   | 9%         | 8%        |
| Scams  | 5%         | 3%        |
| Other high-impact predicate offences                                     | 1.07%      | 9.6%      |
| <b>Other high-impact predicate offences</b>                              |            |           |
| Sanctions violations   | 0.40%      | 3.9%      |
| Bribery and corruption   | 0.20%      | 3.4%      |
| Child exploitation   | 0.30%      | 1.7%      |
| Firearms trafficking   | 0.20%*     | 0.6%      |
| Modern slavery   | 0.01%*     | 0%        |
| Environmental crimes (includes wildlife trafficking)                     | 0.03%*     | 0%        |
| *determined using keyword analysis                                       |            |           |
| <b>Customer type (proportion of reports that identified a predicate)</b> |            |           |
| Individual   | 89%        | 73%       |
| Company  | 22%        | 46%       |
| Sole trader  | 4%         | N/A       |
| Trust  | 1%         | N/A       |

| ATTRIBUTE                                  | SMR SAMPLE | IR REVIEW |
|--|------------|-----------|
| <b>Involved PEP</b>                        |            |           |
| Yes  | 0.4%       | 2%        |
| No   | 99.6%      | 98%       |
| <b>Product used</b>                        |            |           |
| Transaction account                        | 65%        | 92%       |
| Chequebooks                                | 9%         | 5%        |
| Bank cheques                               | 2%         | 5%        |
| Loan accounts                              | 4%         | 1%        |
| Credit card accounts                       | 7%         | 1%        |
| <b>Direction of funds</b>                  |            |           |
| Domestic                                   | 90%        | 30%       |
| Incoming                                   | 3%         | 16%       |
| Outgoing                                   | 7%         | 21%       |
| Incoming and Outgoing                      | 0.4%       | 25%       |
| <b>Involved a higher-risk jurisdiction</b> |            |           |
| Yes  | 10%        | 59%       |
| No   | 90%        | 41%       |
| <b>Involved cash</b>                       |            |           |
| Yes  | 79%        | 93%       |
| No   | 21%        | 7%        |

## TERRORISM FINANCING ATTRIBUTES FROM SMR SAMPLE AND IR REVIEW

| ATTRIBUTE  | SMR SAMPLE | IR REVIEW |
|--|------------|-----------|
| Major bank reports that identified TF                          | 0.3%       | 9%        |
| % of all TF-related reports across entire reporting population | 74%        | 46%       |
| <b>Top 5 suspicious transaction activities</b>                 |            |           |
| Multiple transactions  | 46%        | N/A       |
| Cash deposits (face-to-face)                                   | 29%        | N/A       |
| Large transactions   | 25%        | N/A       |
| Rapid or complex movement of funds                             | 21%        | N/A       |
| Multiple parties   | 17%        | N/A       |
| <b>Customer type</b>   |            |           |
| Individual   | 96%        | 85%       |
| Company  | 8%         | 9%        |
| Association  | 4%         | 9%        |
| <b>Product used</b>  |            |           |
| Transaction account  | 88%        | 97%       |
| Chequebooks  | 4%         | 0%        |
| Stored value card  | 0%         | 6%        |
| Loan accounts  | 0%         | 6%        |
| Credit card accounts   | 7%         | 1%        |

| ATTRIBUTE                                  | SMR SAMPLE | IR REVIEW |
|--|------------|-----------|
| <b>Direction of funds</b>                  |            |           |
| Domestic                                   | 54%        | 21%       |
| Incoming                                   | 4%         | 3%        |
| Outgoing                                   | 38%        | 42%       |
| Incoming and outgoing                      | 4%         | 33%       |
| <b>Involved a higher-risk jurisdiction</b> |            |           |
| Yes  | 63%        | 64%       |
| No   | 37%        | 36%       |
| <b>Involved cash</b>                       |            |           |
| Yes  | 50%        | 61%       |
| No   | 50%        | 39%       |



AUSTRAC.GOV.AU

