



Australian Government

AUSTRAC

FIGHTING  
FINANCIAL  
CRIME  
TOGETHER



# FOREIGN SUBSIDIARY BANKS IN AUSTRALIA

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 foreign subsidiary 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>09</b>
<b>BACKGROUND</b>	<b>11</b>
<b>METHODOLOGY</b>	<b>13</b>
<b>FOREIGN SUBSIDIARY BANKS: REPORTING TO AUSTRAC</b>	<b>16</b>
<b>CRIMINAL THREAT ENVIRONMENT</b>	<b>18</b>
Money laundering	20
Terrorism financing	26
Predicate offences	28
<b>VULNERABILITIES</b>	<b>38</b>
Customers	39
Products and services	47
Delivery channels	55
Foreign jurisdictions	59
<b>CONSEQUENCES</b>	<b>63</b>
<b>RISK MITIGATION STRATEGIES</b>	<b>67</b>
<b>APPENDICES</b>	<b>73</b>



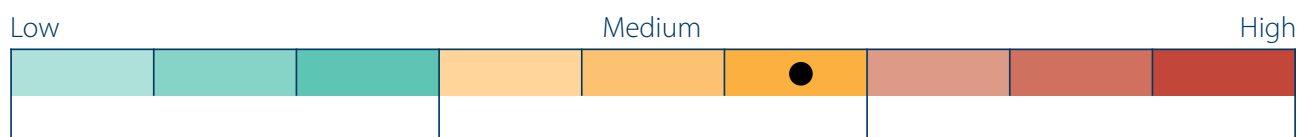
# EXECUTIVE SUMMARY

Foreign subsidiary banks operating in Australia are authorised deposit-taking institutions (ADIs) licensed by the Australian Prudential Regulation Authority (APRA). Foreign subsidiary banks carry on business through a locally incorporated subsidiary that is a separate legal entity from its foreign bank parent. As at June 2021, seven foreign subsidiary banks operate in Australia, providing services to approximately 4.8 million customers.

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



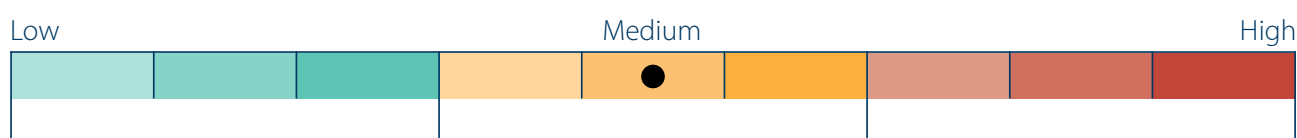
## OVERALL RISK RATING



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

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

## CRIMINAL THREAT ENVIRONMENT



AUSTRAC assesses the threat of ML/TF facing foreign subsidiary banks as **medium**.

The criminal threat environment facing foreign subsidiary banks is varied. While there is a moderate to high volume of suspected criminal misuse of the subsector, methods are largely unsophisticated. Data-matching to criminal lists also suggests the subsector is not significantly exposed to national or transnational, serious and organised criminal entities, or entities linked to terrorism or terrorism financing activities. The primary threats facing the subsector are frauds, money laundering, scams and tax evasion.

## MONEY LAUNDERING

The nature and extent of money laundering threats facing foreign subsidiary banks is assessed as **medium**.

This assessment is based on a moderate number of suspicious matter reports (SMRs) reported by the subsector which suggest money laundering predominantly relates to cash and transaction account-based services. Partner agencies report very low levels of suspected or detected money laundering in the subsector. Data-matching to criminal lists suggests foreign subsidiary banks are not significantly exposed to known or suspected criminals.

Foreign subsidiary banks are more likely to be exploited during the placement and layering phases of the money laundering process. This is due to the subsector's retail banking footprint which enables customers to place cash directly into the financial system, and offers multiple products and services that enable fast and efficient movement of funds. A number of foreign subsidiary banks operate a branchless business model and rely on third-party agent banking relationships to allow customers to transact in cash. These delivery channels introduce additional money laundering vulnerabilities to the product delivery chain.

To a lesser extent, foreign subsidiary banks can also be exploited during the integration phase of the money laundering process. This primarily occurs through the purchase of high-value assets.

## TERRORISM FINANCING

The nature and extent of terrorism financing threats facing the subsector is assessed as **low**.

Across the entire reporting population, foreign subsidiary banks submit a very small fraction of all terrorism financing-related SMRs. Less than one per cent of SMRs reviewed for this report related to suspected terrorism financing. These reports related predominantly to customers appearing in adverse media or on watch lists and there were no confirmed instances of terrorism financing. In addition, data-matching to criminal lists suggests foreign subsidiary banks are not significantly exposed to known or suspected terrorists or their financiers.

## PREDICATE OFFENCES

The nature and extent of threat posed by predicate offending involving foreign subsidiary banks is assessed as **high**.<sup>1</sup>

Predicate offending is varied, extensive and sometimes involves sophisticated methods. Frauds were most common, followed by scams and tax evasion.

Frauds were observed in 47 per cent of SMRs reviewed for this report. Many cases involved identity fraud, where the offender used fraudulent documents and/or a stolen identity to open a transaction account online. The volume of online fraud detected by reporting entities is consistent with their use of remote service delivery channels.

Scams were observed in nine per cent of SMRs reviewed for this report. Phishing and remote access scams were most common, with individual customers targeted in these activities.<sup>2,3</sup>

Tax evasion was observed in nine per cent of SMRs reviewed for this report. Suspected personal income tax evasion was most commonly reported, followed by corporate tax evasion and other tax-related offences. Despite this, AUSTRAC assesses corporate tax evasion probably poses the same level of risk as personal income tax evasion because associated values are often much larger.

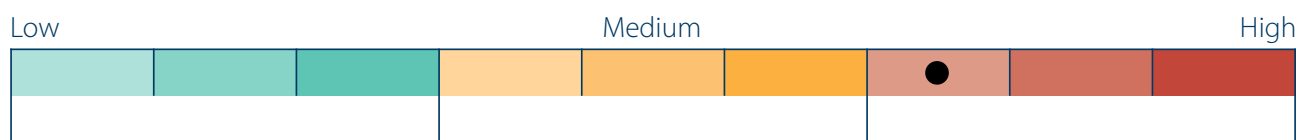
The subsector is also exposed to high-impact offences like sanctions violations, bribery and corruption, drug trafficking and child exploitation.

1 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.

2 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.

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

## VULNERABILITIES



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

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

- a moderate number of **higher-risk customers**, which can present across a range of categories including:
  - 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>
  - foreign-based customers
  - temporary visa holders
  - financial institutions.<sup>6</sup>
- **a moderate exposure to cash**
- **products and services** that can be used to **store and move funds** in and out of the subsector such as:
  - transaction, savings and trust accounts
  - credit cards
  - chequebook access
  - correspondent banking services.
- heavy reliance on **remote service delivery channels**, particularly online banking and automatic teller machines (ATMs). These channels provide anonymity, facilitate identity fraud and other financial crimes, and complicate detection of suspicious transactions.
- high exposure to **foreign jurisdictions**, including **higher-risk jurisdictions**.

Other features that can expose the subsector to ML/TF vulnerability include:

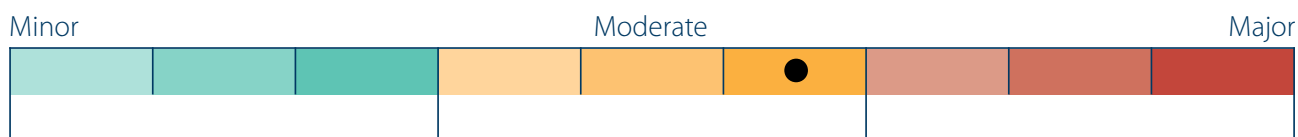
- lack of clarity and oversight of **agent bank arrangements** and reporting obligations
- **limited SMR reporting** leading to reduced financial intelligence and detection of criminality.

<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 foreign subsidiary 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 **moderate**.

### CUSTOMERS

AUSTRAC assesses criminal activity likely has **moderate** consequences for customers. Given the subsector's large individual customer base, the most significant impacts relate to financial loss and emotional distress caused by fraud and scam-related offences. For company customers or sole traders, criminal exploitation can also cause reputational damage to business or brand image.

### INDIVIDUAL BUSINESSES AND THE SUBSECTOR

Criminal activity can have **moderate** consequences for a foreign subsidiary bank's Australian operation, as well as their broader business group. Impacts can be financial, reputational and operational. These consequences vary between reporting entities and largely depend on the extent to which they understand and mitigate their ML/TF risks, as well as their ability to absorb potential financial losses or withstand reputational damage.

### AUSTRALIAN FINANCIAL SYSTEM AND COMMUNITY

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

### NATIONAL AND INTERNATIONAL SECURITY

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

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



## RISK MITIGATION STRATEGIES

Most reporting entities indicate they have implemented risk mitigation strategies, including customer due diligence (CDD) procedures, customer risk rating tools, product controls and transaction monitoring. However, several reporting entities acknowledge a need to improve technological capabilities. Improvements to the quality and quantity of SMR submissions can also be made across the subsector.

Because financial crime programs are often developed offshore by head office, the effectiveness of ML/TF risk mitigation strategies is largely incumbent on:

- the culture and maturity of AML/CTF processes and programs employed by head office, and their understanding of local risks
- the effectiveness of AML/CTF regimes in the jurisdiction in which head office is based.



# PURPOSE

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

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

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

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

## ASSESSING ML/TF RISK IN AUSTRALIA'S BANKING SECTOR

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

This report represents one of four risk assessments on Australia's banking sector that are being completed under this program of work. The other assessments focus on major domestic banks, other domestic 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 also 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

Foreign subsidiary banks operating in Australia are ADIs licensed by APRA. Foreign subsidiary banks should not be confused with branches of foreign banks.<sup>7</sup> Foreign subsidiary banks are incorporated in Australia, must hold capital locally and are subject to the same prudential standards and supervision as Australian-owned banks.<sup>8</sup>

Currently, seven foreign subsidiary banks operate in Australia, providing services to approximately 4.8 million customers.<sup>9</sup> Combined, foreign subsidiary banks hold assets worth \$195 billion, representing approximately four per cent of the Australian ADI market. Compared to other banking subsectors in Australia, the financial scale of foreign subsidiary banks is the second smallest (Australia's mutual banks subsector is the smallest).

Foreign subsidiary banks are largely retail focused and primarily provide products and services to individual customers. Some reporting entities also provide products and services to a small number of corporate and institutional customers, as well as some private banking customers. Refer to the **Glossary** at **Appendix A** for an explanation of these terms.

<sup>7</sup> AUSTRAC has completed a separate ML/TF risk assessment on foreign bank branches operating in Australia.

<sup>8</sup> By contrast, foreign bank branches are not locally incorporated, do not hold capital locally and are mainly supervised by the prudential regulator in their home country.

<sup>9</sup> A list of foreign subsidiary banks operating in Australia can be found on APRA's website at [apra.gov.au/register-of-authorised-deposit-taking-institutions](https://apra.gov.au/register-of-authorised-deposit-taking-institutions).

Foreign subsidiary banks are recognised as both licensed ADIs and reporting entities providing designated services under the AML/CTF Act. Under the AML/CTF Act, foreign subsidiary banks are required to have a compliant AML/CTF program and report to AUSTRAC:

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

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

Across the subsector, the characteristics and activities of individual foreign subsidiary banks vary significantly. There is diversity in factors like size and composition of customer bases, types of products offered, channels used to deliver services and foreign jurisdiction risk exposure.

For example, several reporting entities offer a wide array of products through various in-person and online channels, while other reporting entities offer fewer products and operate solely online. Consequently, the ML/TF risks facing individual reporting entities vary.

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 foreign subsidiary 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>



**7**

Number of reporting entities



**4.8 MILLION**

Number of customers



Total resident assets

**4%** of all ADIs



Total deposits

**3%** of all ADIs



Total loans to households

**4%** of all ADIs



Loans to households (housing only)

**5%** 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 foreign subsidiary 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 through the subsector may cause.

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

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

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

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

1. Analysis of transaction reports, compliance reports and other holdings, including 1,321 SMRs submitted by foreign subsidiary banks between 1 April 2018 and 31 March 2019 (the **SMR sample**). See the call-out box **Labelling the SMR sample** on page 15 for more detail.
2. A comprehensive review of almost 700 AUSTRAC and partner agency intelligence reports produced between January 2018 and February 2019. Five per cent of these related to foreign subsidiary 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 foreign subsidiary banks between 30 March 2018 and 1 April 2019 and criminal entities who were:
  - recorded as a member of a significant national or transnational criminal group as at May 2020
  - charged with a money laundering or proceeds of crime-related offence between 1 January 2017 and 31 December 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 foreign subsidiary bank 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. To account for any intelligence gaps, AUSTRAC issued a survey to all partner agencies. This survey included questions regarding the criminal threat environment and various factors of ML/TF vulnerability.

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 Money laundering
<b>Suspicious transactional activity</b>	Cash deposits Structuring Money mules
<b>Products and services</b>	Transaction account
<b>Customer type</b>	Company
<b>Entity attribute</b>	Third party DNFBP lawyer
<b>Foreign jurisdiction</b>	Jurisdiction 'X'

# FOREIGN SUBSIDIARY BANKS: REPORTING TO AUSTRAC

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

### SMRs



**2,610**  
reports

**7**  
Number of reporting entities  
submitting at least one SMR

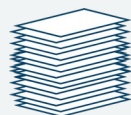


**\$1.3**  
BILLION

Total  
value

**1**  
Number of reporting entities  
accounting for 40 per cent of all  
SMRs submitted

### TTRs



**18,836**  
reports



**\$398**  
MILLION

Total  
value



**\$317**  
MILLION

Cash  
component

### IFTIs



**1.9+**  
MILLION  
reports



**\$844**  
BILLION

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

Across the subsector, there is wide variation in the quality and content of SMR submissions in the sample. For example, one reporting entity accounted for 40 per cent of all SMR submissions. Refer to the **Risk mitigation strategies** section for more detailed feedback.

### 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

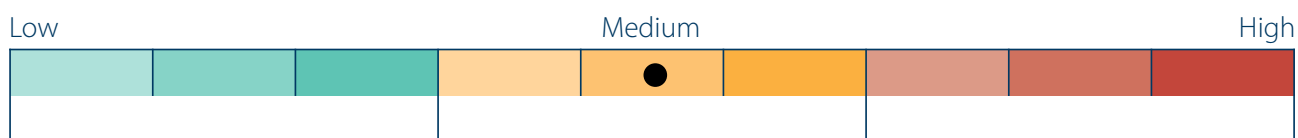
In December 2020, the Australian Parliament passed the *Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Act 2020* (the Amendment Act) to implement the next phase of reforms to the AML/CTF Act.<sup>16</sup> The Amendment Act includes, among other things, reforms to 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



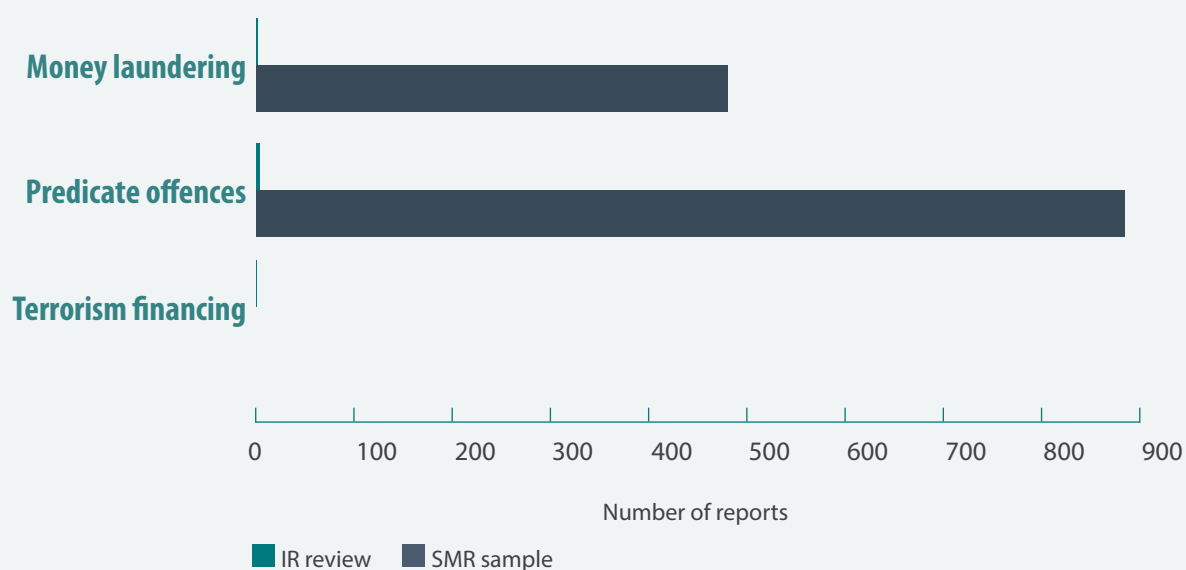
CRIMINAL THREAT ENVIRONMENT FACTOR	RATING
Money laundering	
Terrorism financing	
Predicate offences	

AUSTRAC assesses the threat of ML/TF facing the foreign subsidiary banks subsector as **medium**.

The criminal threat environment refers to the nature and extent of money laundering, terrorism financing and predicate offences associated with foreign subsidiary banks.

While there is evidence of some complex criminal methods used, those detected to date are relatively unsophisticated. The primary threats facing foreign subsidiary banks are frauds, money laundering, scams and tax evasion. No confirmed instances of terrorism financing in the subsector were identified during the reporting period.

#### FOREIGN SUBSIDIARY BANKS: DETECTED THREATS



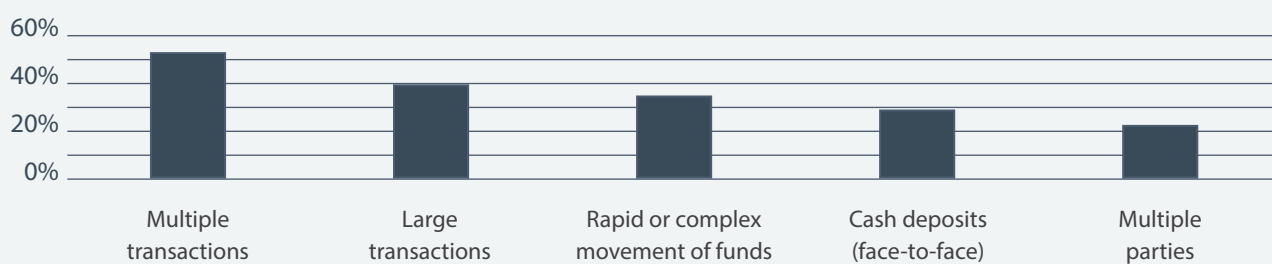
## MONEY LAUNDERING

AUSTRAC assesses the nature and extent of money laundering threats facing foreign subsidiary banks as **medium**.

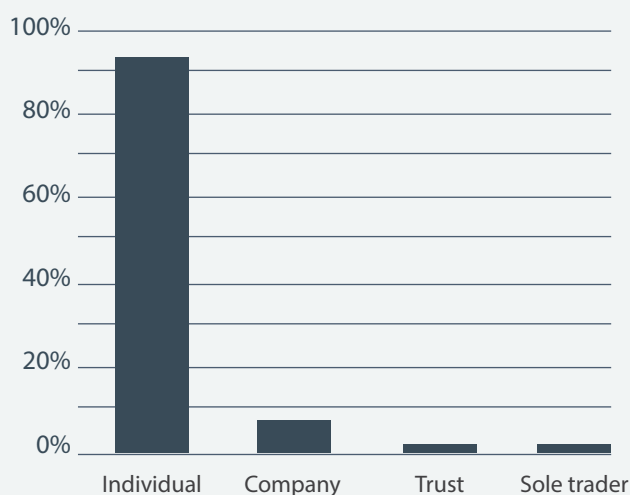
This assessment is based on a moderate number of SMRs reported by foreign subsidiary banks and a small proportion of reports in the IR review which suggest money laundering relates predominantly to cash and transaction account-based services.

Anecdotally, partner agencies report extremely low levels of suspected or detected money laundering in the subsector and data-matching to criminal lists suggests foreign subsidiary banks are not significantly exposed to known or suspected criminals (see page 40 for a detailed overview of higher-risk customer data-matching results).

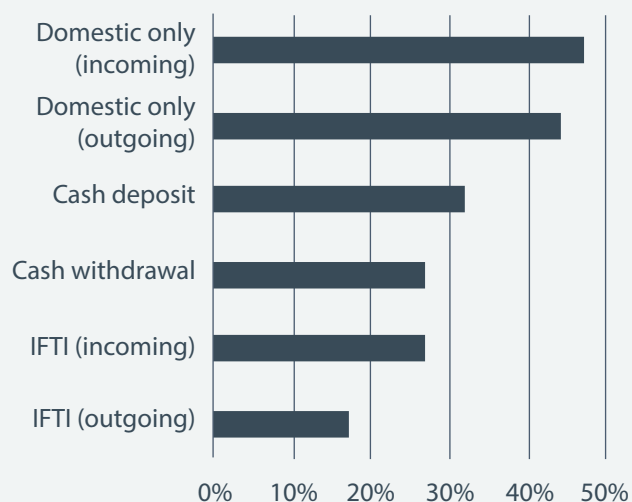
### ML-RELATED SMRs: METHODS



### ML-RELATED SMRs: CUSTOMER TYPES



### ML-RELATED SMRs: DIRECTION OF FUNDS



During the reporting period, 36 per cent of the SMR sample and 59 per cent of the IR review related to suspected money laundering.<sup>17</sup> In line with the subsector's customer base, individual customers were most prominently observed. Even when company customers were identified, individual customers were also often involved, suggesting individuals layer illicit funds through company and personal accounts in attempt to obscure the money trail.

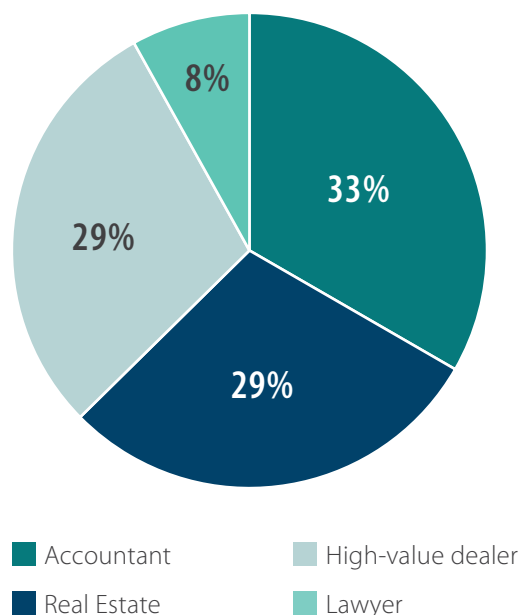
In addition, individuals were observed combining several money laundering methods, likely to avoid reporting obligations and evade detection. For example, structuring was often seen in combination with the rapid or complex movement of funds. Other common suspicious transactional activity included multiple transactions (potentially without economic rationale), large and unusual transactions and activity inconsistent with a customer's profile.

Foreign subsidiary banks are more likely to be exploited during the placement and layering phases of the money laundering process. This is due to the subsector's large retail banking footprint which enables customers to place cash directly into the financial system, and offers multiple products and services that enable fast and efficient movement of funds. The SMR sample and IR review indicate customers often engage in rapid movement of funds between accounts and between other domestic ADIs. This is particularly prominent following cash deposits. Suspicious funds are also layered through incoming and outgoing international transfers.

To a lesser extent, foreign subsidiary banks are exploited during the integration phase of the money laundering process. This primarily occurs through the purchase of high-value assets. Collectively, the subsector accounts for four per cent of all loans to households in Australia, valued at \$91 billion.<sup>18</sup> In the reporting period, just over one per cent of SMRs noted the suspicious purchase of a high-value asset. The majority of these purchases were for property. However, cars, boats and watches were also observed.

The purchase of high-value assets are often facilitated by DNFBPs. In the reporting period, five per cent of money laundering SMRs referenced DNFBPs. Accountants, real estate agents and high-value dealers were most often identified (see pie chart below). ML/TF vulnerabilities associated with DNFBPs is discussed in **Higher-risk customers** on page 42.

#### OCCURRENCE OF DNFBPs IN MONEY LAUNDERING-RELATED SMRs



<sup>17</sup> In the SMR sample and IR review, 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> APRA, *Monthly authorised deposit-taking institution statistics backseries: July 2019*, [apra.gov.au/monthly-authorised-deposit-taking-institution-statistics](https://apra.gov.au/monthly-authorised-deposit-taking-institution-statistics).

### **CASE STUDY: SUSPECTED MONEY LAUNDERING BY ENTITY LINKED TO SERIOUS AND ORGANISED CRIME**

In 2019, a foreign subsidiary bank identified a series of financial transactions that indicated layering activity involving a new customer account. This included multiple large deposits and incoming transfers followed by rapid movement of funds out of the account to service a personal home loan, fund lifestyle expenses, make luxury purchases and make transfers to a business partner. Following detection of these transactions, the reporting entity conducted enhanced customer due diligence (ECDD) on the customer and submitted an SMR to AUSTRAC.

An AUSTRAC investigation confirmed the customer was a known criminal who had been investigated by several partner agencies for suspected money laundering and links to large scale drug importations. AUSTRAC produced an intelligence report outlining the recent suspicious financial activity and provided it to partner agencies.

Suspicious financial activity and red flags for reporting entities in this example include:

#### **SUSPICIOUS FINANCIAL ACTIVITY**

- In a two-week period, incoming transfers and deposits totalling \$235,000 including:
  - two \$50,000 domestic transfers from the same third-party payer on the same day
  - over \$100,000 in cash deposits via eight separate threshold transactions
  - rapid incoming domestic transfers from the entity's personal bank account held with a major domestic bank. These funds were originally placed with the major bank through structured cash deposits, including by third parties.
- Rapid outgoing transfer of funds to:
  - service the entity's personal home loan
  - offshore companies involved in selling luxury goods – likely for the purchase of high-value assets
  - the entity's business partner.

#### **RED FLAGS**

- Relatively new client – suspicious activity commenced five months after account opening
- Suspected use of personal account for business activities
- Unclear source of funds
- Multiple large cash transactions, particularly in a short period of time
- Multiple third-party cash deposits.



## CASH-RELATED SUSPICIONS

Suspicious cash transactions were a common theme of money laundering-related SMRs. Analysis of the SMR sample showed that most suspicious cash deposits were made in-branch. This is likely because only two foreign subsidiary banks operate ATMs that accept cash deposits, therefore displacing this activity to branch locations. Conversely, most suspicious cash withdrawals were made at ATMs. Of SMRs that identified ATM cash withdrawals:

- 46 per cent involved rapid or complex movement of funds prior to the withdrawal
- 36 per cent involved a withdrawal at an overseas ATM
- 23 per cent involved suspected gambling activities including:
  - online wagering, where the customer withdrew cash after receiving funds from an online bookmaker
  - suspicious transactions made near casinos where the customer is a known frequent patron.

A number of foreign subsidiary banks operate a branchless business model and rely on third-party agent banking relationships to allow customers to transact in cash. These delivery channels introduce additional ML/TF vulnerabilities to the product delivery chain, which are discussed on page 57.

## COMMON CASH-BASED MONEY LAUNDERING METHODS USED BY SERIOUS ORGANISED CRIME GROUPS

National and transnational, serious organised crime groups use a variety of banking products and services to launder illicit cash. Common methods include:

- cuckoo smurfing, offsetting arrangements and the use of money mules and other third parties to make significant cash deposits
- large or rapid domestic transfer of funds between personal and business transaction accounts
- use and transfer of funds between transaction accounts held with multiple domestic and foreign banks (e.g. transferring funds offshore and returning them to a different domestic account)
- misrepresentation of personal details on bank forms or threshold transaction reports.

**i** Foreign subsidiary banks should remain vigilant to common cash-based money laundering methods used by these criminal groups, and continue to report suspicious transactions to AUSTRAC.

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

## TRADE-BASED MONEY LAUNDERING

Only one report in the SMR sample identified suspected trade-based money laundering (TBML).<sup>19</sup> However, TBML is likely under-represented in reporting due to challenges in detection. In addition, reporting entities across all banking subsectors as well as industry representatives indicated their concerns relating to TBML given the often large values of associated transactions.

While industry identified trade finance as particularly vulnerable to TBML, partner agencies and industry representatives report that TBML is likely to be under-represented and is often enabled by simpler products like transaction accounts and international funds transfers.

### 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
  - 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 in excess of expectations for that business
- companies operating in porous border regions close to higher-risk jurisdictions.

<sup>19</sup> TBML refers to 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.

Foreign subsidiary banks that offer trade finance products are also exposed to trade finance-based money laundering. 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 appear 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.

 Foreign subsidiary banks should continue strengthening systems and controls to identify possible TBML across all products and services, while also remaining alert to risks associated with trade finance.

### **FINTEL ALLIANCE TBML WORKING GROUP**

In 2020, AUSTRAC's public-private partnership Fintel Alliance established a dedicated working group on TBML. The working group includes representatives from public and private Fintel Alliance members, including one foreign subsidiary bank, who convene monthly to focus on priority issues. The working group fosters knowledge exchange among Fintel Alliance members. For example, a 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.

## TERRORISM FINANCING

AUSTRAC assesses the nature and extent of terrorism financing threats facing the foreign subsidiary bank subsector as **low**.

This assessment is based on the very small number of terrorism financing-related SMRs submitted by foreign subsidiary banks, information provided by partner agencies and Australia's terrorism financing environment. In addition, the data-matching exercise suggests foreign subsidiary banks are not significantly exposed to known or suspected terrorists or their financiers.

Less than one per cent of the SMR sample related to possible terrorism financing activity. In all cases, AUSTRAC could not confirm terrorism financing had actually occurred. Identified themes include:

- trigger-based reporting in response to an entity being recorded in adverse media or on a watch list
- suspicions relating to a family member of an Islamic State of Iraq and the Levant (ISIL) supporter
- low-value outgoing funds transfers to known higher-risk jurisdictions
- deliberate attempts to avoid reporting obligations or evasive responses to requests for further information.

**i** Foreign subsidiary 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.

## AUSTRALIA'S TERRORISM FINANCING ENVIRONMENT

Since the territorial collapse of ISIL'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.

## IDENTIFYING TERRORISM FINANCING

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

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

Common indicators of terrorism financing include:

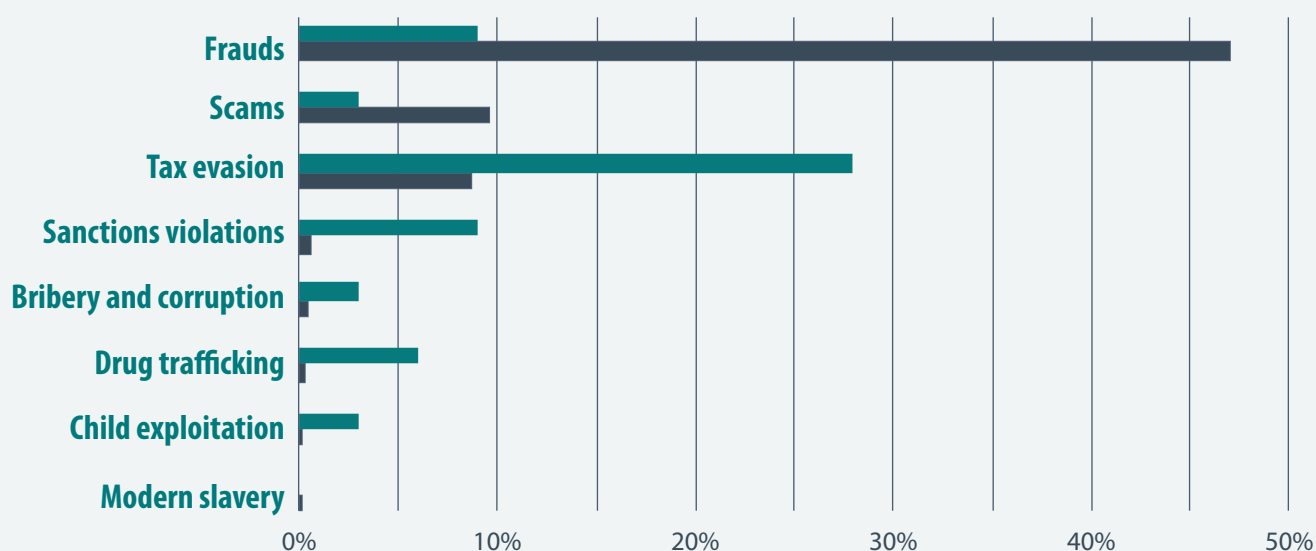
- a customer conducting international funds transfers to multiple beneficiaries located in the same jurisdiction that is deemed higher risk for terrorism financing
- unusual or unusually large cash withdrawals after a financial institution refused to conduct an international transfer to a jurisdiction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

## PREDICATE OFFENCES

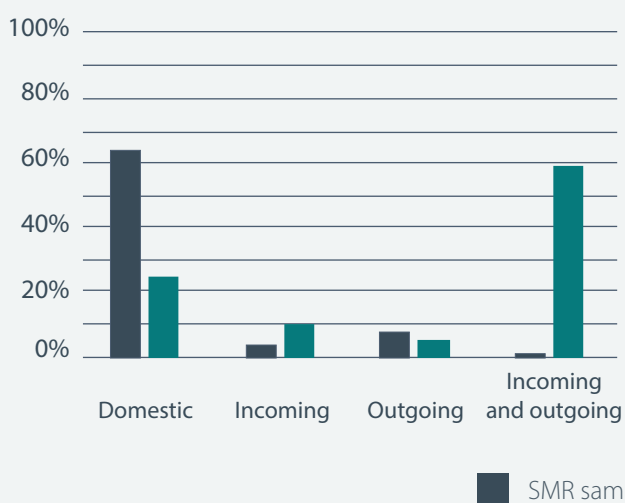
AUSTRAC assesses the nature and extent of threat posed by predicate offending involving foreign subsidiary banks as **high**.

This assessment is based on the SMR sample and consultations with partner agencies.

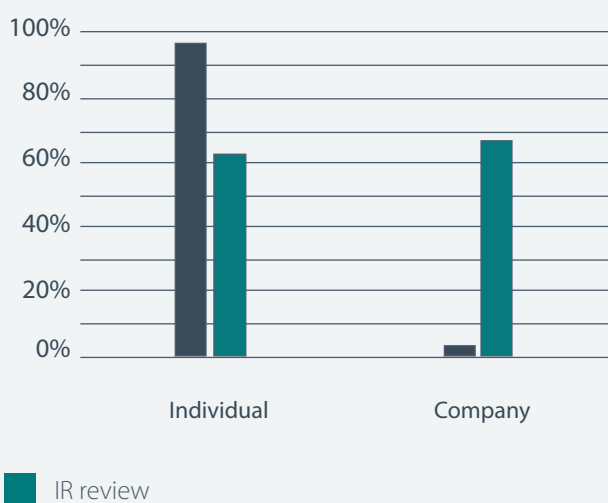
Key offences include frauds, scams and tax evasion. To a lesser extent, the subsector is also exposed to other high-impact offences like sanctions violations, bribery and corruption, drug trafficking and child exploitation. Foreign subsidiary banks may also be exposed to modern slavery, firearms trafficking and environmental crimes given the size of the customer base and retail banking products that are vulnerable to misuse. However these offences were not identified in the SMR sample or IR review.



### PREDICATE REPORTS: DIRECTION OF FUNDS



### PREDICATE REPORTS: CUSTOMER TYPE





## IDENTIFYING PREDICATE OFFENCES – A CHALLENGE FOR REPORTING ENTITIES

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

 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

### FRAUD

Frauds were identified in 47 per cent of the SMR sample and nine per cent of the IR review. While most frauds were relatively simplistic in nature, a few were more sophisticated and had potentially significant consequences. Identity fraud was most common (70 per cent), followed by loan application fraud (16 per cent). The exact nature of fraud activity was not known or reported in a number of SMRs. These reports were often submitted by foreign subsidiary banks after being notified by another financial institution that their customer had received fraudulent funds and no further details were given.

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

- cyber-enabled activity, particularly in relation to fraudulent account openings
- the use of stolen identity documents to establish a banking profile and open new accounts – criminals then used these accounts for money mule purposes
- the use of stolen identity documents to gain access to existing bank accounts followed by theft of funds
- 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 or non-existent property
- the use of specific email domains with fewer security features.

Loan application fraud was often enabled by fraudulent identity documents. These frauds shared the above indicators, as well as forged or altered payslips inflating or ‘staging’ an individual’s income.

Successfully-opened fraudulent accounts were used to layer funds by conducting rapid fund movement to other accounts prior to the fraud being detected. This included flow-through domestic transfers as well as incoming domestic transfers followed swiftly by ATM withdrawals. Reporting entities generally closed these accounts within a short timeframe.

## SCAMS

Scams were identified in nine per cent of the SMR sample and three per cent of the IR review. Many reports were the result of other financial institutions advising a reporting entity that one of their customers had been involved in a scam, whether implicit or not. The exact nature of scam activity was often not known or reported. Where it was identified, phishing and remote access scams were the most common, followed by false-billing scams and romance scams.<sup>20</sup>

### Phishing and remote access scams

Phishing and remote access scams were identified in almost 30 per cent of scam-related SMRs. Common methods involving phishing or remote access scams include:

- stolen funds sent to a third-party account, usually held at another domestic financial institution
- the exploitation of transaction accounts
- the use of public domain email addresses, malware, and encrypted, self-destructing messaging services
- cash withdrawals, often immediately following the receipt of scam funds
- rapid movement of funds, exploiting accounts before foreign subsidiary banks recognise suspicious behaviour and close accounts.

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

### False-billing scams

False-billing scams were identified in approximately 20 per cent of scam-related SMRs. Cases involved businesses being issued fraudulent invoices via email, and then paying the invoice to a fictitious account. In some cases, email accounts were hacked. In these instances, methods used were the same as those used in phishing and remote access scams.

### Romance scams

Romance scams were identified in approximately 13 per cent of scam-related SMRs. In most cases, the customer was a victim of scam activity. However, transaction accounts offered by the subsector were also used to facilitate a scam or launder the proceeds of a scam. Common themes included:

- outgoing international funds transfers, usually to a higher-risk jurisdiction
- use of transaction accounts for money mule purposes.

Although reporting entities and law enforcement agencies often advised targeted customers they were victims of a romance scam, this was often denied or ignored. In some instances, customers responded by trying to obfuscate their transactions from the bank by withdrawing funds in cash or transferring funds to other external accounts. This behaviour raised further red flags for reporting entities.

<sup>20</sup> 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, 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.

**i** AUSTRAC acknowledges that fraud and scam threats are continually evolving. Foreign subsidiary 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 fraud and scam-related activity in SMRs.

## TAX EVASION

Tax evasion was identified in nine per cent of the SMR sample and 28 per cent of the IR review. In the SMR sample, suspected personal income tax evasion was most commonly reported, followed by corporate tax evasion and other tax-related offences.<sup>21</sup> In the IR review, the volume of suspected personal income and corporate tax evasion was equal. Despite comprising a much smaller customer base, AUSTRAC assesses corporate tax evasion likely poses the same level of risk as personal income tax evasion given associated values are often much larger.

### Personal income tax evasion

The volume of suspected personal income tax evasion observed in reporting is consistent with the high proportion of individual customers in the subsector. Associated values varied but the average value of SMRs was relatively high at \$160,217. Common themes in the SMR sample include:

- the use of non-resident accounts to receive rental income, business income or suspicious cash deposits
- transactions and movement of funds inconsistent with the customer profile
- transactions to higher-risk jurisdictions, including tax secrecy jurisdictions
- a high volume of cash
- structuring.

<sup>21</sup> SMRs were assessed as 'other tax evasion' when a judgement could not be determined clearly identifying either corporate or personal tax evasion. Examples include suspicion formed on complex attempts to circumvent tax obligations involving multiple parties; attempts to preserve undeclared assets/wealth often located offshore and scenarios where a customer was evasive with the provision of tax information.

### Corporate tax evasion

The volume of suspected corporate tax evasion observed in reporting is surprising given the small number of non-individual customers in the subsector. In addition, the average value of SMRs relating to suspected corporate tax evasion was high at \$561,581, suggesting the potential impact from corporate tax evasion can be significant. Common themes from the SMR sample include:

- payments suspected to be tied to the shadow economy (businesses transacting in cash)
- using personal accounts for a business operation
- involvement of a DNFBP, namely accountants and real estate agents
- transactions and movement of funds inconsistent with a customer's profile or do not make economic sense
- international transfers involving higher-risk jurisdictions
- phoenixing.<sup>22</sup>

**i** AUSTRAC expects foreign subsidiary banks to continue reporting suspicions of personal and corporate tax evasion. In cases involving multiple suspicions relating to one customer, reporting entities should include results of ECDD and financial investigation in their SMR submissions. This information is highly valuable in assisting our partner agencies, including the ATO, in investigating related offending.

### OTHER HIGH-IMPACT PREDICATE OFFENCES

AUSTRAC assesses the subsector is likely exposed to some criminal proceeds generated from high-impact predicate offences, particularly sanctions violations, drug trafficking, child exploitation and bribery and corruption. This assessment is based on the financial scale of these criminal markets, as well as the subsector's retail banking footprint and medium-sized customer base. While these offences did not frequently feature in the SMR sample, they were observed in a small number of intelligence reports.

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

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

<sup>22</sup> 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.



## SANCTIONS VIOLATIONS

Suspected or attempted sanctions violations were observed in less than one per cent of the SMR sample and in nine per cent of the IR review. Transactions are evenly split between incoming and outgoing international funds transfers and usually involve individual customers. While the number of suspected sanctions violations was low relative to other predicate offences, associated consequences relating to national and international security, and Australia's reputation as a well-regulated financial system, are high.

## SANCTIONS CONTROLS

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

## DRUG TRAFFICKING

Suspected drug use or trafficking was not commonly observed in the SMR sample or IR review. Despite this, AUSTRAC assesses foreign subsidiary banks are exposed to criminal proceeds generated by drug trafficking activities. Australians pay some of the highest prices in the world for illicit drugs, making Australia an attractive market for traffickers. The ACIC estimates Australians spent more than \$11 billion on illicit drugs in 2018-19.<sup>23</sup>

AUSTRAC assesses some of these funds will likely enter the subsector at either placement, layering or integration given the size of the customer base and retail banking products that are vulnerable to criminal misuse.

The data-matching exercise identified approximately \$1.6 million in transactions through foreign subsidiary banks linked to members of national and transnational, serious 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 foreign subsidiary banks. It does not reflect instances of these entities conducting a range of other banking transactions that could be exploited for criminal purposes (e.g. domestic transfers or purchase of assets).

AUSTRAC acknowledges it is very difficult for reporting entities to distinguish transactions linked to drug proceeds from other money laundering activities in the absence of law enforcement information. This almost certainly accounts for the low number of SMRs submitted by foreign subsidiary banks with a direct link to drug activity. SMRs that had a direct link to drug activity were triggered by 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 32 per cent of SMRs that identified money laundering as the only threat are linked to drug proceeds.

<sup>23</sup> 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).

## BRIBERY AND CORRUPTION

Bribery and corruption were observed in less than one per cent of the SMR sample and three per cent of the IR review. Reporting often involved foreign-based entities, including PEPs, and most SMRs were submitted following a law enforcement enquiry or identification of a related party on a watch list or in adverse media reporting. There was an even split of incoming and outgoing international funds transfers, and suspicion almost always related to offshore activities.

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>24, 25</sup>

**i While detected and suspected instances of bribery and corruption are low, foreign subsidiary banks should remain vigilant, particularly given their high exposure to foreign entities and PEPs. Some foreign subsidiary banks have more mature anti-bribery and corruption controls in place as a result of the extra-territorial obligations arising from AML/CTF legislation in their country of incorporation.**

## CHILD EXPLOITATION

Misuse of foreign subsidiary banks to fund child exploitation activities was observed in an extremely small number of SMRs and reports in the IR review. SMRs are generally submitted following adverse media reporting involving a customer. While not specific to the subsector, banks are used to facilitate payments for access to child exploitation material, as well as to facilitate 'grooming' and child sex tourism. Offenders often use various reporting entities across the banking and remittance sectors to make offshore payments to try and avoid being detected.

### 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.

<sup>24</sup> Transparency International, *Corruption Perception Index 2019: Asia Pacific*, 23 January 2020. Viewed: 9 November 2020, [www.transparency.org/en/news/cpi-2019-asia-pacific](https://www.transparency.org/en/news/cpi-2019-asia-pacific).

<sup>25</sup> 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).

## 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>26</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>27</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>28</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>29</sup>

Financial information provided by reporting entities plays a key role in combating modern slavery. While not specific to foreign subsidiary banks, analysis of AUSTRAC data:

- led to the conviction of an individual running a business involving sexual servitude in July 2019
- identified a syndicate that transferred more than \$1 million to a jurisdiction of interest over a 12-year period in order to facilitate human trafficking for the purposes of sexual services.

## FIREARMS TRAFFICKING AND ENVIRONMENTAL CRIMES

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

### 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>30</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>31</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.

26 For more see: [homeaffairs.gov.au/criminal-justice/Pages/modern-slavery.aspx](http://homeaffairs.gov.au/criminal-justice/Pages/modern-slavery.aspx).

27 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](http://aic.gov.au/publications/sb/sb16).

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

29 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](http://aph.gov.au/Parliamentary_Business/Committees/Joint/Foreign_Affairs_Defence_and_Trade/ModernSlavery/Final_report).

30 ACIC, *Illicit firearms in Australia*, 2018, page 7, [aic.gov.au/publications/unclassified-intelligence-reports/illicit-firearms-australia-report](http://aic.gov.au/publications/unclassified-intelligence-reports/illicit-firearms-australia-report).

31 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, [aic.gov.au/about-crime/crime-types/illicit-firearms](http://aic.gov.au/about-crime/crime-types/illicit-firearms).

## Environmental crimes

Environmental crimes incorporate an array of offences, including wildlife trafficking, logging and the dumping of illegal waste, among others. These offences can generate significant illicit profits and attract lower criminal penalties than other crimes, making them lucrative for criminals. The value of proceeds generated from environmental crimes in Australia is unknown. The United Nations Environment Programme and INTERPOL estimate the global market is worth in excess of US\$91 billion, making it the fourth most profitable crime type in the world.<sup>32</sup>

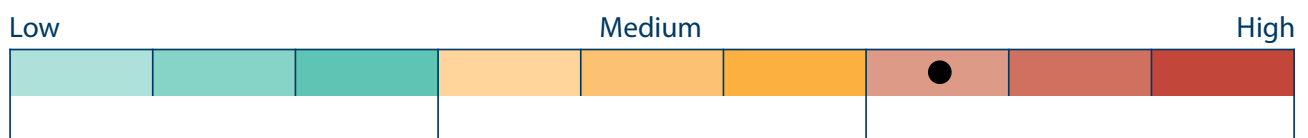
Wildlife trafficking is of particular concern in Australia. Traffickers often sell native wildlife to overseas buyers, where they can receive significant mark-ups. Animals can be sold to breeding facilities in foreign jurisdictions, where they are 'laundered' and then on-sold.

 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>32</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).

# VULNERABILITIES



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



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

AUSTRAC assesses that foreign subsidiary 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 sections:

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

## CUSTOMERS

AUSTRAC assesses the foreign subsidiary bank subsector's customer base presents a **medium** level of inherent ML/TF vulnerability. Vulnerability largely stems from the size of the customer base and the subsector's exposure to higher-risk customers.

### SIZE OF THE CUSTOMER BASE

Foreign subsidiary banks have a moderately-sized customer base. They provide services to approximately 4.8 million customers and hold \$102 billion in residential deposits and \$195 billion in residential assets.<sup>33</sup> Based on feedback provided by foreign subsidiary banks, the subsector is likely to experience gradual growth over the next five years as some reporting entities expect to expand retail business banking and lending services and enhance digital banking services.

Foreign subsidiary banks predominantly service individuals (including sole traders), which can pose a lower ML/TF risk compared to corporate, trust or other legal entity customers – which provide greater scope to obscure beneficial ownership, the source of funds or the purpose of transactions. Most foreign subsidiary banks report that between 80 and 99 per cent of their customer base is comprised of individual customers.

## HIGHER-RISK CUSTOMERS

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




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

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

33 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).

## 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 a small number of known and suspected criminal customers present a high inherent ML/TF vulnerability to the subsector. This assessment is based on the results of the data-matching exercise that identified the proportion of customers who were:<sup>34</sup>

- recorded as a member of a significant national or transnational serious 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>35</sup>
- charged with a terrorism-related offence between 1 January 2014 and 31 December 2018.<sup>36</sup>

Data-matching indicated that a low proportion of individuals charged with money laundering or terrorism financing-related offences were customers of the subsector. Transactions involving these individuals were generally low value. Likewise, there was a low proportion of significant national or transnational criminal group members that were identified as customers of the subsector. The most common transactions linked to these individuals were IFTIs involving Hong Kong Special Administrative Region of the People's Republic of China (Hong Kong SAR), the United Kingdom (UK), the United States of America (USA), Singapore and Lebanon.

### DISPLACEMENT OF HIGHER-RISK CUSTOMERS TO FOREIGN SUBSIDIARY BANKS

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

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

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

<sup>34</sup> This analysis was completed on IFTIs, TTRs and SMRs submitted by foreign subsidiary 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>35</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>36</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>37</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. While not specific to the foreign subsidiary bank subsector, PEP customers have used family members to receive illicit funds through international transfers. In some cases, these funds have been used to purchase real estate or enable gambling activity in Australia.

AUSTRAC assesses a very small number of PEP customers likely pose a high ML/TF vulnerability to foreign subsidiary banks. The subsector reports a very small number of PEP customers, most of whom are based overseas. Consistent with their PEP customer base, most PEP-related reports in the SMR sample pertained to foreign-based individuals. Approximately half of these reports involved suspicion of bribery and corruption.

**i Foreign subsidiary banks should remain vigilant to the risks posed by PEPs, and continue to apply elevated risk mitigation strategies and report all suspicious related activity in SMRs.**

## 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.<sup>38</sup>

Combined, foreign subsidiary banks service a small number of companies, trusts and other legal entities. These customers were reported in approximately six per cent of the SMR sample, and were primarily linked to suspected money laundering and corporate tax evasion activities. These reports often involved foreign-based entities, including companies domiciled in higher-risk jurisdictions as well as the use of suspected offshore shell and shelf companies.

37 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.

38 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).

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

- There are limitations in the identity verification process when registering a company in Australia. This can create opportunities for criminals to use stolen identities to establish a company that is subsequently used to launder criminal proceeds.
- Criminal entities often appoint a family member or 'cleanskin' associate as a director or shareholder to distance themselves from the purportedly legitimate entity.<sup>39</sup>
- Australian companies can be registered by foreign nationals. Transnational, serious organised crime groups exploit this vulnerability by compelling individuals on temporary visas to register companies that are subsequently used to place, layer and integrate illicit funds.
- Criminals may own or control multiple companies that are registered or operate in various jurisdictions. Banking arrangements linked to these companies are then used to facilitate global movement of funds and evasion of taxation obligations.

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

**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 PROFESSIONALS**

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

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

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

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


<sup>39</sup> A 'cleanskin' is a person without a criminal history nor identifiable links to criminals who acts on behalf of a criminal entity in order to provide a veneer of legitimacy to such activities.

AUSTRAC assesses a small number of high-risk DNFBPs will present ongoing ML/TF risk to the subsector. This assessment is based on a limited number of reports in the SMR sample and partner agency information that suggests known criminal exploitation by DNFBPs in the subsector is minimal. In the reporting period, less than three per cent of the SMR sample identified a DNFBP. These reports outlined suspected money laundering by accountants and real estate agents, and largely involved either incoming international transfers and/or at least one cash transaction.

### 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 looking to engage in criminal activity. 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 foreign subsidiary banks to facilitate tax evasion and the movement of funds internationally. AUSTRAC expects foreign subsidiary banks to report any suspicions of professional facilitators or enabling parties to illicit activity, and encourages mature risk mitigation strategies for limiting insider threats.

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

### FOREIGN-BASED CUSTOMERS

During consultations, reporting entities highlighted foreign-based customers as posing a higher ML/TF risk than Australian-based customers. The major ML/TF vulnerabilities relate to onboarding and local risks posed by a customer’s residential location, as reporting entities rely on their foreign counterparts to conduct know your customer (KYC) and CDD checks. These processes can vary in effectiveness and unwittingly expose a bank to a criminal entity.

Foreign-based entities were observed in approximately nine per cent of the SMR sample. Most reports related to suspected money laundering (72 per cent) and involved individual customers making suspicious domestic funds transfers, or international transfers involving China and Hong Kong SAR.



## TEMPORARY VISA HOLDERS

### Visitor visa holders

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

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

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

## MITIGATING EXPLOITATION BY VISITOR 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 temporary visa.

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

### Student visa holders

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

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

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

## FINANCIAL INSTITUTIONS

While limited in number, financial institution customers may pose a higher ML/TF vulnerability to foreign subsidiary banks. 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 foreign subsidiary bank to many underlying customers. Foreign subsidiary 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. Some financial institution customers may expose foreign subsidiary banks to a high volume of cash transactions, particularly if they allow their underlying customers to make deposits into an account held by a foreign subsidiary 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.

### Correspondent banking services

Foreign subsidiary banks also count some offshore financial institutions as customers through the provision of correspondent banking services.<sup>40</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.

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.

40 Correspondent banking is the provision of banking services by one bank (the correspondent bank) to another bank (the respondent bank).

**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>41</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 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.

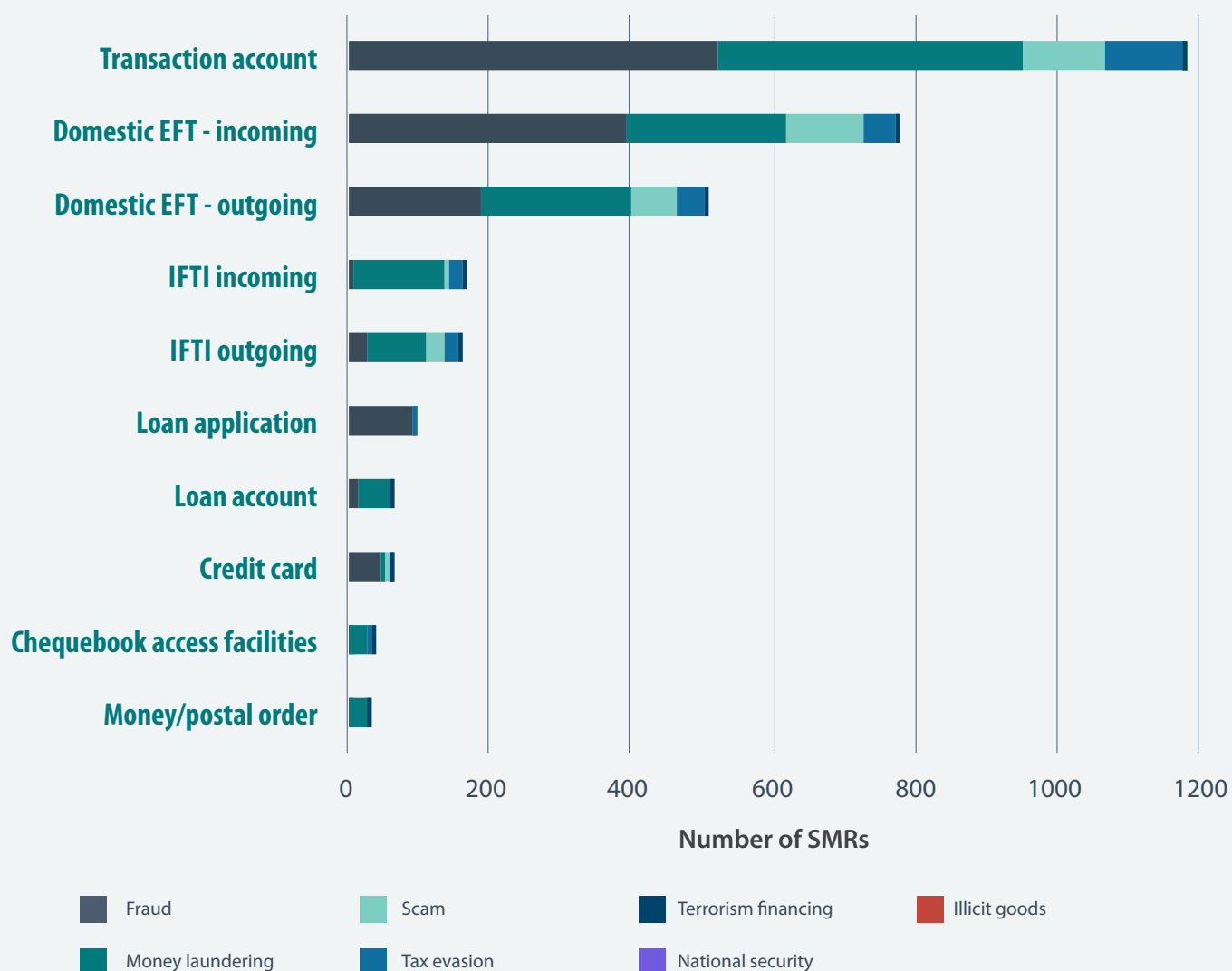
Legislation under the *Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Act 2020* strengthen protections on correspondent banking. The new measures prohibit financial institutions from entering into a correspondent banking relationship with another financial institution 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.

 **AUSTRAC recommends foreign subsidiary banks continue to conduct risk assessments aligned with FATF guidelines on correspondent banking services and the AML/CTF Act.**

<sup>41</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.

## PRODUCTS AND SERVICES

### MOST COMMON PRODUCTS OR SERVICES AND THREAT – SMR SAMPLE



AUSTRAC assesses the nature and extent of products and services offered by the foreign subsidiary bank subsector pose a **high** inherent ML/TF vulnerability.

Foreign subsidiary banks have a high exposure to cash. While dealing with cash transactions is an inherent part of banking operations, it also increases the industry's exposure to the proceeds of crime, 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.

The subsector also offers a variety of products and services that can be used to store and move illicit funds. Those most vulnerable to ML/TF include transaction accounts, credit card accounts and savings accounts.

Across the subsector, the extent of cash exposure for individual reporting entities varies:

- Three reporting entities operate a branchless model and facilitate cash transactions through agent banking relationships only. Agent banking relationships expose reporting entities to separate ML/TF vulnerabilities, which are discussed on page 57.
- Four reporting entities operate a combined total of 69 branches across Australia. Two of these reporting entities also offer a combined total of 68 ATMs.

In the reporting period, 18,836 TTRs were submitted by these reporting entities for a total value of approximately \$317 million. However, the total value of cash transactions is higher given TTRs are not submitted for transactions under the \$10,000 reporting threshold. Transactions below this threshold are also vulnerable to ML/TF misuse as criminals structure deposits to avoid reporting obligations.

## USE OF CASH

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

- Total number of TTRs submitted to AUSTRAC: **18,836**
- Total cash value of TTRs: **\$317.2 million**
- Largest cash deposit: **\$437,195**
- Largest cash withdrawal: **\$333,034**
- Total number of cash-related SMRs: **1,112**
- Total value of cash-related SMRs: **\$39.7 million**

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

### SUSPICIOUS CASH TRANSACTIONS

Nearly half (42 per cent) of the reports in the SMR sample involved a suspicious cash transaction. The total cash value of these reports was approximately \$40 million. Suspicious cash transactions most often involved ATM withdrawals followed by face-to-face cash deposits (see table below). Money laundering was the most common suspected threat (which is discussed in detail on page 23), followed by tax evasion. Other themes of suspicious cash transactions include:

- rapid transfer of funds following deposit (suspected layering activity)
- 13 per cent involved at least one IFTI - China, Hong Kong SAR, Nigeria, USA and Singapore were most often noted
- seven per cent involved overseas cash withdrawals – primarily in Malaysia.

### CASH-RELATED TRANSACTIONS IN THE SMR SAMPLE (%)<sup>42</sup>

TYPE OF TRANSACTION	ATM	IN-BRANCH	UNSPECIFIED	OVERSEAS
Deposit	14	59	8	-
Withdrawal	76	30	5	7
Cash payment	-	-	1	-
Undeclared cash	-	-	2	-

### PUSH AND PULL FACTORS ON CASH USE

As electronic payments become more popular, cash use is in steady decline in Australia. The Reserve Bank of Australia calculates that cash payments as a share of consumer payments have more than halved between 2010 and 2019.<sup>43</sup> The number of foreign subsidiary bank SMRs containing a suspicious cash transaction have also declined, from 67 per cent of SMRs in 2013-14 to 42 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>44</sup> Overall, the Reserve Bank noted a “substantial increase in high-value cash withdrawals at branches” in the first half of 2020.<sup>45</sup>

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

<sup>42</sup> SMRs often note several types of suspicious transactions. Therefore the total per cent of reports noted in each category may exceed 100.

<sup>43</sup> 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://www.rba.gov.au/speeches/2020/sp-ag-2020-06-03.html).

<sup>44</sup> T Richards, C Thompson and C Dark, *Retail central bank digital currency: Design considerations, rationales and implications*, Reserve Bank of Australia, 2020, page 31, [rba.gov.au/publications/bulletin/2020/sep/pdf/retail-central-bank-digital-currency-design-considerations-rationales-and-implications.pdf](https://www.rba.gov.au/publications/bulletin/2020/sep/pdf/retail-central-bank-digital-currency-design-considerations-rationales-and-implications.pdf).

<sup>45</sup> L Delaney, N McClure and R Finlay, *Cash Use in Australia: Results from the 2019 Consumer Payments Survey*, Reserve Bank of Australia, 2020, page 50, [rba.gov.au/publications/bulletin/2020/jun/pdf/cash-use-in-australia-results-from-the-2019-consumer-payments-survey.pdf](https://www.rba.gov.au/publications/bulletin/2020/jun/pdf/cash-use-in-australia-results-from-the-2019-consumer-payments-survey.pdf).



## **ABILITY TO STORE AND MOVE FUNDS OR 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, foreign subsidiary banks offer hundreds of products and services. The extent of product offerings is a vulnerability in itself. Criminals are known to probe the features of similar products to find gaps and inconsistencies to exploit for illicit purposes.

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

- transaction accounts
- credit card accounts
- savings accounts.

While there were no known or suspected cases of criminal misuse involving trade finance facilities in the reporting period, industry representatives consider these products highly vulnerable to ML/TF. This is particularly true given the potentially large values of associated transactions. While few foreign subsidiary banks offer trade finance, those that do should apply appropriate enhanced customer and transaction due diligence and post-transaction monitoring processes to detect suspicious or unusual activity. Indicators of trade finance-based money laundering (and TBML more generally) are discussed on page 24.

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

To better assess the inherent vulnerability of products and services offered by foreign subsidiary banks, AUSTRAC developed a product risk matrix (the matrix). The results and ratings from this exercise can be found in the table on page 52.

**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 foreign subsidiary banks' responses to the perceived inherent vulnerability of their products or services across four ML/TF risk factors:
  - the extent to which cash can be placed using the product or service
  - the extent to which funds or value can be stored using the product or service
  - the extent to which funds or value can be moved domestically using the product or service
  - the extent to which funds can be moved overseas using the product or service.
2. The detected exploitation rating assesses the known or suspected criminal misuse of a product or service category. This was determined by analysing information from the SMR sample, IR review and survey responses from partner agencies.
3. The value of median transaction indicates the median amount of funds flowing through a product or service and was determined by data provided by foreign subsidiary 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 foreign subsidiary banks.

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

Discussion is then provided on the three product and service categories that had the highest overall rating only.

## PRODUCT AND SERVICE VULNERABILITY RATINGS

PRODUCT/SERVICE	VULNERABILITY PERCEPTION RATING	DETECTED EXPLOITATION	VALUE OF MEDIAN TRANSACTION	TRANSACTION VOLUME	OVERALL RATING
Transaction accounts		High	\$\$	Medium	
Credit cards		Medium	\$	N/A	
Savings accounts		N/A	\$\$	Medium	
Chequebook access		Low	\$\$	Low	
Trust accounts		High	\$	Low	
Correspondent banking		High	\$	Low	
Business loan account		Medium	\$\$	Low	
Home loan account		Medium	\$\$\$	Low	
Trade finance		Medium	\$\$\$	Low	
Personal loan account		Medium	\$	N/A	
Foreign currency accounts		Low	\$	Low	
Term deposits		Low	N/A	Low	
Store value cards		Medium	\$	Low	
Loan offset accounts		Low	\$	Low	
Foreign currency exchange services		Low	\$	Low	
Asset financing		Low	N/A	Low	

**TRANSACTION ACCOUNTS**

Transaction accounts are one of the most commonly misused financial products for money laundering and other financial crimes because they enable fast and effective storage and movement of funds, both domestically and internationally. Transaction accounts can facilitate all stages of the money laundering process and appear in a wide range of established money laundering methodologies. Partner agencies rate them as the highest-risk product offered by all banks.

Transaction accounts were identified in 86 per cent of the SMR sample. Key themes include:

- suspicious domestic funds movements (see table below), likely associated with layering activity
- use of non-resident accounts in reports relating to suspected tax evasion
- threats associated with individual customer accounts include frauds, scams, tax evasion and money laundering
- threats associated with company customer accounts include frauds, scams, phoenixing, co-mingling, use of shell companies and complex offshore company structures.

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

TRANSACTION TYPE	% OF SMRs
Domestic electronic funds transfer into account	58
Domestic electronic funds transfer out of account	37
Cash withdrawal	33
Cash deposit	19
International funds transfer into Australia	13
International funds transfer out of Australia	11

**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 do 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, 12 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, 15 per cent of reports relating to loan application fraud involved a credit card account.
- Allowing international transactions, including offshore cash withdrawals, which can be funded by onshore third-party cash deposits.

### SAVINGS ACCOUNTS

In general, high-yield savings accounts operate in much the same way as transaction accounts. However, they are associated with incentives such as higher interest rates and early withdrawal penalties to encourage customers to deposit heavily and withdraw sparingly. Despite this, savings accounts are open to criminal exploitation as they allow quick storage and access to funds, with the ability to move funds with relative ease. Additionally, higher interest rates may be attractive to an entity that is prepared to wait long periods of time before accessing funds.

Savings accounts were noted in one per cent of the SMR sample.<sup>46</sup> The reason for suspicion often related to unknown source of funds and rapid movement of funds, particularly following a deposit to a linked account.

---

<sup>46</sup> Savings accounts were not specifically labelled in the SMR sample. This figure was derived using keyword analysis of the SMR sample and likely under-represents the actual number of reports relating to savings accounts.

## DELIVERY CHANNELS

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

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

### LEVEL OF CUSTOMER CONTACT

The level of customer contact varies significantly across the subsector. For example, four reporting entities have a branch presence in Australia and offer in-branch services, while three reporting entities operate a remote service model. Compared to Australia's domestic banks, foreign subsidiary banks have a small ATM and branch network, and largely rely on other delivery channels to service their customers. This includes phone, online and through third-party arrangements.

The trend towards more remote and streamlined 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

Foreign subsidiary banks that operate branches are exempt from mandated COVID-19 closures. However, some banks implemented measures to reduce face-to-face contact with customers where possible. For example, banks have encouraged and supported customers to use online banking and have directed relationship managers or brokers to interact with customers over the phone or via videoconferencing where possible.

It is likely these changes will accelerate the trend away from face-to-face product delivery and towards online banking, particularly as more customers become accustomed to these channels.

#### 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. They allow for the withdrawal of cash, which can facilitate the layering and integration of funds, and cash deposits, which can be used to place criminal proceeds into the financial system and are highly vulnerable to criminal misuse.

Across the subsector, the number of ATMs owned and operated by foreign subsidiary banks is low. This includes a combined total of 68 ATMs operated by just two reporting entities. However, all ATMs are equipped as 'intelligent deposit machines' (IDMs), which introduce unique ML/TF vulnerabilities (see below). In addition, customers of foreign subsidiary banks that do not offer ATM facilities can access ATMs operated by some domestic banks through agent banking relationships. ML/TF vulnerabilities introduced through these relationships are discussed on page 57.

ATM transactions were identified in 27 per cent of the SMR sample. Of these reports, suspicious withdrawals were most commonly noted, often in connection with rapid movement of funds and structuring activity. Fraud was the primary suspected threat, followed by suspected money laundering.



### 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. While IDMs provide convenience for both the bank and the customer, they also expose banks to unique ML/TF vulnerabilities compared to in-branch deposits and their use can make it harder to identify criminal proceeds. For example, IDMs allow cardless cash deposits to be made by anonymous third parties. In such instances, the only identifying information collected is a mobile number. IDMs also reconcile deposits to accounts in real time without the need for human intervention, and those located outside of a branch can be used 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>47</sup>

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

### 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.

During industry consultations, reporting entities acknowledged the vulnerabilities associated with anonymous cash channels as one of their highest ML/TF risks. To counter this, the subsector introduced a range of limits on cash deposits (between \$1,000 and \$10,000), which are often subject to internal review and modification in an effort to mitigate 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 the banking system.

### ONLINE BANKING

The vast majority of transactions facilitated by foreign subsidiary banks originate online – either through banking apps or through websites. A significant and increasing number of products can also be applied for online.

While this trend is driven by consumer demand for faster, more convenient banking options, the increasingly online nature of bank transactions introduces significant 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 move funds through multiple bank products with separate financial institutions, masking the true source or destination of the funds.

With no face-to-face interactions or CCTV monitoring, online banking also introduces an additional element of anonymity to bank transactions, which can be attractive to criminals. For example, an individual applying for a bank account online may not be subject to visual identification.

Misuse of online banking channels was common in the SMR sample. Nearly all identity fraud (95 per cent) and fraudulent loan applications (98 per cent) occurred through online banking.

### Mobile banking applications

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

**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.

<sup>47</sup> The New Payments Platform is discussed on page 58.

## COMPLEXITY OF PRODUCT DELIVERY ARRANGEMENTS

Given the subsector's limited branch network, reporting entities outsource certain banking services to other financial institutions and non-ADI third parties to meet their customers' needs. This process is known as agent banking and can include transactions such as deposits and withdrawals.

While outsourcing to third parties can provide advantages such as greater accessibility for customers and improved services, using third parties can create vulnerabilities in the ability to detect and act upon suspicious activity. Reporting entities are ultimately responsible for the behaviour and compliance of third-party agents and brokers.

### AGENT BANKING ARRANGEMENTS

An agent banking arrangement consists of:

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

While these arrangements provide a higher degree of access to customers' 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 foreign subsidiary bank, which may create difficulties for transaction monitoring and establishing appropriate governance frameworks to manage ML/TF risks
- limiting the ability for reporting entities 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
- 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.

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

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

### THIRD-PARTY ELECTRONIC BILLERS

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

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

**i Customers seeking to receive third-party biller payments must have an ABN or ACN with incoming payments into a transaction account indicative of business earnings. This is a good starting point for commencing ECDD if the transaction account is held by an individual whose recorded occupation is inconsistent with such 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>48</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 foreign subsidiary banks complete a risk assessment to fully understand the implications of using overlay services and adjust systems and controls accordingly.**

### CONSUMER DATA RIGHT – OPEN BANKING

The Consumer Data Right is a framework designed to enhance a consumer's ability to access the data businesses hold about them and authorise this data to be shared with accredited third parties. The first sector to which the Consumer Data Right applies is the banking sector (also known as Open Banking). Open Banking is designed to encourage greater competition, efficiency and the creation of more tailored products and services. The regime is currently undergoing a phased rollout and individual foreign subsidiary banks are at various stages of this process. At least one reporting entity has already made available product details, such as interest rates, fees and features, while others are still working towards implementation.

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. This disaggregation of transactions across multiple financial services providers reduces a reporting entity's 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.

<sup>48</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. For more see: [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).

## FOREIGN JURISDICTIONS

AUSTRAC assesses foreign subsidiary banks have a **high** inherent ML/TF vulnerability to foreign jurisdiction risk.

Foreign subsidiary banks are widely exposed to foreign jurisdictions, including higher-risk jurisdictions, because of the nature of their business operations and the volume of international funds transfers they facilitate. The parent companies of all foreign subsidiary banks are headquartered overseas, with most domiciled in global financial centres or jurisdictions associated with money laundering, terrorism financing or tax evasion activities.<sup>49</sup>

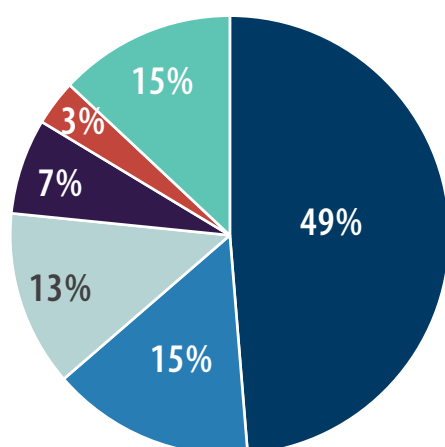
Exposure to foreign jurisdictions poses ML/TF risk because it creates opportunities for international movement of criminal proceeds and the funding of overseas terrorist activity. Further, transactions with foreign jurisdictions add complexity, helping to obscure beneficial ownership and beneficiary customers, and increase potential for offshore tax evasion. This is particularly true when funds have transited through third countries, such as global financial centres. 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

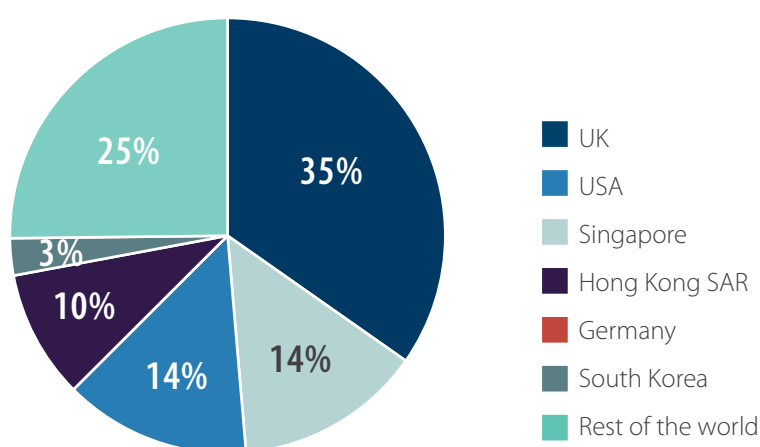
Foreign subsidiary banks facilitate the movement of a large volume of funds into and out of Australia. In the reporting period, the subsector submitted almost two million IFTIs, with a total value of \$844 billion.<sup>50</sup> Incoming funds accounted for 69 per cent of the total value. Almost two-thirds of these transactions were facilitated by one reporting entity. Two reporting entities do not process international transactions.

International transactions were identified in about 25 per cent of the SMR sample. The top five jurisdictions in the SMR sample were China, Hong Kong SAR, Malaysia, Nigeria and USA. Three of these jurisdictions (China, Hong Kong SAR and USA) appear in the top five source or destination jurisdictions by IFTI value, suggesting over-represented suspicious activity in Malaysia and Nigeria. The main threat types identified in the reports were fraud, money laundering, scams and tax evasion.

Incoming IFTIs (\$)



Outgoing IFTIs (\$)



<sup>49</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>50</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. Due to rounding of figures, total percentages depicted in the pie charts above exceed 100.

## TRANSACTIONS WITH HIGHER-RISK JURISDICTIONS

A very large proportion of IFTIs submitted by the subsector involved a higher-risk jurisdiction, in particular a significant volume of funds flows through global financial centres. In total, 87 per cent of IFTIs reported involved a higher risk jurisdiction.<sup>51</sup>

Incoming international funds transfers from jurisdictions considered higher risk for money laundering and tax evasion were most common. This is likely consistent with the broader customer base and their financial interests in Australia. For example, investment in Australia, onshore business operations, transfer of personal wealth, or supporting family members.

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

As all reporting entities are different, foreign subsidiary banks need to consider the products and services they provide, the arrangements they have with their service delivery partners, the nature of their customer base and the purpose of their customers' transactions to assess which foreign jurisdictions pose a high ML/TF risk to them.

## GLOBAL FINANCIAL CENTRES

Four jurisdictions considered high risk for money laundering in this report are also home to the world's top four financial centres as ranked by the Global Financial Centres Index. These jurisdictions are hubs of financial trade and house the headquarters of many large corporations (as well as some foreign subsidiary banks). The result is a significant amount of financial flows into and out of these jurisdictions to support commercial activity. In the reporting period, approximately 81 per cent of IFTIs submitted by the subsector involved a global financial centre. Such vast transactional volumes allow criminals to obscure the movement of illicit funds among legitimate financial activity.

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

<sup>51</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.

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.

## 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



71%



29%

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



51%



49%

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



66%



34%

Jurisdictions considered higher risk for tax evasion



55%



45%

Jurisdictions considered higher risk for terrorism financing



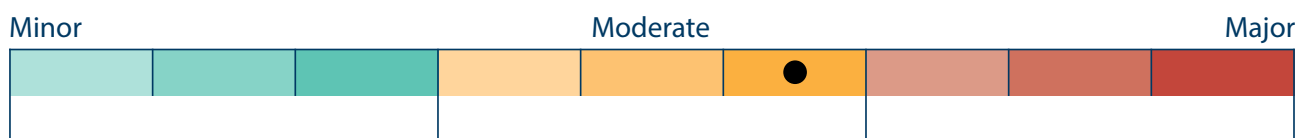
45%



55%

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 foreign subsidiary banks is **moderate**. Consequences include the potential impact or harm that ML/TF and other financial crimes may cause.

Financial crime that impacts foreign subsidiary banks has consequences for customers, individual reporting entities, the subsector as a whole, and the broader Australian and international community. The exploitation of foreign subsidiary 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 foreign subsidiary banks has **moderate** consequences for customers of the subsector.

Foreign subsidiary banks report varying degrees of impact criminal activity can have on their customers. This depends on the type of customer, their ability to detect criminal exploitation and their capacity to absorb potential financial losses. For example, larger, more sophisticated customers such as corporations are better placed to detect and prevent criminal exploitation or absorb financial losses. The prevalence of individual customers versus corporate customers, makes it likely the subsector will experience more instances of fraud and scams.

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

Impacts of criminal activity on customers can include:

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

## INDIVIDUAL REPORTING ENTITIES AND THE SUBSECTOR

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

Most foreign subsidiary banks report criminal activity can have a moderate to major impact on their Australian operation, as well as their broader business group. The level of impact is largely influenced by the type and extent of criminal exploitation. Most reporting entities note criminal exploitation has largely had low to moderate consequences. However, they acknowledge systemic criminal exploitation would likely have major consequences for their business.

The subsector may experience heightened criminal targeting should criminal entities identify certain foreign subsidiary banks with insufficient AML/CTF programs. For smaller foreign subsidiary banks that do not have a large community customer base and entrenched community ties, the impacts from criminal targeting are likely to be more severe.

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

Financial costs may include:

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

Reputational costs may include:

- damage to relations with head office or overseas branches
- damage to brand
- dissatisfaction or loss of investors, customers or partners
- reduced ability to attract investment and business, and skilled staff.

Operational impacts may include:

- heightened regulatory oversight or law enforcement action
- civil or criminal penalties in the event of serious non-compliance
- loss of staff or change of senior management personnel
- decision by head office to withdraw operations from the Australian market.

## AUSTRALIAN FINANCIAL SYSTEM AND COMMUNITY

AUSTRAC assesses that ML/TF and predicate offences involving foreign subsidiary banks has **moderate** consequences for the Australian financial system and the community.

While foreign subsidiary banks have a smaller financial footprint in Australia compared to other banking subsectors, 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. Likewise, despite the low volume of suspected criminality in the subsector, 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 the community can include:

- societal harm inflicted upon the community through offences such as drug trafficking, child exploitation, frauds and scams
- 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>52</sup>
- widespread or concentrated real estate purchases with the proceeds of crime, driving property prices up and pricing legitimate buyers out of the market.

## NATIONAL AND INTERNATIONAL SECURITY

AUSTRAC assesses that ML/TF and predicate offences involving foreign subsidiary 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 and 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 foreign subsidiary banks can also have consequences for national or international security, especially where they undermine sanctions regimes that are designed to restrain rogue governments or violent non-state actors.

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

<sup>52</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.





# 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.

While most reporting entities indicate they have implemented risk mitigation strategies – including CDD procedures, customer risk rating tools, product controls and transaction monitoring – several acknowledge improvements are required to ensure:

- customer risk ratings are regularly reviewed and updated
- transaction monitoring programs are appropriately tailored and technologically advanced to detect suspicious activities, including transactions made via the NPP
- there are appropriate reconciliation, quality assurance and governance processes in place over enterprise systems and controls

- an ML/TF risk assessment is performed where a new system is introduced or where there is a change in a system, product or service
- enterprise ML/TF risk assessments are tailored to the Australian risk environment
- AML/CTF officers are adequately trained for all specific product and service offerings, and are provided adequate support from head office.

Improvements to the quality and quantity of SMR submissions can also be made across the subsector.



In addition, it is common practice for the offshore head office of a foreign subsidiary bank to develop financial crime programs applicable to its operations in Australia. The level of implementation of ML/TF risk mitigation strategies is therefore largely incumbent on the culture and maturity of AML/CTF processes and programs employed by head office and their understanding of local risks. This is also influenced by the effectiveness of AML/CTF regimes in the jurisdiction where a foreign subsidiary bank is headquartered.

**i Reporting entities must ensure AML/CTF programs incorporate a genuine understanding of the Australian ML/TF risk environment and expand upon any global program.**

## CUSTOMER DUE DILIGENCE

Foreign subsidiary banks employ CDD checks to assess the legitimacy of customers and their business operations. Depending on the product offering, new customer onboarding is conducted either face-to-face by frontline staff or relationship managers, third-party agents or online. Given the online business model of some reporting entities, there is a heavy reliance on software and technology to conduct CDD. Some foreign subsidiary banks also outsource customer onboarding to third parties who collect the relevant customer information and provide it to a centralised operations team to process.

In some instances, new clients are referred from another subsidiary of the parent company and reporting entities rely on customer information previously collected (and update as required). While this may streamline CDD processes for the bank and the customer, reporting entities must ensure they can access this information for audit or compliance purposes, as well as for conducting appropriate ongoing CDD (e.g. change in beneficial ownership of a company customer).

New customers are required to provide proof of identification, business documentation and other requested information. For example, source of funds, customer background and purpose for opening the account, or ultimate beneficial ownership, which is then verified via third-party digital systems. Where electronic verification is not confirmed, customers are required to verify their identification in person. For reporting entities with no branch presence in Australia, this can be done via a third-party agent or a relationship manager.

Foreign-based customers, whether in Australia or abroad, can open accounts but might be classified high-risk and subject to increased CDD and ongoing monitoring. One reporting entity noted they also require foreign-based individual customers to present at an Australian branch to activate their account within six months of account opening. Prior to account activation, funds cannot be moved out of the account. If the customer fails to present within six months, the account will be closed.

All foreign subsidiary banks indicate customers are risk-rated at onboarding. For customers rated high risk, ECDD is generally triggered, senior management approval may be required and ongoing CDD processes may be put in place. In some cases, the customer will not be onboarded (e.g. if the customer is positively identified on a sanctions list, or transacts with specific high-risk jurisdictions).

Most reporting entities indicate customer risk ratings are reviewed periodically, or when a customer triggers an alert. This can include events like changes in customer information or transaction activity. Feedback from industry suggests the sophistication of these review processes vary across the subsector. Some reporting entities use advanced systems that routinely ingest customer information and financial activity, and automatically refresh on a regular basis. Other reporting entities are either not reviewing customer risk ratings or are not reviewing them often enough.

## CUSTOMER RISK RATINGS

Reporting entities are encouraged to review their processes and ensure:

- appropriate mitigation strategies are in place to detect higher-risk customers, including negative news screening and checks against global PEP and sanctions lists
- customer risk ratings are regularly reviewed and updated.

## 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 help prevent exploitation by criminal entities or terrorism financiers. This is particularly important given the high value of transactions processed by the subsector.

Transaction monitoring programs vary in sophistication across the subsector but are generally commensurate with the size, nature and complexity of individual operations. For example, smaller reporting entities that offer relatively few and less complex products often have less sophisticated transaction monitoring programs, while larger operations use well established and widely used third-party applications.

Over half of the foreign subsidiary banks consulted for this report provided a detailed overview of their transaction monitoring programs. All of these entities use automated transaction monitoring programs, and some have manual controls in place to detect unusual activity.

Automated transaction monitoring programs generally include scenario-based profiles, business rules, parameters and alerts adjusted to individual risk profiles to detect suspicious or unusual activity. Following detection, transactions are escalated and analysed to determine their legitimacy. Treatment options can then include:

- delaying transactions until an investigation is complete
- conducting more detailed analysis of transaction monitoring, including transaction patterns
- verifying or re-verifying CDD information
- verifying source of wealth or beneficial ownership
- escalating to senior management.

Transaction monitoring programs need to be regularly reviewed and updated to remain effective. Reporting entities indicate reviews are conducted annually, or when an event triggers a requirement to review a rule.

## INDEPENDENT REVIEWS

All foreign subsidiary banks have their risk management frameworks independently reviewed on a regular basis. AML/CTF policies and programs dealing with material risks are expected to be included in the independent reviews which are conducted by operationally independent, appropriately trained and competent people. This provides an objective mechanism to assess whether AML/CTF programs are appropriate and effective in detecting criminal misuse. In addition, some reporting entities also undergo regular internal audits and reviews by their parent bank that cover AML/CTF policies and programs.

## RISK ASSESSMENT

Across the subsector, there is variation in the sophistication and effectiveness of enterprise risk assessments. Industry feedback highlights gaps in understanding and application of local risks to assessments, with some reporting entities failing to adequately tailor their assessments to the Australian environment.

**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 it reflects the actual risks posed to foreign subsidiary 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

Overall foreign subsidiary banks report a small number of SMRs, particularly given the number of transactions they process, in comparison to Australia's domestic banks. The volume of SMR submissions also varies between individual reporting entities. To some degree, this variation is consistent with differences between reporting entities including their size, customer base and complexity of products and services.<sup>53</sup> However, it also likely reflects varied levels of:

- understanding of ML/TF risks
- effectiveness of CDD, ECDD and transaction monitoring processes
- capacity to conduct financial investigations into flagged transactions and report SMRs to AUSTRAC
- understanding of reporting obligations (e.g. it would be a contravention of the AML/CTF Act if a reporting entity submitted all SMRs in the country of the head office offshore, but failed to also report the matter to AUSTRAC).

There were many examples of good SMR reporting practices from the subsector, with reports including detailed transaction histories, records of contact with the customer or suspicious party, and relevant information uncovered from carrying out ECDD. Many reports evidenced comprehensive investigation and analysis by reporting entities.

<sup>53</sup> For example, foreign subsidiary banks who operate solely online are far more exposed to cyber-enabled criminal activity, and thus report the vast majority of related SMRs.

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 explain what aspects of the transaction(s) or customer behaviour was suspicious and include all information from ECDD activities and financial investigations in the grounds for suspicion.
- **Avoiding trigger-based reporting.** Trigger-based reporting is a practice in which a reporting entity submits an SMR solely on the basis of a trigger generated by their transaction monitoring system without conducting further investigation to form suspicion on reasonable grounds. Similarly, template reporting where there is little unique detail in the grounds for suspicion. Such reports provide little intelligence value and generally cannot be actioned.
- **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.
- **Provide more detail about frauds and scams.** Some reporting entities struggled to identify specific details of fraud and scam activity. While AUSTRAC recognises this can often be due to limited detail being provided by a respondent bank, AUSTRAC encourages follow-up SMR reporting if further detail becomes available.
- **Including documents that provide additional context.** If relevant, include bank statements, CCTV footage, account opening forms or identity verification documents to provide AUSTRAC analysts with a more detailed and complete picture of suspicious transactions while also helping to triage work.

During consultations, some foreign subsidiary bank representatives acknowledged challenges with SMR reporting. AUSTRAC encourages reporting entities to have policies and procedures in place to assist staff to identify and report suspicious matters.

## FURTHER RESOURCES ON SUSPICIOUS MATTER REPORTING

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

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

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

## STAFF TRAINING

Foreign subsidiary banks are required to:

- provide appropriate staff training at appropriate intervals, having regard to ML/TF risk reporting entities may reasonably face
- implement controls to screen prospective employees and rescreen employees who may be in a position to facilitate the commission of a ML/TF offence.

Over half of the foreign subsidiary banks consulted for this report provided a detailed overview of their AML/CTF staff training protocols. All of these reporting entities indicated they meet the minimum standards outlined above. Several reporting entities provided examples of training processes that exceed the minimum standard requirements. For example:

- relevant staff are encouraged to hold professional AML/CTF certification
- dedicated training is provided annually to the Board of Directors.

# APPENDIX A: GLOSSARY

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



NAME	DESCRIPTION
<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.



NAME	DESCRIPTION
<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> <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>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>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>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>Phishing</b>	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.

NAME	DESCRIPTION
<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.
<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>Remote access scam</b>	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.
<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.

NAME	DESCRIPTION
<b>Suspicious matter report (SMR)</b>	A report that must be submitted by a reporting entity under the AML/CTF Act if they have reasonable grounds to suspect that a transaction may be related to money laundering, terrorism financing, tax evasion, proceeds of crime or any other serious crimes under Australian law. An SMR must also be submitted if the reporting entity has reasonable grounds to suspect the customer or an agent of the customer is not who they say they are.
<b>Structuring</b>	Making or receiving a series of cash transactions intentionally structured to avoid going over 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 (TSOC) 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.



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 sector, and low associated values.	Moderate number of money laundering cases in the sector, and moderate associated values.	High number of money laundering cases in the sector, 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 sector.	Terrorist financing methodologies are somewhat varied. There is a small number of terrorist groups, financiers, associates and facilitators utilising the sector.	Terrorist financing methodologies are highly varied. There are several terrorist groups, financiers, associates and facilitators utilising the sector.
Very few instances of terrorism financing in the sector, with negligible or very low associated values.	Some instances of terrorism financing in the sector, with low associated values.	Multiple instances of terrorism financing in the sector, 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 sector, and low associated values.	Moderate number of predicate offences in the sector, and moderate associated values.	High number of predicate offences in the sector, and high associated values.

VULNERABILITIES		
Low	Medium	High
Sector has a small customer base.	Sector has a medium customer base.	Sector 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.
Sector tends to have simple and direct delivery arrangements.	Sector tends to utilise some complex delivery arrangements.	Sector 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 sector results in minimal personal loss.	Criminal activity enabled through the sector results in moderate personal loss.	Criminal activity enabled through the sector results in significant personal loss.
Criminal activity enabled through the sector does not significantly erode the sector's financial performance or reputation.	Criminal activity enabled through the sector moderately erodes the sector's financial performance or reputation.	Criminal activity enabled through the sector significantly erodes the sector's financial performance or reputation.
Criminal activity enabled through the sector does not significantly affect the broader Australian financial system and community.	Criminal activity enabled through the sector moderately affects the broader Australian financial system and community.	Criminal activity enabled through the sector significantly affects the broader Australian financial system and community.
Criminal activity enabled through the sector has minimal potential to impact on national security and/or international security.	Criminal activity enabled through the sector has the potential to moderately impact on national security and/or international security.	Criminal activity enabled through the sector 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 THE SMR SAMPLE AND IR REVIEW

ATTRIBUTE	SMR SAMPLE	IR REVIEW
Reports involving suspected money laundering	36%	59%
<b>Top 5 suspicious transaction activities</b>		
Multiple transactions	55%	N/A
Large transactions	41%	N/A
Rapid/complex movement of funds	36%	N/A
Cash deposits (face-to-face)	30%	N/A
Multiple parties	23%	N/A
<b>Customer type</b>		
Individual	94%	89%
Company	7.5%	42%
Trust	1.7%	N/A
Sole trader	1.7%	N/A

ATTRIBUTE	SMR SAMPLE	IR REVIEW
<b>Involved PEP</b>		
Yes	0.4%	5%
No	99.6%	95%
<b>Involved designated non-financial businesses and professions (DNFBP)</b>		
Yes	5%	0%
No	95%	100%
<b>Involved foreign-based entity</b>		
Yes	19%	5%
No	81%	95%
<b>Product used</b>		
Transaction account	90%	63%
Bank cheque or chequebook	10%	16%
Loan account	9%	0%
Credit card	2.5%	5%
<b>Direction of funds</b>		
Domestic	63%	5%
Incoming	27%	26%
Outgoing	17%	11%
Incoming and outgoing	7%	53%
Flow-through	7%	N/A
Returning	2%	N/A
<b>Involved a higher-risk jurisdiction</b>		
Yes	42%	74%
No	58%	26%
<b>Involved cash</b>		
Yes	71%	89%
No	29%	11%

**PREDICATE OFFENCES IN THE SMR SAMPLE AND IR REVIEW**

ATTRIBUTE	SMR SAMPLE	IR REVIEW
Reports involving a suspected predicate offence	62%	66%
<b>Key predicate offences (proportion of all foreign subsidiary bank reports)</b>		
Frauds	47%	9%
Scams	9.6%	3%
Tax evasion	8.7%	28%
Other high-impact predicate offences	1.7%	21%
<b>High-impact predicate offences</b>		
Sanctions violations	0.6%	9%
Bribery and corruption	0.5%	3%
Drug trafficking	0.3%	6%
Child exploitation	0.08%	3%
Modern slavery	0.04%*	0%
*determined using keyword analysis		
<b>Customer type (proportion of reports that identified a predicate)</b>		
Individual	97%	62%
Company	3.6%	67%
Sole trader	1.3%	N/A
<b>Involved PEP</b>		
Yes	0.4%	0%
No	99.6%	100%
<b>Involved DNFBP</b>		
Yes	1.7%	0%
No	98.3%	100%
<b>Involved foreign-based entity</b>		
Yes	4.7%	19%
No	95.3%	81%

ATTRIBUTE	SMR SAMPLE	IR REVIEW
<b>Product used</b>		
Transaction account	84%	N/A
Loan account	14%	N/A
Credit card	6%	N/A
Chequebook	1.5%	N/A
Bank cheques	0.9%	N/A
<b>Direction of funds</b>		
Domestic	64%	24%
Incoming	4.2%	10%
Outgoing	8%	5%
Incoming and outgoing	1.2%	57%
Flow-through	0.6%	N/A
Returning	0.1%	N/A
<b>Involved a higher-risk jurisdiction</b>		
Yes	13%	57%
No	87%	43%
<b>Involved cash</b>		
Yes	41%	62%
No	59%	38%



AUSTRAC.GOV.AU

