



Australian Government

AUSTRAC

FIGHTING
FINANCIAL
CRIME
TOGETHER

The background of the lower half of the page is a night-time photograph of a city skyline, likely Sydney, with numerous skyscrapers illuminated. Overlaid on this is a large, semi-transparent digital globe showing the Eastern Hemisphere, with glowing blue lines representing data or network connections. A large, dark teal diagonal stripe runs from the top left towards the bottom right, separating the header from the main content area.

FOREIGN BANK BRANCHES 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).

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

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



USE OF THE COMMONWEALTH COAT OF ARMS

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

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

CONTACT US

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

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

CONTENTS

| | |
|----------------------------------------------------|-----------|
| EXECUTIVE SUMMARY | 03 |
| PURPOSE | 09 |
| BACKGROUND | 11 |
| METHODOLOGY | 13 |
| FOREIGN BANK BRANCHES: REPORTING TO AUSTRAC | 16 |
| CRIMINAL THREAT ENVIRONMENT | 18 |
| Money laundering | 20 |
| Terrorism financing | 23 |
| Predicate offences | 24 |
| VULNERABILITIES | 31 |
| Customers | 32 |
| Products and services | 40 |
| Delivery channels | 47 |
| Foreign jurisdictions | 50 |
| CONSEQUENCES | 55 |
| RISK MITIGATION STRATEGIES | 59 |
| APPENDICES | 64 |

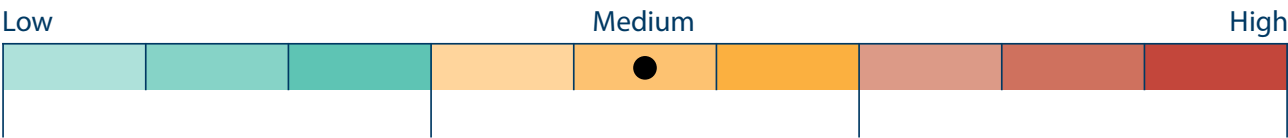


EXECUTIVE SUMMARY

Foreign bank branches operating in Australia are foreign authorised deposit-taking institutions (ADIs) licensed by the Australian Prudential Regulation Authority (APRA). Foreign bank branches are not separate entities incorporated and independently capitalised in Australia, but are a part of a foreign bank incorporated overseas. As at June 2021, 48 foreign bank branches operate in Australia, providing services to approximately 75,000 customers. For the purpose of this report, this subsector of ADIs is referred to as foreign bank branches.

The characteristics and activities of individual foreign bank branches 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.

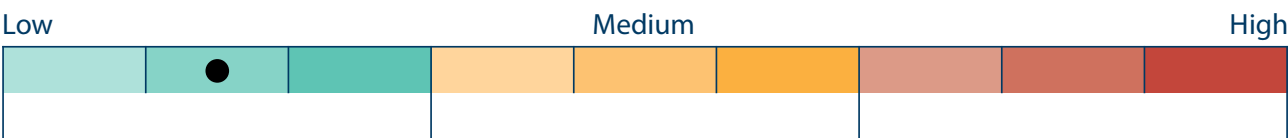
OVERALL RISK RATING



AUSTRAC assesses the overall ML/TF risk associated with foreign bank branches as **medium**. This rating follows assessments of the criminal threat environment, inherent vulnerabilities in the subsector and the consequences associated with the criminal threat.

Where possible, this assessment considers the risks associated with foreign bank branches in the context of AUSTRAC’s entire reporting population.

CRIMINAL THREAT ENVIRONMENT



AUSTRAC assesses the threat of ML/TF facing the foreign bank branch subsector as **low**.

The criminal threat environment facing foreign bank branches is somewhat complex, with a variety of money laundering methods and predicate offence types detected. However, the overall extent of criminal activity in the subsector is very low. In addition, AUSTRAC assesses reporting entities are not significantly exposed to transnational, serious and organised crime groups, or entities linked to terrorism or terrorism financing activities. The primary threats facing foreign bank branches are frauds and scams committed against their customers, followed by tax evasion and money laundering.

MONEY LAUNDERING

The nature and extent of money laundering threats facing the foreign bank branch subsector are assessed as **low**.

While some sophisticated methodologies were identified, the extent of suspected misuse is low. During the reporting period, approximately 15 per cent of suspicious matter reports (SMRs) submitted by the subsector related to suspected money laundering. Most reports related to company customers, and involved complex company ownership structures and intricate banking arrangements and obscure beneficial ownership. Very few reports related to suspected trade-based money laundering (TBML).¹ However, reports involving suspected TBML had much higher associated values than other money laundering-related SMRs.

Foreign bank branches are more likely to be exploited during the layering and integration phases of the money laundering process. This is because the subsector’s limited retail banking offerings reduces its exposure to cash, which remains the key medium in which criminal proceeds are generated.

¹ 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.

TERRORISM FINANCING

The nature and extent of terrorism financing threats facing the foreign bank branch subsector are assessed as **low**.

Across the entire reporting population, foreign bank branches submit an extremely small fraction of all terrorism financing-related SMRs. In the reporting period, foreign bank branches submitted just three SMRs involving suspected terrorism financing. These reports included international funds transfers to a higher-risk jurisdiction and correspondent banking services.

PREDICATE OFFENCES

The nature and extent of threat posed by predicate offending involving foreign bank branches is assessed as **low**.²

While predicate offences are sometimes varied and complex, the overall extent of offending is minimal. Frauds, scams and tax evasion were most commonly observed, and a small number of higher-risk entities were identified as posing a risk of sanctions violations.

Frauds and scams accounted for nearly 70 per cent of SMRs submitted by foreign bank branches in the reporting period. Customers of foreign bank branches were both targeted directly as well as indirectly in cases involving correspondent banking services. The exact nature of fraud and scam offences was difficult to determine in many SMRs but, where discernible, most involved the customer as the victim of the fraud or scam. The most common observed typologies were cyber-enabled scams such as false billing, email compromise, phishing³ and remote access.⁴

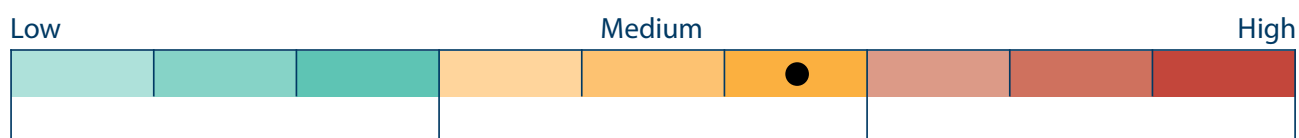
Tax evasion accounted for approximately 19 per cent of SMRs submitted by foreign bank branches in the reporting period. Corporate tax evasion likely poses the most significant tax-related threat to foreign bank branches, based on the subsector's large company customer base and core products and services offered.

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

3 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.

4 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 the foreign bank branch subsector as being subject to a **medium** level of inherent ML/TF vulnerability.

Given the subsector's large corporate and institutional banking footprint, ML/TF vulnerability largely stems from its customer base and exposure to foreign jurisdictions, including products and services that facilitate significant volumes of international funds flows.

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

- a high proportion of **higher-risk customers**, which can present across a range of categories including:
 - companies, trusts and other legal entities
 - financial institutions⁵
 - foreign-based customers
 - politically exposed persons (PEPs)
 - high net-worth individuals
 - designated non-financial businesses and professions (DNFBPs)⁶
 - temporary visa holders
 - known and suspected criminals.⁷
- products and services that can be used to **store and move funds** in and out of the subsector such as:
 - **accounts**, including transaction, savings and foreign currency accounts
 - **international funds transfers**
 - **correspondent banking services**
- high exposure to **foreign jurisdictions**, including **higher-risk jurisdictions**.

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

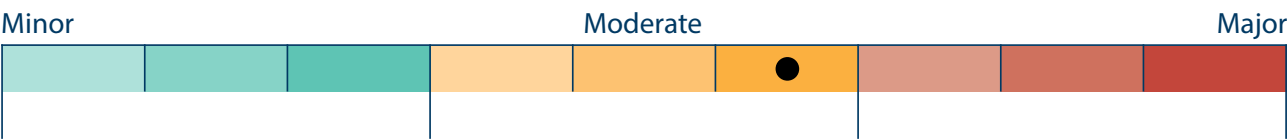
- lack of clarity and oversight of **agent bank arrangements** and reporting obligations
- customers engaged in **international trade** or who hold **trade finance** facilities
- private and investment banking products and services that help **disguise the true source and destination of funds**.

⁵ Please refer to the **Glossary** in **Appendix A** for a definition of 'financial institutions'.

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

⁷ 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 bank branches do not knowingly provide products or services to known or suspected criminals.

CONSEQUENCES



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

CUSTOMERS

AUSTRAC assesses criminal activity likely has **minor** consequences for customers. The severity of impact varies, and largely depends on the customer type and their ability to detect criminal exploitation early, as well as their capacity to absorb potential financial losses.

Across the subsector, many customers have mature fraud and scam management practices and controls in place, and are fairly resilient to criminal exploitation. While some customers experience financial or reputational loss following criminal exploitation, the impact is largely mitigated by the foreign bank branch assuming associated costs.

INDIVIDUAL BUSINESSES AND THE SUBSECTOR

Criminal activity can have **major** consequences for a foreign bank branch’s Australian operation, as well as their broader business group. Impacts can be financial, reputational and operational. The severity of impact varies between reporting entities, and largely depends on the extent to which they understand and mitigate their ML/TF risks, as well as their capacity to absorb potential financial losses.

AUSTRALIAN FINANCIAL SYSTEM AND COMMUNITY

Significant or systemic criminal exploitation of the subsector could result in **moderate** damage to Australia’s international economic reputation by undermining the security and safety of Australia’s financial sector. This is particularly true given the size of the subsector’s financial footprint in Australia and the significant value of transactions it facilitates. 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 bank branches can have **major** consequences for national and international security. Successful money laundering through the subsector can result in the preservation of illicit assets and help finance new crimes. Transnational, 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.

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

Many 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, some entities lack technological and data capabilities and improvements could be made. 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
- their understanding of Australian ML/TF risks and requirements under Australia's AML/CTF framework
- the effectiveness of AML/CTF regimes in the jurisdiction in which head office is based.



PURPOSE

This risk assessment provides specific information to foreign bank branches in Australia 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 bank branches in Australia 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 subsidiary banks. This approach recognises discrete segments within Australia's banking sector, each facing unique ML/TF risks which may not necessarily be shared across the entire sector.

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

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



BACKGROUND

Foreign bank branches operating in Australia are foreign ADIs licensed by APRA. Foreign bank branches differ from foreign subsidiary banks in that foreign bank branches are a part of a foreign bank incorporated overseas. They are not separate entities incorporated and independently capitalised in Australia. For the purpose of this report, this subsector of Australian ADIs is referred to as foreign bank branches.

As at June 2021, 48 foreign bank branches operate in Australia, providing services to approximately 75,000 customers.⁸ Combined, foreign bank branches hold assets worth \$427 billion, representing approximately nine per cent of the ADI market.⁹

Foreign bank branches are granted an ADI licence subject to conditions restricting retail deposits. They have an extremely small retail banking footprint and primarily provide products and services to corporate and institutional customers, as well as some private banking customers. Please refer to the **Glossary** at **Appendix A** for an explanation of these terms.

⁸ For the purpose of this assessment, 46 reporting entities have been included in scope. Two of the 48 foreign bank branches were granted licences by APRA after the reporting period end-date of 31 March 2019. For a full list of foreign bank branches in Australia, please visit APRA's website at apra.gov.au/register-of-authorized-deposit-taking-institutions.

⁹ APRA, *Monthly authorised deposit-taking institution statistics backseries: July 2020*, apra.gov.au/monthly-authorized-deposit-taking-institution-statistics.

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

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

Foreign bank branches are also required to provide AUSTRAC with AML/CTF compliance reports.

Across the subsector, the characteristics and activities of individual foreign bank branches vary significantly. There is extreme diversity in jurisdiction of head office, number and type of customers, and products and services offered. Consequently, the ML/TF risks associated with individual businesses also varies.

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

SIZE OF THE SUBSECTOR¹⁰



48

Number of reporting entities



~75,000

Number of customers



Total resident assets

9% of all ADIs



Total deposits

4% of all ADIs



Total loans
to households

<1% of all ADIs



Loans to households
(housing only)

<1% of all ADIs

¹⁰ APRA, *Monthly authorised deposit-taking institution statistics backseries: July 2020*, 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 bank branches that make them attractive for ML/TF purposes. This includes features that can be exploited, such as customer types, products and services, delivery channels and the foreign jurisdictions with which the subsector transacts. This report assesses inherent ML/TF vulnerability only.
- **Consequence** refers to the impact or harm that ML/TF activity within the subsector may cause.

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

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

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

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

1. Analysis of transaction reports, compliance reports and other holdings, including review and labelling of all SMRs submitted by foreign bank branches (n = 484) 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. One per cent of these related to foreign bank branches (the **IR review**).^{11,12}
3. The results of data-matching (the **data-matching exercise**) of IFTIs, TTRs and SMRs submitted to AUSTRAC by foreign bank branches between 30 March 2018 and 1 April 2019 and criminal entities who were:
 - recorded as a member of a significant transnational, serious and organised crime group as at May 2020
 - charged with a money laundering or proceeds of crime-related offence between 1 January 2017 and 31 December 2018¹³
 - charged with a terrorism-related offence between 1 January 2014 and 31 December 2018.¹⁴
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 bank branch representatives, as well as industry experts and associations.

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

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

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

14 Includes persons charged with a terrorism offence in section 3 of the *Crimes Act 1914* (Cth) and/or offences contrary to the *Crimes (Foreign Incursion and Recruitment) Act 1978* (Cth).

LABELLING THE SMR SAMPLE

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

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

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

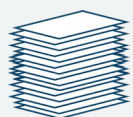
For example, a single SMR could be categorised with multiple labels as follows:

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

FOREIGN BANK BRANCHES: REPORTING TO AUSTRAC

REPORTS SUBMITTED BY FOREIGN BANK BRANCHES BETWEEN 1 APRIL 2018 AND 31 MARCH 2019

SMRs



484
reports

24

Number of reporting entities submitting at least one SMR during the sample period



\$215
MILLION

Total
value

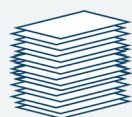
22

Number of reporting entities that did not submit any SMRs during the sample period

13

Number of reporting entities that have never submitted an SMR as at 31 March 2019

TTRs



380
reports



\$7.5
MILLION

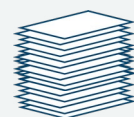
Total
value



\$7.5
MILLION

Cash
component

IFTIs



4.4
MILLION
reports



\$1
TRILLION

Total
value

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

FEEDBACK FOR REPORTING ENTITIES REGARDING SMR SUBMISSIONS

Across the subsector, SMR reporting is fragmented and there is wide variation in the quality and content of reports in the sample. For example, three reporting entities accounted for 70 per cent of all SMR submissions and 22 reporting entities did not submit a single report. Refer to the section **Risk mitigation strategies** for more details.

SMRs PLAY A CRUCIAL ROLE IN LAW ENFORCEMENT

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

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

WHAT HAPPENS AFTER AUSTRAC RECEIVES AN SMR?

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

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

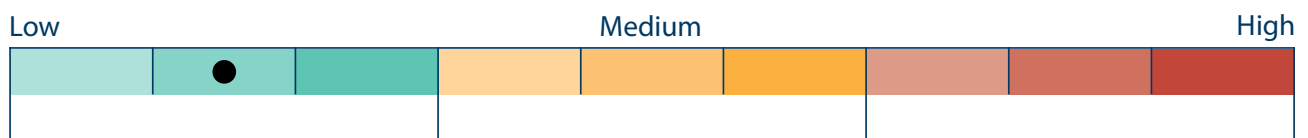
REFORMS TO 'TIPPING OFF' RESTRICTIONS

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

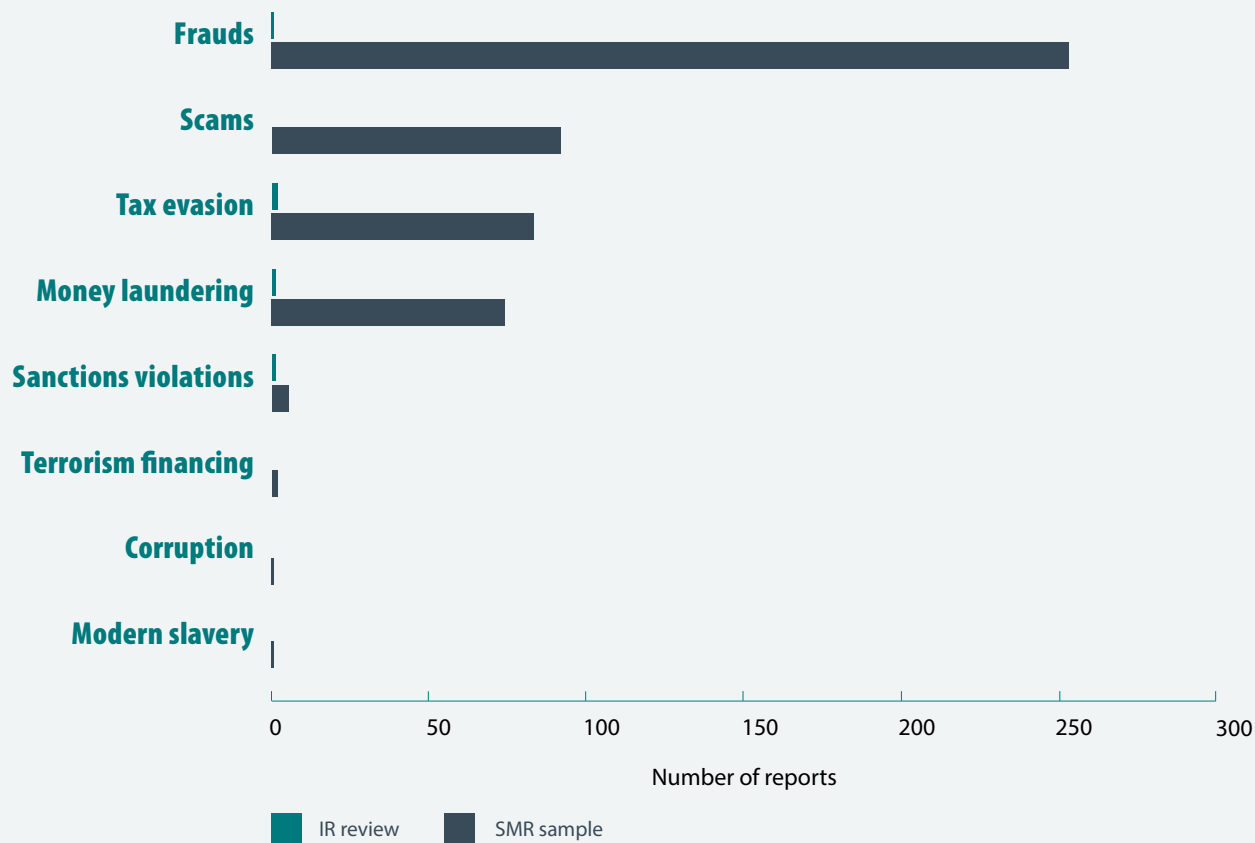
¹⁶ The reforms introduced by the Amendment Act commenced on 17 June 2021.

CRIMINAL THREAT ENVIRONMENT



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

FOREIGN BANK BRANCHES: DETECTED THREATS



AUSTRAC assesses the threat of ML/TF facing the foreign bank branch subsector as **low**.

The criminal threat environment refers to the nature and extent of ML/TF and predicate offences associated with Australia’s foreign bank branch subsector.

The criminal threat environment facing foreign bank branches is somewhat complex, with a variety of money laundering methods and predicate offence types detected. However, the overall extent of criminal activity in the subsector is very low. In addition, AUSTRAC assesses reporting entities are not significantly exposed to transnational, serious and organised crime groups, or entities linked to terrorism or terrorism financing activities. The primary threats facing foreign bank branches are frauds and scams committed against their customers, followed by tax evasion and money laundering. No confirmed instances of terrorism financing in the subsector were identified during the reporting period.

MONEY LAUNDERING

AUSTRAC assesses the nature and extent of money laundering threats facing foreign bank branches as **low**.

This assessment is based on the limited number of money laundering-related SMRs reported by foreign bank branches and minimal detection by partner agencies of criminal misuse of the subsector. In addition, the data-matching exercise indicates the subsector was not significantly exposed to members of transnational, serious and organised crime groups or individuals charged with a money laundering-related offence between 1 January 2017 and 31 December 2018 (see page 40 for a detailed overview of data-matching results).

During the reporting period, approximately 15 per cent of SMRs related to suspected money laundering.¹⁷ The most commonly reported customer type was companies, which is consistent with the subsector's customer base. While individual customers were also reported, they were often linked to a company as either an authorised individual or a third party acting on behalf of a company or trust. Commonly observed suspicious transactional activity included:

- multiple transactions (potentially without economic rationale)
- large or unusual transactions
- activity inconsistent with a customer's profile.

Despite the overall nature and extent of money laundering being assessed as low, the average value associated with money laundering-related SMRs is much higher than other banking subsectors. For example, they are more than triple the value of money laundering-related SMRs submitted by major domestic banks in the same period.

Foreign bank branches are more likely to be exploited during the layering and integration phases of the money laundering process. This is due to the subsector's limited retail banking offerings, which reduce customer capacity to directly place cash into the financial system. However, foreign bank branches should remain conscious of risks across all money laundering phases and proactively report any indicators of suspected placement, layering or integration of illicit funds.¹⁸

COMPLEX COMPANY AND BANKING STRUCTURES

Clients with complex company ownership structures and intricate banking arrangements (onshore and offshore) were identified in 40 per cent of money laundering-related SMRs. AUSTRAC assesses this to be the highest risk money laundering method applicable to foreign bank branches. Common observed themes and associated risk factors include:

- obscuring beneficial ownership or source of funds
- receipt of high-value international transfer of funds
- rapid and complex movement of funds between multiple companies linked by shareholders, trusts and beneficial owners
- companies moving funds to and from higher-risk and tax secrecy jurisdictions.

Criminals will continue to exploit complex company structures and banking arrangements to insulate and obfuscate their illicit financial activity. The use of these structures extends to relatively unsophisticated criminals, as well as serious and organised crime groups. It is acknowledged, however, that relative risk depends on multiple factors including company size, industry type, transparency and jurisdiction, with some companies more vulnerable to criminal exploitation than others. See page 34 for a discussion on vulnerability associated with company customers.

¹⁷ In the SMR sample, a report was labelled as 'money laundering' when AUSTRAC analysts deemed the nature or extent of suspicious indicators suggested money laundering was likely. Such indicators can include unexplained wealth, an attempt to obscure the source of funds or purpose of transaction, where the source of funds was possibly linked to proceeds of crime, or when money laundering methodologies were identified (e.g. cuckoo smurfing or rapid movement of funds).

¹⁸ The stages of the money laundering cycle – placement, layering and integration – are defined in the **Glossary** at **Appendix A**.

CASE STUDY: COMPLEX COMPANY STRUCTURES AND OFFSHORE ACCOUNTS RAISE SUSPICION

During the reporting period, one SMR detailed multiple indicators of suspected money laundering involving company structures and offshore bank accounts. The reporting entity was providing a credit facility to a company customer to fund investment in Australia. An initial suspicion was formed on the source of funds after the customer received multiple high-value international funds transfers from entities based in known tax secrecy jurisdictions. The transfers were noted as 'gifts'.

During enhanced customer due diligence (ECDD) investigation by the reporting entity, it was identified the company group had undergone recent restructuring in a manner likely to obscure beneficial ownership, effective control and managing directorship. Additionally, one foreign-based entity sending funds to the company group was identified as a politically exposed person (PEP) and subject to adverse media. This resulted in the submission of an SMR to AUSTRAC based on concerns of money laundering, avoidance of reporting obligations and suspicious source of funds.

AUSTRAC acknowledges the depth of the investigation completed by the reporting entity and the subsequent submission of a high-quality SMR. AUSTRAC encourages reporting entities to include all findings from financial investigations and ECDD activities in the grounds for suspicion section of the SMR.

MINIMAL CASH-RELATED SUSPICIONS

Foreign bank branches are not widely exposed to cash-related money laundering methods. This is primarily due to their limited retail banking footprint and the subsequent low volume of cash exposure. In the reporting period, 20 SMRs detailed suspicious face-to-face cash deposit activity. Reported suspicions include:

- structuring
- company customers operating in known higher-risk industries (bullion and other high-value dealers)
- use of a third party by a customer's customer (correspondent banking services)
- rapid transfer of funds offshore immediately after deposit.

i Foreign bank branches that facilitate cash transactions should remain cognisant of the associated risks and continue strengthening their systems and controls to mitigate illicit cash activity.

TRADE-BASED MONEY LAUNDERING

Approximately three per cent of the SMR sample identified suspected TBML. However, actual criminality is probably higher as TBML can be extremely difficult for reporting entities to detect. Nonetheless, the SMR sample highlights TBML as a low-volume, high-impact threat to the subsector. While very few reports were submitted, associated values were usually high. For example, two separate attempts by a customer to fund trade-related transactions over \$475 million.

Some foreign bank branches are particularly exposed to TBML because they offer a comprehensive range of trade finance products and service a high number of corporate customers. In addition to trade finance products, TBML 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 bank 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 that exceed expectations for that business
- companies operating in porous border regions close to higher-risk jurisdictions.

Some foreign bank branches also offer trade finance products. This exposes these entities 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.

i Foreign bank branches 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.

TERRORISM FINANCING

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

This assessment is based on the very small number of terrorism financing-related SMRs, information provided by partner agencies and Australia's terrorism financing environment. In addition, foreign bank branches were not identified as being used by relevant criminal entities in the data-matching exercise.

Less than one per cent of the SMR sample related to possible terrorism financing activity. Observed themes include:

- risk exposure observed via correspondent banking services – where suspicion was formed on the respondent bank's customer
- 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 The risk of customers supporting or funding offshore terrorism is reduced given the subsector's limited number of individual customers. Nonetheless, foreign bank branches 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 Islamic State of Iraq and the Levant's caliphate in Syria and Iraq, there has been a sharp decline in the number of foreign terrorist fighters departing Australia. However, the security environment continues to evolve and the COVID-19 pandemic, while inhibiting some aspects of the terrorism threat through the restricted cross-border movement of people, has also presented a platform for recruitment and the promotion of extremist narratives online. Amid this evolving environment, supporters and sympathisers in Australia are likely to continue to send funds internationally in support of terrorist activity.

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

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

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

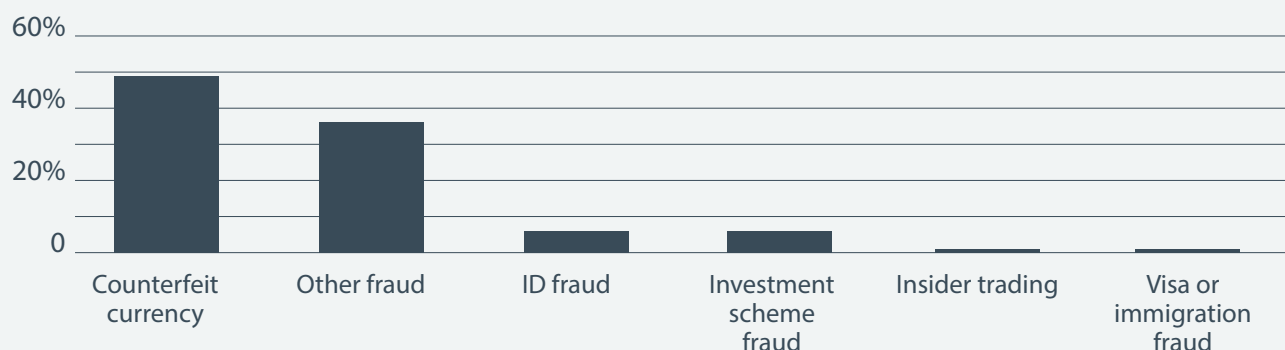
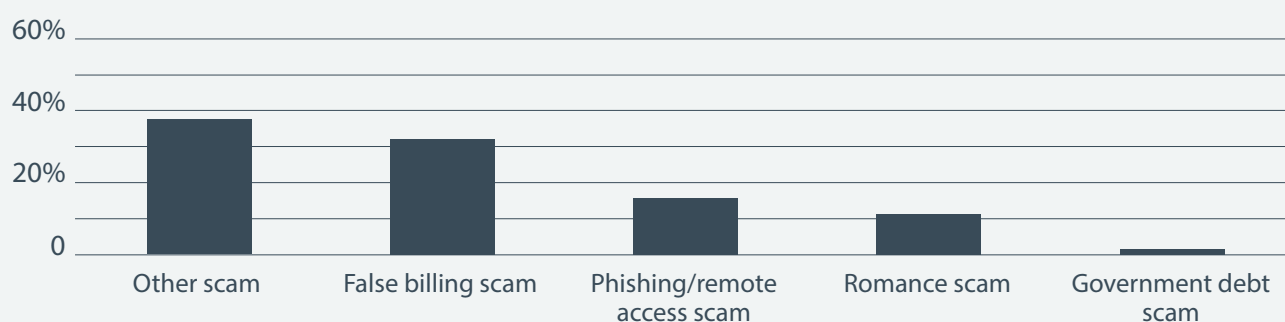
AUSTRAC assesses the nature and extent of threat posed by predicate offending involving foreign bank branches as **low**.

While offences are sometimes varied and complex, the overall extent of offending is minimal. Frauds (including counterfeit currency notes) and scams were the most common offences, and associated values were sometimes high. A small number of high-risk entities were also identified as posing a risk of sanctions violations.

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](#).

TYPE OF FRAUD: PERCENTAGE OF FRAUD-RELATED SMRs**TYPE OF SCAM: PERCENTAGE OF SCAM-RELATED SMRs****FRAUDS AND SCAMS**

Frauds and scams accounted for nearly 70 per cent of the SMR sample. Over half of these reports related to counterfeit currency notes. There was no level of sophistication demonstrated in these reports and cases almost always involved extremely low values (e.g. less than USD\$100). While prominent in the SMR sample, AUSTRAC assesses the overall threat to the subsector from counterfeit currency notes is **low**.

Foreign bank branches were both the direct target of offending as well as the indirect target in frauds and scams involving correspondent banking services. In these instances, the victim was a customer of the respondent bank. ML/TF vulnerabilities associated with correspondent banking are further discussed on page 46.

The exact nature of fraud and scam activity was difficult to determine in many SMRs, as evidenced by the large portion labelled 'other fraud' or 'other scam'.¹⁹ These reports were often the result of correspondence from a respondent bank requesting recovery of fraudulently transferred funds.

i In these circumstances, reporting entities may not be provided details of the nature of predicate offending or enabling methodologies and therefore cannot include them in the SMR. However, if further details do become known, AUSTRAC encourages them to be included in further or additional lodging of SMRs.

¹⁹ An SMR was assessed as 'other fraud' or 'other scam' if no information was available to determine the nature of the predicate fraud or scam offence, or the methodology employed to conduct the offence.

Where discernible, the most common offending involved cyber-enabled scams. To a lesser extent, foreign bank branches were also exposed to the following:

- identity fraud – usually involving fraudulently altered documentation. It is worth noting foreign bank branches are far less exposed to identity fraud and identity theft than other ADIs that have large retail banking offerings and online banking services.
- investment scheme fraud – commonly associated with boiler room activity or customers transferring funds under the false guise of investment opportunities²⁰
- romance scams – often involving correspondent banking services where a foreign bank branch facilitated the movement of funds offshore
- insider trading.

CYBER-ENABLED SCAMS


AUSTRAC assesses cyber-enabled scams such as false billing, email compromise, phishing and remote access to be key threats to foreign bank branches, even when these scams are relatively unsophisticated. Values associated with these offences were high compared to similar activity targeting other banking subsectors. This is consistent with variation in expected financial activity between retail and corporate customers.

Cyber-enabled scam typologies commonly include the use of public domain email addresses, malware, and encrypted, self-destructing messaging services. Some criminal activity resulted in the successful procurement of fraudulently obtained funds, while other attempts were identified and prevented by AML/CTF systems and controls.

CASE STUDY: CYBER-ENABLED FALSE BILLING SCAMS TARGET AUSTRALIAN COMPANIES

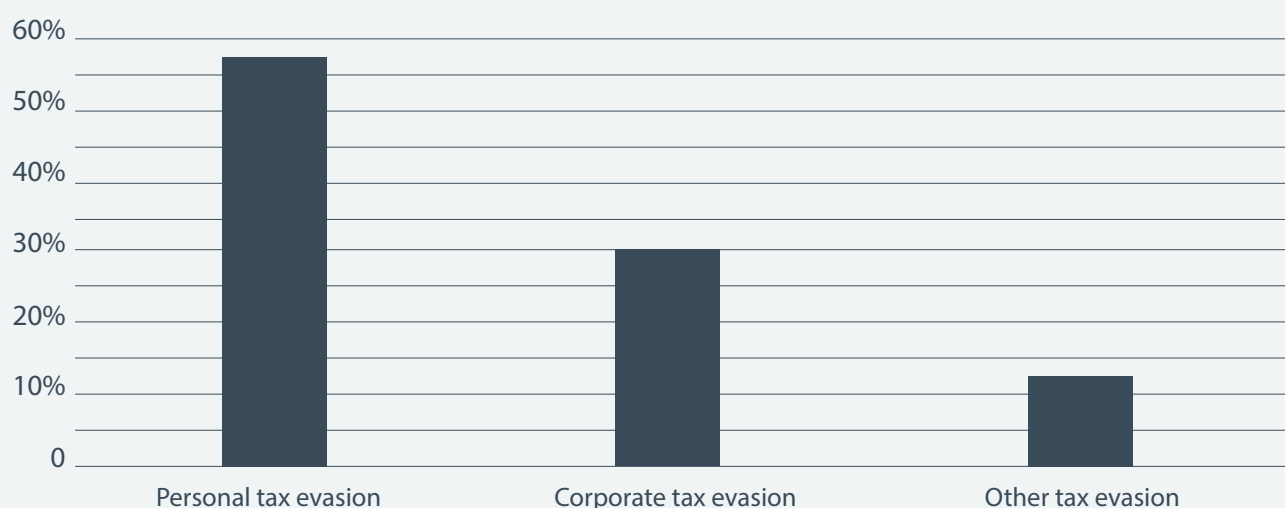
During the SMR sample period, a corporate client was scammed into transferring over \$60,000 in a false billing scam. A cyber-criminal posing as a known supplier contacted the customer from a public domain email address, advising they had new account details for an outstanding invoice. The customer then transferred the funds to the new account held with a domestic ADI.

The scam and resultant fraud was not identified until the real supplier contacted the client to follow up the outstanding invoice. By this time, the funds had been withdrawn from the domestic ADI and could not be recovered.

 AUSTRAC acknowledges fraud and scam threats are continually evolving. Foreign bank branches should remain vigilant of specific fraud and scam methods relevant to their operations and customers. AUSTRAC encourages the subsector to:

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

²⁰ The terms 'boiler room fraud' and 'boiler room scam' are used to describe a fraud committed by means of distance selling, telemarketing or telesales, where victims are pressured into buying products or investments on a false premise.

TYPE OF TAX EVASION: PERCENTAGE OF TAX EVASION-RELATED SMRs**TAX EVASION**

Tax evasion accounted for approximately 19 per cent of the SMR sample. Suspected personal income tax evasion was the most commonly reported tax-related threat, followed by corporate tax evasion and other tax-related offences.²¹

PERSONAL INCOME TAX EVASION

Despite being the most commonly reported tax-related threat, the overall extent of personal income tax evasion in the subsector is assessed as **low**. For example, the same customer was reported in over half of the reports in the SMR sample.

Common observed methods of personal income tax evasion identified in the SMR sample include:

- the use of non-resident accounts to receive rental income, business income or suspicious cash deposits
- movement of funds to tax secrecy jurisdictions
- exploitation of term deposits.

i Reporting entities most exposed to personal tax evasion are those offering private banking services and those who bank high net-worth individuals. While many foreign bank branches do not offer these products and services, reporting entities that do must stay updated on personal tax evasion methods and continue to report suspicious transactions to AUSTRAC.

²¹ 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

Despite the small number of SMRs in the sample, AUSTRAC assesses corporate tax evasion likely poses the most significant tax-related threat to foreign bank branches. This is based on the subsector's large company customer base, core products and services offered by most reporting entities, information provided by partner agencies, and the high values associated with company-related SMRs. For example, the total value of SMRs in the sample was \$36.4 million, including one suspicious transaction of \$17 million.

Other commonly observed features of suspected corporate tax evasion include:

- the use of non-resident accounts to receive rental income, business income or suspicious cash deposits
- exploitation of complex company structures (including shell companies) to place, layer and conceal wealth
- international funds transfers most commonly made to/from Taiwan and Hong Kong Special Administrative Region of the People's Republic of China (Hong Kong SAR) followed by China and Singapore
- phoenixing
- knowingly withholding information from, or providing misleading information to, tax authorities and the reporting entity (including manipulation of loan facilities).

USE OF NON-RESIDENT ACCOUNTS TO AVOID TAXATION OBLIGATIONS

In the reporting period, 35 SMRs were submitted by foreign bank branches relating to suspected misuse of non-resident accounts to avoid both personal and corporate taxation obligations. In this scenario, a non-resident opens an account and adds a local signatory (often a family member). The local signatory then conducts most or all transactions, effectively maintaining control of the account. These transactions almost always involve frequent deposits suspected to be related to personal or business income earned in Australia, and are often related to residential or commercial property rental income.

Use of non-resident accounts to receive locally-derived income is a legitimate arrangement. In these scenarios, the non-resident account holder is subject to Australian taxation laws. Exploitation occurs when the local signatory uses the account to place their income but fails to declare these earnings to the ATO.

i AUSTRAC expects the foreign bank branch subsector to continue reporting any suspicions of corporate tax evasion. This information assists our partners, including the ATO, in investigating related offending.

SANCTIONS VIOLATIONS

Less than one per cent of the SMR sample related to suspected or attempted sanctions violations as administered by the Department of Foreign Affairs and Trade (DFAT). One suspicious entity was identified acting as a possible shell company in a tax secrecy jurisdiction, with a physical presence in another higher-risk jurisdiction. This entity was suspected of using a foreign bank branch to facilitate the 'flow-through' of funds via Australia, further obscuring the ultimate ordering and beneficiary customers.

Other suspicions related to beneficial owners of assets and transactional activity being domiciled in sanctioned jurisdictions. In some reports where violations were identified, the reporting entity did not record details of how the risk was mitigated or considered. These details should be included whenever possible to help AUSTRAC understand a reporting entity's AML/CTF controls.

i Foreign bank branches may be attractive to sanctioned entities because of the types of products and services offered and foreign jurisdiction exposure they afford. While the extent of sanctions risk is assessed as low, associated consequences are high. Foreign bank branches should ensure risk mitigation strategies aimed at identifying and disrupting this activity are strong.

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.

BRIBERY AND CORRUPTION

Bribery and corruption were identified in one SMR. The report related to a private banking customer who knowingly provided bribes to a foreign official in exchange for real estate development opportunities. The offences occurred in a foreign jurisdiction before the customer was onboarded by the reporting entity. The reporting entity moved to close the customer's accounts once the information became known.

i While detected and suspected instances of bribery and corruption are low, industry and partner agencies suggest foreign bank branches should remain vigilant, particularly given their high exposure to PEPs.

It is worth noting some foreign bank branches 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.

MODERN SLAVERY

Modern slavery was identified in one SMR. The report detailed several low-value incoming transfers to one company customer and an individual customer of a correspondent bank. No direct link between the customers and suspected modern slavery activities was made, but the report highlights ML/TF vulnerability posed by corporate customers and correspondent banking arrangements. These vulnerabilities are further discussed in the section **Higher-risk customers**.

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.²² 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 2017.²³

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.²⁴ 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.²⁵

Financial information provided by reporting entities plays a key role in combating modern slavery. While not specific to foreign bank branches, 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.

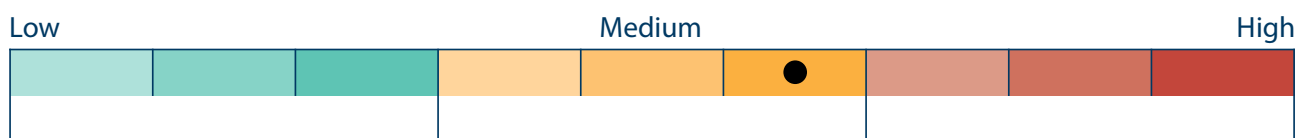
22 For more see: homeaffairs.gov.au/criminal-justice/Pages/modern-slavery.aspx.

23 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.

24 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.

25 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.

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 bank branches are subject to a **medium** level of inherent vulnerability related to ML/TF and other predicate offences. AUSTRAC's assessment of vulnerabilities falls into four broad categories:

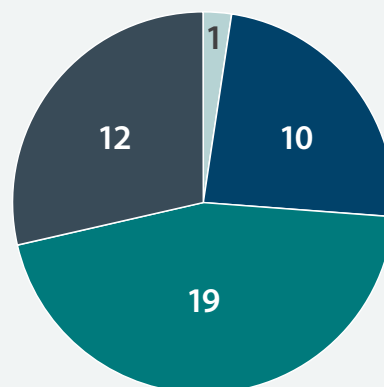
- customers
- products and services
- delivery channels
- exposure to foreign jurisdictions.

CUSTOMERS

AUSTRAC assesses the foreign bank branch subsector's customer base presents a **medium** level of inherent ML/TF vulnerability.

The subsector's customer base is proportionately small, yet extensively diverse. Customer numbers, types and jurisdiction of home office vary extensively between individual foreign bank branches. AUSTRAC assesses this diversity translates to a medium level of risk exposure, with foreign bank branches providing products and services to a variety of low, medium and high-risk customers.

SIZE OF THE CUSTOMER BASE:²⁶



Number of REs with:

- >10,000 customers
- Between 1,000-10,000 customers
- Between 100-1,000 customers
- <100 customers

CUSTOMER BASE

Foreign bank branches have a small customer base, with approximately 75,000 customers banking across 48 foreign bank branches. Customer numbers vary significantly, ranging from one customer to more than 30,000.

Foreign bank branches predominantly bank large corporate clients. This is due to operating obligations, access to global markets and capability to manage large exposure limits. Other customer types include small and medium-sized businesses, domestic and foreign government institutions and high net-worth individuals. The subsector has an extremely small retail banking footprint.

Based on the steady increase of foreign ADIs entering the Australian market and information provided during consultations, AUSTRAC expects the subsector's customer base to continue experiencing gradual growth. This increase will not result in an immediate change to the level of customer-related risk exposure, with subsector-wide risk mitigation strategies considered mature enough to manage steady growth.

²⁶ Customer number data was provided by 42 reporting entities.

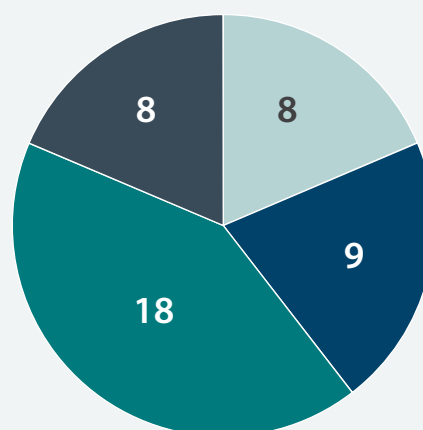
HIGHER-RISK CUSTOMERS

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

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

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

INDUSTRY CUSTOMER RISK RATINGS: PORTION OF HIGH-RISK CUSTOMER BASE (BY NUMBER)²⁷



Number of REs with:

- Nil
- Less than 5%
- Between 5-20%
- Over 20%

Industry customer risk ratings vary significantly among foreign bank branches. Some reporting entities, notably those with small customer bases (<50), report banking no high-risk customers. These foreign bank branches are commonly either new market entrants or they deliberately bank only low-risk, established clients. Eight foreign bank branches indicated more than 20 per cent of their customer base are rated high-risk – including one reporting entity whose high-risk customer base was 50 per cent.

The most common high-risk customer types include respondent banks and other financial institutions, commercial companies and trusts. Refer to the **Risk mitigation strategies** section for an overview of risk treatment strategies commonly applied by the subsector to these high-risk customers.

²⁷ Industry customer risk rating data was provided by 43 reporting entities.

COMPANIES, TRUSTS AND OTHER LEGAL ENTITIES

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 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.²⁸

The subsector services a large number of companies, trusts and other legal entities. These customers were reported in approximately half of the SMR sample and were overwhelmingly linked to suspected money laundering or fraud activities. Common observed themes include:

- foreign-based entities, including companies domiciled in higher-risk jurisdictions as well as use of suspected offshore shell and shelf companies
- customers involved in industries such as gambling, natural resource extraction and real estate sectors
- links to individuals holding an Australian Significant Investor visa or Business Investor visa
- correspondent banking services
- involvement of DNFBPs – namely real estate agents and associated trust accounts.

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

- There are limitations in the identity verification process when registering a company in Australia. This can create opportunities for criminals to use stolen identities to establish a company that is subsequently used to launder criminal proceeds.
- Criminal entities often appoint a family member or ‘cleanskin’ associate as a director or shareholder to distance themselves from the purportedly legitimate entity.²⁹
- Australian companies can be registered by foreign nationals. Transnational, serious and organised crime groups exploit this vulnerability by compelling individuals on temporary visas to register companies that are subsequently used to place, layer and integrate illicit funds.
- Criminals may own or control multiple companies that are registered or operate in various jurisdictions. Banking arrangements linked to these companies are then used to facilitate global movement of funds and evasion of taxation obligations.

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

²⁸ 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).

²⁹ 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.

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.

FINANCIAL INSTITUTIONS

Financial institution customers may pose a higher ML/TF vulnerability because they have many hundreds or thousands of customers of their own (underlying customers). Therefore, banking with a single financial institution exposes a foreign bank branch to many underlying customers. Foreign bank branches have limited visibility of these underlying customers and their transactions, meaning reporting entities are partially reliant upon the quality of the financial institution's AML/CTF controls.

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

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

Reporting entities also count some offshore financial institutions as customers through the provision of correspondent banking services, which is discussed further on page 46.

FOREIGN-BASED CUSTOMERS

Foreign-based customers pose ML/TF vulnerabilities relating 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 identified in 27 per cent of the SMR sample. Most reports related to suspected fraud (including where the customer was a victim) and involved transactions with Hong Kong SAR and the USA.

i While foreign-based customers are consistent with the subsector's operating models and business strategies, reporting entities must be vigilant to elevated risks associated with foreign jurisdiction exposure (discussed in the **Foreign jurisdictions** section) and ensure appropriate mitigation strategies are in place to minimise and detect criminal misuse.

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.³⁰ 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.

Foreign bank branches service a large number of PEP customers relative to other reporting entities.³¹ Despite this, SMR reporting is extremely low (three reports in the sample period). In all instances, the customer was identified through PEP list screening or adverse media and involved a high-value international transfer. Industry feedback indicates ECDD on PEP customers rarely returns adverse findings and very few are refused at onboarding, subject of an SMR or exited as a customer (i.e. de-banked).

i AUSTRAC assesses the overall number of PEP customers will continue to present a high ML/TF vulnerability to some reporting entities. AUSTRAC recommends elevated risk mitigation strategies continue to be applied for PEP customers, and all suspicious related activity reported in SMRs.

HIGH NET-WORTH INDIVIDUALS

Across the subsector, several foreign bank branches provide private banking services to high net-worth individuals. Generally, these customers are individuals, trusts and trustees, or companies. While defined differently by each foreign bank branch, a high net-worth individual generally has \$1 million in assets they wish the bank to manage.

Private banking provides highly personalised wealth management services including investing and portfolio management, tax services, insurance, and trust and estate planning. At least one reporting entity also specifically assists inbound investors to meet requirements associated with the Australian Business Innovation and Investment visa. Key ML/TF vulnerabilities associated with high net-worth individuals relate to transparency of beneficial ownership and source of funds. Factors that may obscure transparency include:

- accounts for non-residents located in jurisdictions with weak AML/CTF regimes
- accounts with third-party power of attorney operation
- business accounts with multilayer ownership structures
- trust accounts and the involvement of accountants/lawyers acting on behalf of clients
- use of private investment companies (or shell companies) established in tax secrecy jurisdictions
- customers maintaining personal and business wealth in numerous jurisdictions
- use of numerous legal entities for personal and family estate planning purposes.

30 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.

31 The high number of PEPs may be influenced by the way some foreign bank branches define these customers. Some reporting entities apply stricter definitions of PEPs based on their global policies and standards, in addition to the Australian definition. For example, some reporting entities will consider an individual a PEP years after they have left office.

i The perceived high profitability of private banking can lead to intense pressure for private bankers to attract and retain clients. Foreign bank branches should ensure such pressure does not lead to business practices that create a permissible environment for criminal exploitation. For example, a culture of secrecy developed by a relationship manager for their clients.

DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

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

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

Lawyers and accountants have specialist knowledge and services that can be exploited by those seeking to conceal wealth or launder criminal proceeds. They can establish complex legal and banking structures, execute financial transactions, facilitate the purchase of high-value assets and act as trustees or directors of companies. They often have a strong understanding of the regulatory environment and their professional status can be used to provide a veneer of legitimacy to otherwise suspicious transactions.

Lawyers and accountants can also accept large amounts of cash on behalf of criminals, which may be deposited into the firm's trust account and co-mingled with legitimate funds. There may also be a perception among criminals that funds held by their lawyer or accountant cannot be seized by law enforcement, and that transactions executed by these professionals cannot be subject to investigation.

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

AUSTRAC assesses a small number of 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, several SMRs related to DNFBPs including real estate agents, high-value dealers (namely jewellery and gold dealers) and lawyers. These reports outlined suspected money laundering and tax evasion by these entities and included the following suspicious activities:

- incoming and outgoing funds transfers to real estate companies and trust accounts
- under-reporting and lack of reporting to tax authorities
- requests by real estate agents to transact in cash.

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

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

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

i AUSTRAC encourages foreign bank branches to remain aware of enduring ML/TF risks posed by DNFBPs and continue reporting detailed SMRs when a related suspicion is formed.

TEMPORARY VISA HOLDERS

AUSTRAC assesses a small number of Business Innovation and Investment visa holders present a high risk for both money laundering and tax evasion activity in the subsector. Partner agencies report known and suspected cases of criminal exploitation of these visa classes, and industry representatives report varying degrees of associated ML/TF risk. Some reporting entities consider Significant and Premium Investor visa holders to be lower risk due to their visa status, while others indicated they were not within their bank's risk appetite.

AUSTRAC acknowledges a lawful visa status for a non-citizen may contribute to a bank's overall risk assessment at onboarding of a prospective client. However, this status alone should not determine a client's risk rating or influence future monitoring and reporting. The assessment conducted by the Department of Home Affairs when assessing whether to refuse or cancel a visa is largely set out under section 501 of the *Migration Act 1958* (Cth), and does not fully mitigate against a temporary visa holder engaging in future illicit criminal activity.

i AUSTRAC encourages the subsector to remain aware of visa conditions applied to respective customers who are on temporary visas, including those in Significant and Premium Investor streams. This awareness is likely to facilitate internal risk assessments both at onboarding and during ongoing CDD and transaction monitoring.

KNOWN AND SUSPECTED CRIMINALS

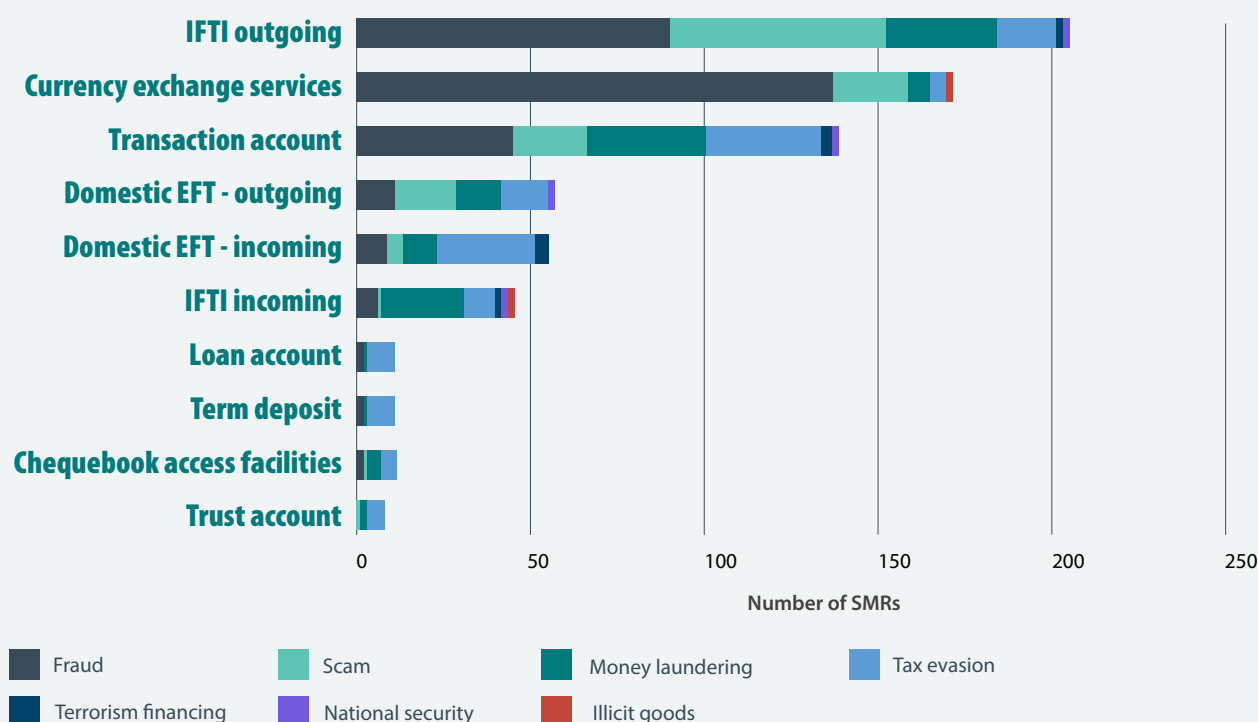
AUSTRAC assesses a very small number of known and suspected criminals present a high inherent ML/TF vulnerability to the subsector. This assessment is based on the results of the data-matching exercise which identified an extremely small number of known and suspected criminal entities transacting with the subsector. This included:

- several individuals with a recent criminal charge for either money laundering or a proceeds of crime-related offence
- several individuals linked to transnational, serious and organised crime groups.

The most common transactions by these customers were international funds transfers, both into and out of Australia. The most common jurisdictions included New Zealand, UK, China, US and Hong Kong SAR. Despite the very small number of criminal entities identified, these customers present a very high ML/TF risk to the subsector.

PRODUCTS AND SERVICES

MOST COMMON PRODUCTS OR SERVICES AND THREAT – SMR SAMPLE



AUSTRAC assesses the nature of products and services offered by the foreign bank branch subsector poses a **medium** level of inherent ML/TF vulnerability.

ML/TF vulnerability largely stems from the potential to store and move illicit funds through certain products and services. Foreign bank branches are more likely to be exploited during the layering and integration phases of the money laundering process. This is because the subsector's limited retail banking offerings reduce its exposure to cash, which remains the key medium in which criminal proceeds are generated.³²

Across the subsector, there is wide variation in the number and type of products and services offered by individual bank branches. These range from very small operations with specific product offerings to much larger operations that offer a multitude of products and services. Generally, foreign bank branches offer fewer products and services than other ADIs in Australia, and not all foreign bank branches offer products or services considered to be more vulnerable to ML/TF and criminal misuse.

³² Foreign bank branches are restricted in their product and services offerings by the banking licence authorised by APRA. They are not permitted to accept initial deposits (and other funds) from individuals and non-corporate institutions of less than \$250,000. However, they can accept deposits and other funds in any amount from incorporated entities, non-residents and their employees.

USE OF CASH


A reporting entity's exposure to money laundering placement risk significantly increases when facilitating a large volume and high value of cash transactions. This is because criminal proceeds are often derived in cash, which is very difficult to trace. Cash is also a key facilitator of the shadow economy, including tax evasion.

Foreign bank branches are far less exposed to cash compared to other ADIs in Australia. Therefore, their risk exposure to illicit cash placement is assessed as low. Several foreign bank branches provide a direct capability for their customers to transact in cash (including at one of Australia's major domestic ADIs).³³ However, most reporting entities that offer a cash capability indicate their customers rarely use it.

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

- Total number of TTRs submitted to AUSTRAC: **380**
- Total cash value: **\$7,522,086**
- Largest cash deposit: **\$85,280**
- Largest cash withdrawal: **\$60,664**
- Total number of cash-related SMRs: **20**
- Total value of cash-related SMRs: **\$837,624**

Between 1 April 2018 and 31 March 2019, foreign bank branches submitted 380 TTRs to AUSTRAC. The total value of the reports was \$7.5 million. Compared to other banking subsectors, this figure is extremely low. In addition, all TTRs were submitted by just five reporting entities, including one reporting entity that submitted over 85 per cent of all reports. In the reporting period, only 20 SMRs related to suspicious cash transactions. Most reports related to suspected structuring activity.

 Some reporting entities have agent bank arrangements with major domestic ADIs to facilitate cash deposits for their customers. It is essential reporting entities understand their reporting obligations for TTRs in these arrangements. Further details of ML/TF vulnerability associated with these arrangements and TTR reporting obligations is provided in the section **Delivery channels**. Reporting entities can also refer to AUSTRAC's [website](#) for specific guidance.

33 A very small number of foreign bank branches offer employee accounts which allow for cash deposits and withdrawals.

ABILITY TO STORE AND MOVE FUNDS AND VALUE

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

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

- transaction accounts (including foreign currency accounts and savings accounts)
- correspondent banking services.

Known cases of criminal misuse of trade finance facilities and investment products in the subsector are low. However, some reporting entities and industry representatives note these products are highly vulnerable to ML/TF, and the potential impacts from criminal misuse can be significant. This is particularly true given the often large values of associated financial transactions. These products are not discussed in-depth below as they did not rate 'high' on the product risk matrix (see page 43). However, reporting entities who offer these services should apply appropriate enhanced customer and transaction due diligence and post-transaction monitoring processes to detect suspicious or unusual activity.

Indicators of TBML and trade finance-based money laundering are discussed on page 22. Reporting entities can also review [AUSTRAC's ML/TF risk assessment of Australia's securities and derivatives sector](#). This report provides an in-depth analysis of ML/TF vulnerability associated with these investment products.

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

To better assess the inherent vulnerability of products and services offered by foreign bank branches, AUSTRAC developed a product risk matrix (the matrix). The results and ratings from this exercise can be found in the table on page 44.

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 simplicity and design purposes. For each product category, two aspects were assessed:

1. The vulnerability perception rating is an average score of foreign bank branch responses to the perceived 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.

The vulnerability perception rating score and detected exploitation rating were equally weighted and an average score was used to determine the overall rating.

An indication of the number of foreign bank branches who report offering the product/service is also noted. This provides context regarding the extent of the product or service offering across the subsector.

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

PRODUCT AND SERVICE VULNERABILITY RATINGS

| PRODUCT/SERVICE | VULNERABILITY PERCEPTION RATING | DETECTED EXPLOITATION | OVERALL RATING | NUMBER OF REPORTING ENTITIES |
|------------------------------------|---------------------------------|-----------------------|----------------|------------------------------|
| Transaction accounts | | Very high | | |
| Correspondent banking | | High | | |
| Foreign currency accounts | | Low | | |
| Savings accounts | | Low | | |
| Trust accounts | | Medium | | |
| Credit cards | | Medium | | |
| Term deposits | | Low | | |
| Foreign currency exchange services | | High | | |
| Chequebook access | | Low | | |
| Business/bilateral loans | | Negligible | | |
| Bank cheques | | Negligible | | |
| Personal loans | | Low | | |
| Investment products | | Negligible | | |
| Trade finance | | Low | | |
| Syndicated loans | | Negligible | | |
| Home loans | | Negligible | | |
| Asset financing | | Negligible | | |

LEGEND

| NUMBER OF REPORTING ENTITIES | = 1-10 | = 11-20 | = 21-30 | = >30 |
|------------------------------|--------|---------|---------|-------|
|------------------------------|--------|---------|---------|-------|

SPOTTING DIFFERENCES IN VULNERABILITY PERCEPTION AND DETECTED EXPLOITATION RATINGS

Reporting entities have identified foreign currency accounts and savings accounts as particularly vulnerable to criminal misuse. However, the SMR sample and IR review indicate detected exploitation of these products is limited. This discrepancy is due to the way these products are recorded in SMR submissions, and the extent of actual exploitation is likely much higher. Unless specifically noted in the grounds for suspicion, these products are often recorded as a transaction account.

Foreign currency accounts function like a transaction account, but have the ability to hold different currencies. These accounts are vulnerable to criminal misuse because of their ability to move funds quickly across international borders and into different currencies. Depending on global exchange rates, a criminal could also potentially increase the value of illicit funds.

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.

Reporting entities have identified foreign currency exchange services as posing a medium ML/TF vulnerability. However, the SMR sample indicates detected exploitation of these products is high. This discrepancy is due to a large number of SMRs submitted by one reporting entity relating to the receipt of low-value counterfeit notes. Very few reports in the SMR sample or IR review indicate foreign currency exchange services are being used to launder large quantities of criminal proceeds.

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. Additionally, partner agencies rate them as the highest risk product offered by all banks.

In the reporting period, nearly all SMRs (93 per cent) involving a transaction account related to suspicious funds movements (see table below) and reporting entities consistently noted international funds movements as particularly vulnerable to ML/TF. Higher-risk international funds flows are further discussed in the **Foreign jurisdictions** section.

SMR SAMPLE: SUSPICIOUS FINANCIAL ACTIVITY INVOLVING A TRANSACTION ACCOUNT

| TRANSACTION TYPE | % OF SMRs |
|---------------------------------------------------|-----------|
| International funds transfer out of Australia | 59 |
| Domestic electronic funds transfer out of account | 15 |
| Domestic electronic funds transfer into account | 10 |
| International funds transfer into Australia | 9 |

CORRESPONDENT BANKING SERVICES

Correspondent banking is the provision of banking services by one bank (the correspondent bank) to another bank (the respondent bank). Such arrangements are common in Australia's foreign bank branch subsector.³⁴ Respondent banks may be provided with a wide range of services, including cash management, international transfers, cheque clearing and foreign exchange services.

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:

- 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.
- 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.

Correspondent banking services were identified in a quarter of the SMR sample. However, most reports involved the reporting entity attempting to recover funds on behalf of the respondent bank's customer after the individual was victim to fraud or scam-related activity. Few reports recorded the respondent bank's customer as the suspicious party.

³⁴ The parents of foreign bank branches in Australia include a number of very large global banks that maintain correspondent banking relationships with thousands of respondent banks. Foreign bank branches in Australia are able to access these respondent banks via their parent or regional headquarters.

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.


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* strengthens protections on correspondent banking. The new measures will 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 bank branches continue to conduct risk assessments aligned with FATF guidelines on correspondent banking services and the AML/CTF Act.**

DELIVERY CHANNELS

AUSTRAC assesses the delivery channels used by foreign bank branches to provide services to their customers present a **medium** inherent ML/TF vulnerability.

Across the subsector, customer contact and understanding of customer transaction patterns are relatively high, and most delivery arrangements are simple and direct. The subsector is exposed to some ML/TF risk with respect to the use of agent bank arrangements and third-party agents, but use of these arrangements is not widespread.

LEVEL OF CUSTOMER CONTACT

DIRECT CUSTOMER CONTACT

Despite a small ATM and branch footprint in Australia, foreign bank branches maintain a high level of direct contact with their customers. Particularly given the common types of products and services offered, nearly all initial banking relationships are established face-to-face, and ongoing correspondence and transaction instructions are handled by relationship managers.

Face-to-face and direct customer interaction allows staff to identify suspicious behaviour or unusual transaction requests in real time. Relationship managers have a comprehensive understanding of their customers, their business needs and transaction history, and can readily identify unusual or suspicious transaction requests. Relationship managers exist for both domestic and offshore customers, while some offshore customers have access to relationship managers in their resident jurisdiction.

The role of relationship managers in AML/CTF compliance and control

Corporate and institutional banking customers are commonly provided relationship managers by their respective financial institutions. Relationship managers often have comprehensive oversight of transactional activity, detailed knowledge of customer profiles and regular communication with their customers. This also places relationship managers in a unique position to identify and report suspicious behaviour.

Multiple SMRs demonstrate the important role relationship managers can play. In one scenario, a relationship manager was pivotal in identifying inconsistencies with stated business activities and identity documents at onboarding. This was reported to the respective compliance team and the customer's application was subsequently declined. In another scenario, a relationship manager conducted site visits and reported discrepancies with a customer's declared assets. After triggering ECDD, the respective foreign bank branch submitted an SMR based on possible tax evasion offences.

i AUSTRAC acknowledges the valuable reporting instigated by relationship managers and attributes many of the SMRs submitted during the reporting period to this function. AUSTRAC encourages the continued development of AML/CTF culture and awareness among relationship managers. AUSTRAC also promotes regular internal communication between this function and respective compliance teams.

While there is no evidence of employee corruption within the subsector, foreign bank branches should remain alert to the threat of trusted insiders (the role of trusted insiders is discussed on page 38). Given the niche and complex nature of corporate and institutional banking (e.g. investment services), a relationship manager would likely be able to disguise illicit activity.

REMOTE SERVICE DELIVERY

Across the subsector, remote services are often used, including receipt of transaction instruction via fax, email or post. However, typical risk associated with these delivery arrangements is largely mitigated as foreign bank branches almost always confirm the instruction with the customer via telephone or video call-back protocols prior to executing the transaction. Any attempt to fraudulently misrepresent the customer is also largely mitigated by a relationship manager's comprehensive understanding of their customer, business needs and usual transacting patterns.

Some reporting entities also use authenticated electronic means including Society for Worldwide Interbank Financial Telecommunications (SWIFT) as the preferred bank-to-bank payment system, or an authorised appointed delegate. With the latter, transaction instructions are sometimes supported by written confirmation.

Online banking

Few foreign bank branches offer online banking services. Online banking services increase exposure to cyber-enabled fraud, such as online account openings and attempts to obtain financial benefit using stolen or fraudulent identities. Online banking services can also increase the speed and anonymity with which value can be moved between accounts and financial institutions.

While some reporting entities stated they intend to provide online banking services in the near future, they noted the service will allow customers to view their account details only. It will not have transaction functionality and will therefore not be exposed to further ML/TF risk.

COMPLEXITY OF PRODUCT DELIVERY ARRANGEMENTS

Across the subsector, outsourcing of service delivery and the use of third-party agents is minimal. It is largely restricted to several reporting entities and includes:

- agent bank arrangements with major domestic ADIs to accept cash deposits
- third-party agents or brokers in a syndicated loan arrangement.

While outsourcing to third parties can provide advantages such as greater accessibility for members and improved sophistication of services, using third parties can create vulnerabilities in the ability to detect and act upon suspicious activity. That being said, syndicated loan arrangements probably present a low ML/TF risk as the foreign bank branch is investing with other major financing companies and banks – all of which will be conducting due diligence on their customers. Nonetheless, reporting entities are ultimately responsible for the behaviour and compliance of third-party agents and brokers.

AGENT BANK ARRANGEMENTS

An agent banking arrangement consists of:

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

These arrangements carry ML/TF vulnerability because third-party ADIs do not have visibility or knowledge of customer transactional history, and are thus less likely to identify unusual activity. Agent banks also supply transactional details to reporting entities retrospectively, which can inhibit timely detection of suspicious transactions.

REPORTING OBLIGATIONS TO AUSTRAC

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.

FOREIGN JURISDICTIONS

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

Foreign bank branches 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 for their customers. All foreign bank branches are headquartered overseas (see table right) and half are domiciled in global financial centres or jurisdictions associated with money laundering, terrorism financing or tax evasion activities.³⁵

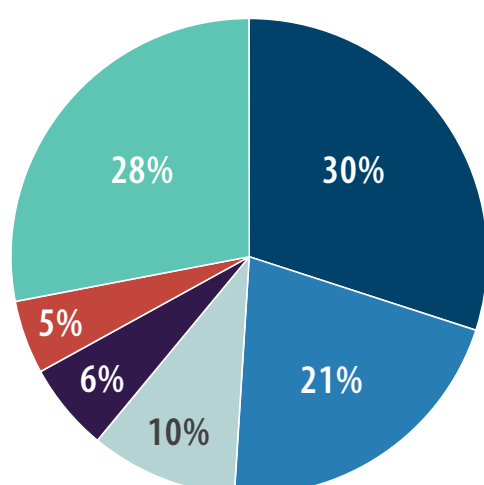
Exposure to foreign jurisdictions poses ML/TF risk because it creates opportunities for international movement of criminal proceeds and the funding of overseas terrorist activity. Further, transactions with foreign jurisdictions add complexity, helping to obscure beneficial ownership and beneficiary customers, and increase potential for offshore tax evasion.

LOCATION OF FOREIGN BANK BRANCH HEADQUARTERS

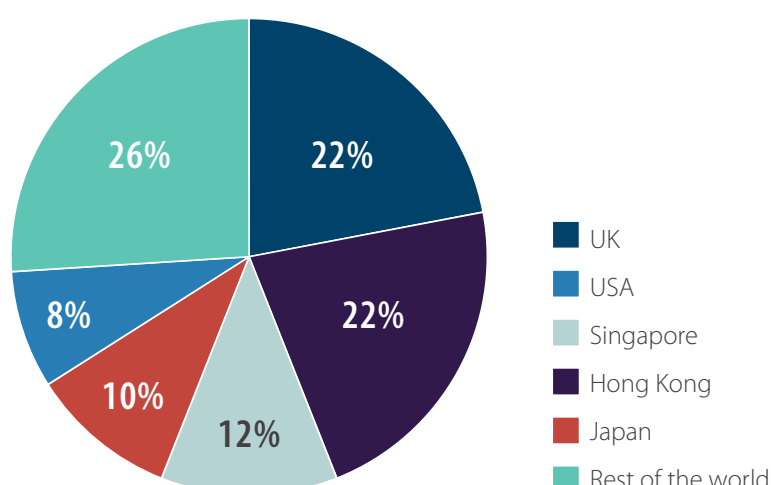
| REGION | NUMBER OF REPORTING ENTITIES |
|----------------------|------------------------------|
| Asia and the Pacific | 27 |
| Western Europe | 10 |
| North America | 9 |

MOVEMENT OF FUNDS OR VALUE INTERNATIONALLY

Incoming IFTIs (\$)



Outgoing IFTIs (\$)




³⁵ 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.

Foreign bank branches facilitate the international movement of a very large volume of funds into and out of Australia. In the reporting period, foreign bank branches submitted approximately 4.4 million IFTIs with a total value of \$1.02 trillion.³⁶ Incoming funds flows were more prevalent (approximately 60 per cent) than outgoing funds flows.

By subsector, the total value of IFTIs submitted by foreign bank branches is second only to Australia's major domestic banks. Particularly given the small customer base of foreign bank branches, this constitutes a significant vulnerability as it exposes reporting entities to ML/TF and a range of predicate offences.

Approximately half of the SMR sample involved an IFTI. The five most common foreign jurisdictions were the USA, Hong Kong SAR, China, India and Taiwan. The main suspected threat types identified in these reports were fraud, money laundering, scams and tax evasion. Only two of these jurisdictions (USA and Hong Kong SAR) appear in the top five source or destination IFTI jurisdictions. This suggests suspicious financial activity involving China, India and Taiwan are over-represented relative to the volume of transactions with these jurisdictions.

 To mitigate foreign jurisdiction risk, reporting entities can undertake ECDD processes, ensure effective transaction monitoring is in place and, where appropriate, escalate the approval process to senior management.

³⁶ IFTI-related figures associated with jurisdictions carry a 95 per cent confidence rating unless otherwise specified. Extremely small variations may exist for certain jurisdictions due to reporting anomalies, but these do not impact the findings made in this report.

TRANSACTIONS WITH HIGHER-RISK JURISDICTIONS

Foreign bank branches frequently transact with higher-risk jurisdictions, in particular a significant volume of funds flows through global financial centres (comprising 67 per cent of the total value of IFTIs submitted during the reporting period).³⁷

i While most transactions are likely to be associated with legitimate activities, it is critical foreign bank branches understand their customers' transactions with global financial centres in order to assess their risk exposure and detect criminal behaviour.

Because foreign bank branches often use correspondent banking services to effect international transfers, both the foreign bank branch and the respondent bank have oversight over international transfers. This may insulate the foreign bank branch from their foreign jurisdiction risk to some extent, if the respondent bank's AML/CTF processes are robust.

i As all reporting entities are different, foreign bank branches 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 bank branches). The result is significant financial flows into and out of these jurisdictions to support commercial activity.

In the reporting period, 67 per cent of IFTIs submitted by the subsector involved a global financial centre. Such vast transactional volumes provide opportunities for 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.

³⁷ 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 high risk for money laundering. This is because:

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

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

DETERMINING HIGH-RISK JURISDICTIONS

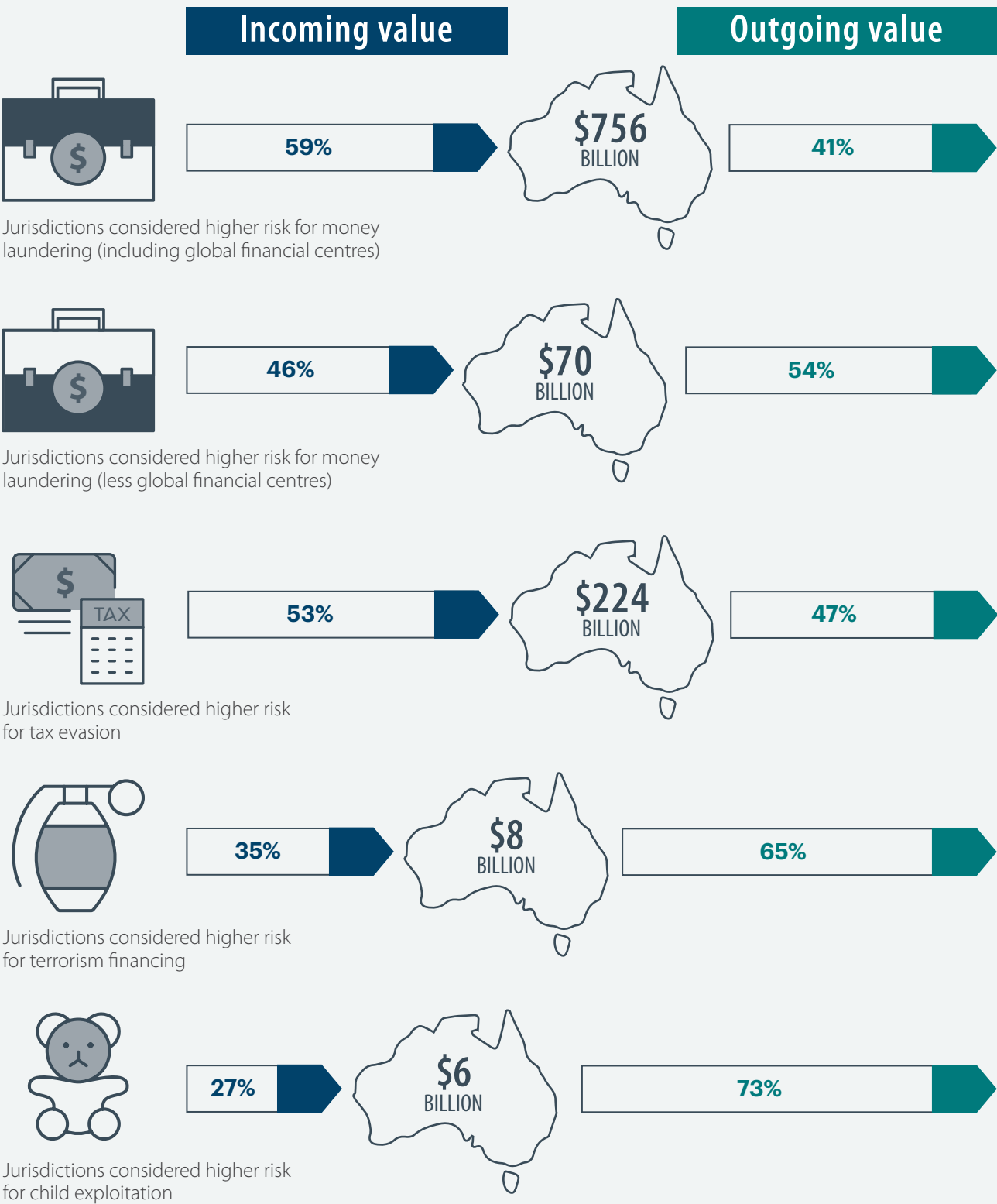
There is no one-size-fits-all list of high-risk jurisdictions. Reporting entities should adopt a risk-based approach when determining which jurisdictions to consider high risk for their business. AUSTRAC encourages the use of a range of sources that assess jurisdictions on different AML/CTF factors, 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.

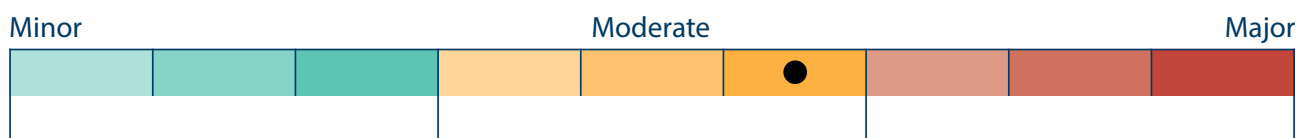
AUSTRAC has made its own determination about which jurisdictions are considered higher-risk for this report. This takes into account Australia-specific factors, such as top source or destination jurisdictions for higher-risk financial flows, as well as global factors, such as the strength or weakness 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



CONSEQUENCES



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

The consequences of ML/TF activity in the foreign bank branch subsector are assessed as **moderate**. Consequence refers to the potential impact or harm that ML/TF and other financial crimes may cause.

Financial crime that impacts foreign bank branches has consequences for customers, individual businesses, the subsector as a whole, and the broader Australian economy. The exploitation of foreign bank branches 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 bank branches has **minor** consequences for customers of the subsector.

Foreign bank branches report varying degrees of impact that criminal activity can have on their customers. This largely depends on the type of customer, their ability to detect criminal exploitation early, as well as their capacity to absorb potential financial losses. However, many customers in the subsector (corporate and wholesale clients) have mature fraud and scam management practices and controls in place, and are fairly resilient to criminal exploitation.

The frequent contact between many customers and their relationship manager also insulates against prolonged criminal exploitation. While some customers experience financial loss following criminal exploitation, the impact is largely mitigated by the foreign bank branch assuming associated costs.

Impacts of criminal activity on customers can include:

- financial losses from fraud and scams
- indirect costs associated with combating criminal attacks/cyber-enabled fraud, in particular IT security costs to build cyber resilience
- reputational damage, leading to loss of customers or increased public relations costs
- emotional distress.

INDIVIDUAL REPORTING ENTITIES AND THE SUBSECTOR

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

Most foreign bank branches report criminal activity can have a moderate to major impact on their Australian operation, as well as their broader business group. In some instances, particularly for many of the smaller reporting entities, this can include a decision by head office to withdraw operations in Australia. The subsector may also experience heightened criminal targeting should criminal entities identify certain foreign bank branches with insufficient AML/CTF programs.

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, partners or debtors
- reduced ability to attract investment and business, and skilled staff.

Operational impacts may include:

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

AUSTRALIAN FINANCIAL SYSTEM AND COMMUNITY

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

Significant or systemic breaches of AML/CTF controls could damage Australia's international economic reputation in relation to the security and safety of Australia's financial sector. This is particularly true given the size of the subsector's financial footprint in Australia and the significant value of transactions it facilitates. 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, fraud or scams
- reduced government revenue due to tax evasion, affecting the delivery of critical government services
- money laundering resulting in the preservation of illicit assets, the financing of new crimes and the corruption of public officials and private enterprise³⁸
- purchases of real estate with the proceeds of crime, driving property prices up and pricing legitimate buyers out of the market.

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

NATIONAL AND INTERNATIONAL SECURITY

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

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

RISK MITIGATION STRATEGIES

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

Many reporting entities indicate they have implemented comprehensive risk mitigation strategies, including CDD procedures, customer risk rating tools, product controls and transaction monitoring. However, some lack technological and data capabilities and improvements could be made to ensure:

- customer risk ratings are regularly reviewed and updated
- transaction monitoring programs are appropriately tailored to detect suspicious activity
- 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 bank branch 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, as well as the effectiveness of AML/CTF regimes in the jurisdiction in which a foreign bank branch is headquartered.

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

CUSTOMER DUE DILIGENCE

Foreign bank branches employ CDD checks to assess the legitimacy of customers and their business operations. New customer onboarding is usually conducted face-to-face, but CDD processes can vary depending on whether the client resides in Australia or overseas. In some instances, clients are referred from head office and reporting entities rely on customer information previously collected (and update as required). Many reporting entities indicate that customers who are assessed at onboarding as high risk are escalated to senior management for approval. Some reporting entities indicate they will decline a customer if they transact with specific high-risk jurisdictions.

Several reporting entities consulted for this report identified the following factors which may increase vulnerability to ML/TF and criminal misuse:

- **Reluctance to provide personal identity documents.** In some instances, reporting entities may experience challenges in collecting personal identity documents from directors, board members or staff of large corporations due to different expectations or regulations in these individuals' home jurisdictions. These individuals may question the need to provide personal identity documents as they are not individually a client of the foreign bank branch.
- **Customer risk ratings based on head office standards.** Foreign bank branches should not rely solely on customer risk rating systems used by head office. Reporting entities should ensure systems are appropriately tailored to the local risk environment and circumstances.
- **Failure to review customer risk ratings.** Some foreign bank branches do not conduct regular reviews of customer risk ratings³⁹ and some lack visibility of when and why a customer's risk rating is modified. Given the subsector's wide exposure to higher-risk customer types, customer risk ratings must be applied appropriately, regularly reviewed and updated

as required. Reviews should not simply be triggered by identification of adverse media, or an alert such as a PEP match or a transaction with a high-risk jurisdiction.

- **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.

ASSESSING PEPs

AUSTRAC reviewed multiple customer risk scoring tools and frameworks provided by foreign bank branches and observed a common approach of PEPs automatically being treated as high risk, irrespective of their ratings from other risk criteria. Several reporting entities also took a conservative view that 'once a PEP, always a PEP' and required individuals who were no longer PEPs to provide evidence and justification to remove the designation.

³⁹ Commonly reported timeframes for conducting customer risk reviews include extreme or high-risk customers every six to twelve months; medium-risk customers every two years; and low-risk customers every three to five years.

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

i Transaction monitoring programs need to be regularly reviewed and updated to remain effective. Reporting entities indicate reviews are conducted every six to 12 months, or when an event triggers a requirement to review a rule.

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.

Across the subsector, transaction monitoring programs vary significantly in sophistication, but are generally commensurate with the size, nature and complexity of individual operations. For example, smaller operations who only process several transactions per day will often manually review customer activity, while larger operations use well established and widely used third-party applications.

While automated transaction monitoring programs were often historically based on retail banking models, appropriate scenarios are now being integrated to detect suspicious and unusual activity across institutional banking products as well (e.g. correspondent banking and trade finance). These advancements will likely continue, particularly with the growth of new fintech and regtech market entrants.

Reporting entities indicate automated transaction monitoring programs generally include scenario-based profiles, business rules, parameters and alerts to detect suspicious or unusual activity. Following detection, transactions are escalated and analysis is completed to determine their legitimacy. Treatment options can then include:

- delay transaction until investigation is complete
- conduct more detailed analysis of transaction monitoring, including transaction patterns
- verify or re-verify CDD information
- verify source of wealth or beneficial ownership
- escalation to senior management.

INDEPENDENT REVIEWS

All foreign bank branches are required to 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 persons. This provides an objective mechanism to assess whether AML/CTF programs are appropriate and effective in detecting criminal misuse. Similar to reviews of transaction monitoring programs, reviews are either scheduled or in response to an event.

RISK ASSESSMENT

Across the subsector, there is wide 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 bank branches 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

Foreign bank branches report a very small number of SMRs – particularly given the vast number of transactions they process, and in comparison to other banking subsectors. The volume of SMR submissions also varies significantly between individual reporting entities. To some degree, this variation is consistent with the vast differences between reporting entities including scale of operations, customer base and complexity of products and services.⁴⁰ However, it also likely reflects varied levels of:

- understanding of ML/TF risks
- effectiveness of CDD, ECDD and transaction monitoring processes
- 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, 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.

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 bank branches to review these resources and consider if their reporting could be improved.

⁴⁰ For example, foreign bank branches are often involved in syndicated loans with other domestic and foreign ADIs. As such, numerous institutions are carrying out due diligence on the customer and the transaction, and the foreign bank branch may only see part of the transaction.

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

- **Include a more detailed grounds for suspicion.** This 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.
- **Avoid trigger-based reporting.** Trigger-based reporting is a practice in which a reporting entity submits a SMR solely on the basis of a trigger generated by their transaction monitoring system without conducting further investigation to form suspicion on reasonable grounds. This is similar to template reporting where there is little unique detail in the grounds for suspicion. Such reports provide little intelligence value and generally cannot be actioned.
- **Summarise suspicions.** Include 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.
- **Include 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.


During consultations, many foreign bank branch representatives had questions about SMR reporting. AUSTRAC encourages reporting entities to have policies and procedures in place to assist staff identify and report suspicious matters.

STAFF TRAINING

Foreign bank branches are required to:

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

All reporting entities consulted for this report indicated their staff complete compulsory AML/CTF training, both at induction and intermittently as required. Some reporting entities also require third-party AML/CTF accreditation, or require staff to demonstrate a certain level of competence. However, across the subsector, AML/CTF capability, capacity, maturity and culture of staff varies significantly.

 Some reporting entities could seek additional support for their AML/CTF officers from head office to ensure staff receive tailored training to account for all products and services offered. This will best equip AML/CTF officers to detect suspected misuse. For example, an AML/CTF officer must be sufficiently trained in TBML methodologies if trade finance is offered. Foreign bank branches who outsource CDD processes (or components thereof) should also ensure relevant parties are receiving appropriate and tailored training.



APPENDIX A: GLOSSARY

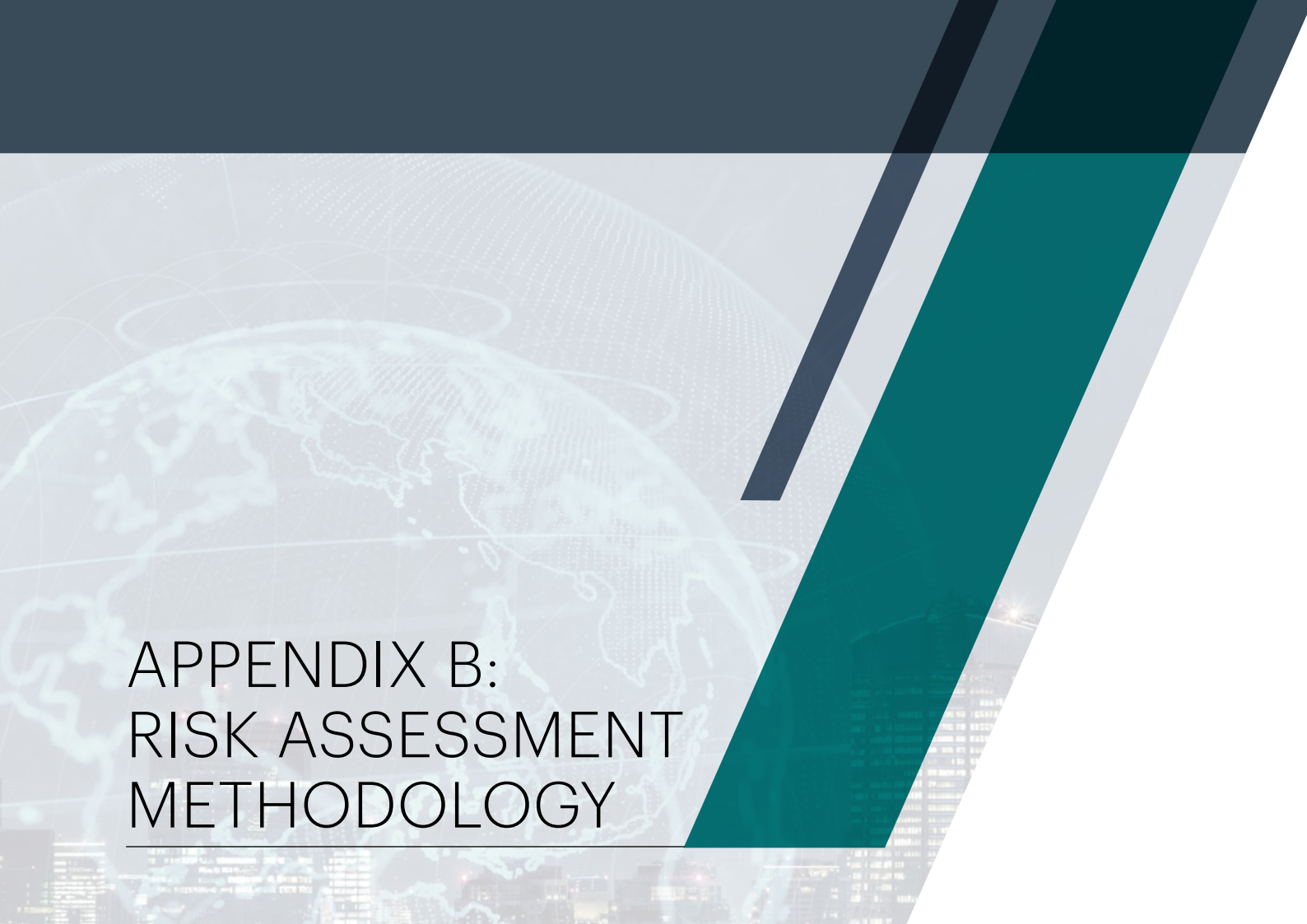
| NAME | DESCRIPTION |
|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------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

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

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

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

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



APPENDIX B: RISK ASSESSMENT METHODOLOGY

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

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

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

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

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

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



AUSTRAC.GOV.AU

