



Australian Government  
AUSTRAC

FIGHTING  
FINANCIAL  
CRIME  
TOGETHER



# REMITTANCE NETWORK PROVIDERS AND AFFILIATES IN AUSTRALIA

MONEY LAUNDERING AND TERRORISM FINANCING RISK ASSESSMENT

## COPYRIGHT

© Commonwealth of Australia 2022

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

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

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



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

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

## CONTACT US

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

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

# CONTENTS

---

<b>EXECUTIVE SUMMARY .....</b>	<b>4</b>
<b>PURPOSE.....</b>	<b>9</b>
<b>BACKGROUND .....</b>	<b>10</b>
<b>METHODOLOGY .....</b>	<b>13</b>
<b>REPORTING TO AUSTRAC.....</b>	<b>15</b>
<b>CRIMINAL THREAT ENVIRONMENT .....</b>	<b>18</b>
Money laundering .....	19
Terrorism financing.....	22
Predicate offences .....	24
<b>VULNERABILITIES .....</b>	<b>29</b>
Customers .....	30
Products and services .....	35
Delivery channels .....	39
Foreign jurisdictions .....	44
<b>CONSEQUENCES.....</b>	<b>48</b>
Customers .....	49
Individual reporting entities and the subsector .....	49
Australian financial system and community .....	50
National and international security .....	50
<b>RISK MITIGATION STRATEGIES.....</b>	<b>51</b>
<b>APPENDIX A: GLOSSARY .....</b>	<b>57</b>
<b>APPENDIX B: RISK ASSESSMENT METHODOLOGY .....</b>	<b>60</b>



# EXECUTIVE SUMMARY

A remittance service provider is an individual, business or organisation that accepts instructions from customers to transfer money or property to a recipient.<sup>1</sup> Remittance services are a crucial component of global financial inclusion, for example by allowing customers to send money to locations that traditional banking infrastructure may not service.

Remittance network providers (RNP) operating in Australia are businesses that allow affiliates to use their platform or operating system to process remittance transactions. Affiliates are independently-owned businesses that have an agreement with an RNP to use the network's brand, products, platforms or systems to provide remittance services. An RNP is responsible for an affiliate's registration and reporting obligations to AUSTRAC, and must ensure the affiliate has an appropriate AML/CTF program.

Based on AUSTRAC's Remittance Sector Register, 96 RNPs and 4,510 affiliates were considered in-scope for this report and these entities provide services to approximately 1.2 million customers. For the purposes of this assessment, RNPs and their affiliates are referred to as the **RNP subsector** or **the subsector**.

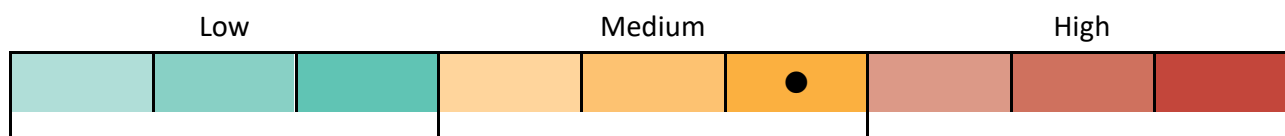
The characteristics and activities of individual businesses across the subsector vary significantly. This means that the money laundering and terrorism financing (ML/TF) risks associated with individual businesses vary, as does their ability to mitigate these risks. The methodology used in this assessment is designed to capture an overall inherent risk rating for the subsector.

---

<sup>1</sup> Remittance service providers are also known globally as 'money transfer businesses'.



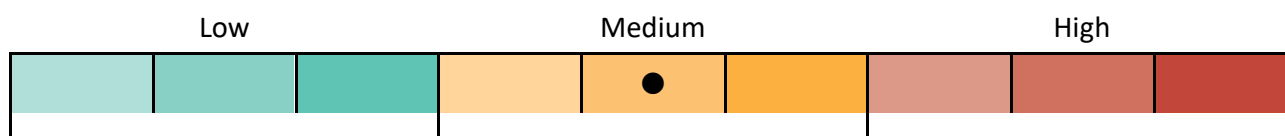
## OVERALL RISK RATING



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

Where possible this assessment considers the risks associated with the RNP subsector in the context of AUSTRAC's entire reporting population.

## CRIMINAL THREAT ENVIRONMENT



AUSTRAC assesses the threat of ML/TF facing the RNP subsector as **medium**.

While low-to-mid level offending dominates the criminal threat environment facing the subsector, exploitation by serious and organised crime groups is also present. Most instances of criminal misuse involve low-value transactions, however, there is also evidence of some large-scale money laundering activity linked to frauds and other crimes.

The primary threats facing the subsector are frauds, money laundering, scams, child exploitation and drug trafficking. The subsector is also exposed to terrorism financing, however, because RNPs and affiliates are often just one layer in a larger international terrorism financing process, the true nature and extent of this activity is likely obscured.

Under- and non-reporting of suspicious matter reports (SMRs) to AUSTRAC remains common in the subsector. Additionally, one-third of SMRs reviewed for this report did not include sufficient details to determine a threat type. While AUSTRAC has increased its guidance and outreach to the subsector in recent years, SMR statistics may not reflect the true extent of the criminal threat facing RNPs and their affiliates.

To address these gaps, this risk assessment uses intelligence holdings produced by AUSTRAC and partner agencies, as well as consultations with industry representatives and partner agencies, to inform the criminal threat picture.

### Money laundering

The nature and extent of money laundering facing the RNP subsector is assessed as **medium**.

Money laundering was the second most common threat impacting the subsector. Suspected instances of money laundering had moderate associated values. Some reporting entities are used by money launderers and members of serious and organised crime groups, particularly to move cash-based domestic criminal proceeds offshore.

The RNP subsector is primarily exploited in the placement and layering phases of the money laundering process.<sup>2</sup> This is because many reporting entities accept cash transactions and specialise in moving funds quickly and at low cost. Criminals wishing to launder funds often seek out reporting entities they perceive to have poor or inconsistent record-keeping practices.

<sup>2</sup> The money laundering process involves three stages: placement, layering and integration. These terms are defined in the **Glossary** at **Appendix A**.

## Terrorism financing

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

While the overall terrorism financing threat to the RNP subsector has declined in recent years, the subsector continues to be exposed to terrorism financing. The subsector submitted a low-to-moderate volume of terrorism financing-related SMRs during the reporting period, however, AUSTRAC and partner agency consultations indicate the actual extent of terrorism financing is likely to be higher. Twenty-one per cent of all terrorism financing intelligence reports assessed for this report were linked to the subsector.

The overall value associated with known and suspected cases of terrorism financing in the subsector are generally low, and methods are largely unsophisticated.

## Predicate offences

The nature and extent of threat posed by predicate offending involving the RNP subsector is assessed as **medium**.<sup>3</sup>

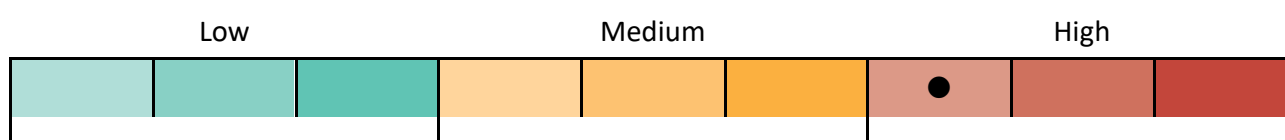
The RNP subsector is exposed to a variety of predicate offences. Most offending appears to be opportunistic, largely unsophisticated and low in associated value. However, some sophisticated and high-value offending has also been observed.

The key predicate offences impacting the subsector are frauds, scams, child exploitation and drug trafficking. To a lesser extent the subsector is also exposed to tax evasion.<sup>4</sup>

Frauds and scams represent more than half of all predicate offences identified by the subsector. Investment fraud, identity fraud and romance scams were the most common types, however, in a significant portion of SMRs the type of suspected scams and frauds was not clear.

The RNP subsector is also exploited to pay for access to child exploitation material, as well as to facilitate 'grooming' and child sex tourism.

## VULNERABILITIES



AUSTRAC assesses the RNP subsector faces a **high** level of inherent ML/TF vulnerability.

Significant factors exposing the subsector to ML/TF vulnerabilities include:

- high exposure to cash, which presents opportunities for money laundering
- products and services that can be used to rapidly move funds, particularly remittance services
- a number of complex product delivery arrangements, specifically:
  - use of offsetting arrangements, which can help mask the ultimate beneficiary and complicate detection of illicit funds flows<sup>5</sup>

<sup>3</sup> For the purposes of this report, a predicate offence is a criminal offence that generates proceeds of crime, or other related crimes such as identity fraud.

<sup>4</sup> For the purposes of this report 'tax evasion' is defined as the non-payment or under-payment of taxes, including duties on goods or services. This definition includes the use of cash payments to avoid or under-declare tax on personal or business earnings. The term 'tax evasion' does not include the legitimate use of legal tax minimisation strategies.

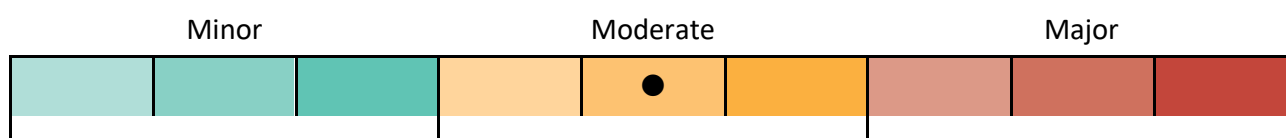
<sup>5</sup> Offsetting is a method of value transfer using reciprocal debit and credit arrangements between businesses.

- the RNP-affiliate operational structure, which lengthens the remittance supply chain and can create difficulties with identifying and reporting suspicious transactions
- outsourcing, which lengthens the product-delivery chain and reduces the level of oversight a reporting entity might have over customers and transactions. This can include intermediaries such as super-agents<sup>6</sup>
- high exposure to foreign jurisdictions, including higher-risk jurisdictions.

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

- a moderately sized customer base
- a moderate proportion of higher-risk customers, including known and suspected criminals, and overseas-based ordering customers.<sup>7</sup>

## CONSEQUENCES



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

### Customers

Criminal activity can have **moderate** consequences for customers of RNPs and affiliates. The most significant impacts for customers relate to financial loss, and emotional distress as a result of fraud and scam-related offences.

### Individual reporting entities and the subsector

The perceived or actual threat of criminal activity can have **moderate** financial, reputational or operational consequences for RNPs, affiliates, and the subsector. In some instances this can lead to the de-banking of reporting entities, particularly smaller RNPs which may be perceived as having less sophisticated risk mitigation strategies.

### Australian financial system and community

Significant or systemic criminal exploitation of the subsector could result in **moderate** damage to Australia's financial system and community. The subsector's modest financial footprint and concentration of activity in a small number of products and services moderates this harm.

Criminal activity also poses harms to the Australian community, including societal harms associated with offences such as child exploitation and drug trafficking.

### National and international security

Criminal exploitation of the RNP subsector can have **moderate** 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. Serious and organised crime groups in Australia can grow larger and stronger if they are able to launder their illicit funds through the subsector, and their activities can impact both national and international security.

<sup>6</sup> A super-agent is any intermediary engaged by an RNP to provide a range of administrative services to their network of affiliates, including compliance and reporting obligations. Super-agents are discussed further on page 41.

<sup>7</sup> Known or suspected criminals were identified by data-matching partner agency criminal lists against AUSTRAC reports. Further details of data-matching activities is provided in the **Methodology** section.

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

## RISK MITIGATION STRATEGIES

Many reporting entities indicate they have implemented risk mitigation strategies consistent with their obligations under the AML/CTF legal framework, including customer due diligence (CDD) procedures, customer risk rating tools, product controls, and transaction monitoring.

Risk mitigation strategies are not evenly applied across the subsector and vary in their sophistication. Some reporting entities have mixed approaches to their CDD activities, deliver limited or no AML/CTF training to their employees, or generally lack a good understanding of their AML/CTF obligations.

The quality and quantity of SMR submissions across the subsector could also be improved. Reduced or low quality SMRs can reduce the amount of financial intelligence available to AUSTRAC and partner agencies, and hamper the ability to detect criminal activity.

Improvements could also be made to the implementation of risk mitigation strategies to ensure:

- CDD processes, including on-going and enhanced CDD procedures, are optimised to meet compliance requirements for corporate customers, not just individual customers
- proof of a customer's source of funds is sought for all unusual and suspicious remittance requests, not just high-value transactions
- increasing due diligence and monitoring on overseas correspondents where transactions are conducted outside the banking system
- RNPs provide their affiliates with a robust AML/CTF program and the capacity to understand and effectively implement it.



## PURPOSE

This assessment provides specific information to the RNP subsector on the ML/TF risks it faces at the national level. Its primary aim is to assist the subsector 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 individual businesses 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 businesses individual operations.

### ASSESSING ML/TF RISK IN AUSTRALIA'S REMITTANCE 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 two risk assessments on Australia's remittance sector that are being completed under this program of work. The other assessment focuses on independent remittance dealers. This approach recognises the different structures within Australia's remittance sector, each facing unique ML/TF risks which may not necessarily be shared across the entire sector.

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

## BACKGROUND

### REMITTANCE SERVICE PROVIDERS IN AUSTRALIA

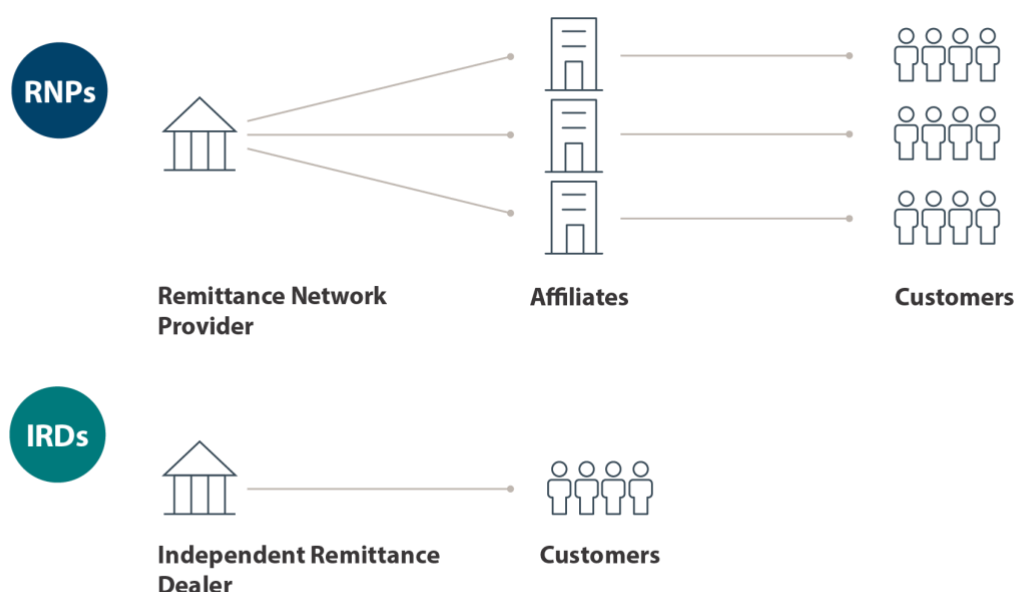
Remittance service providers operating in Australia offer fast and relatively low-cost methods of transferring funds domestically and overseas. These services are particularly important for migrant communities and expatriate workers supporting families in their countries of origin.

Remittance service providers must be registered with AUSTRAC and recorded on the [Remittance Sector Register](#). They must be registered as one or more of the following: an RNP, an affiliate of an RNP or an independent remittance dealer.

- An **RNP** operates a network of affiliates that use the RNP's brand, products, platforms or systems to provide remittance services to customers. An RNP is responsible for an affiliate's registration and reporting obligations to AUSTRAC, and must ensure the affiliate has an appropriate AML/CTF program.
- An **affiliate** has an agreement with an RNP to provide remittance services. Under the agreement the affiliate accepts instructions directly from customers to send funds to a recipient in another location. Affiliates are independently-owned, and the RNP does not exercise control over other activities or services provided by the business.
- **Independent remittance dealers (IRDs)** can be registered as a single entity operating independently, or own and operate multiple branches. They use their own products, platforms or systems to provide remittance services directly to customers. Please refer to AUSTRAC's [ML/TF risk assessment of independent remittance dealers](#) for further information regarding risks specific to these businesses.

AUSTRAC issues a separate registration for each type of remittance service provider. A remittance service provider can maintain multiple registrations with AUSTRAC concurrently. For example, one remittance service provider can be registered as an RNP and IRD at the same time.

The key difference between the RNP subsector and IRDs lies in the control of the business and reporting obligations to AUSTRAC. Specific registration requirements and AML/CTF reporting obligations exist for each type of remittance service provider. Refer to the [guidance for remittance service providers](#) on the AUSTRAC website for further information.



## RNP SUBSECTOR

During the reporting period there were 96 RNPs and 4,510 affiliates operating in Australia. The subsector provided services to an estimated 1.2 million customers.<sup>8</sup>

The number of registered RNPs increased by almost a quarter from 2015 to 2020. However, the number of registered affiliates has decreased by eight per cent. Reporting entities consulted for this report indicate the subsector is likely to continue expanding over the next five years, although growth could be hampered by COVID-19-related impacts on customer numbers and RNP operations. Growth will likely be driven by the registration of online businesses, which generally have lower operating costs and offer greater convenience for customers.

The COVID-19 pandemic led to a temporary decline in customer numbers and transaction volumes. Industry experts project these figures will recover and outgrow pre-pandemic levels over the next five years.<sup>9</sup> These trends are further discussed in the **Customers** section on page 30.

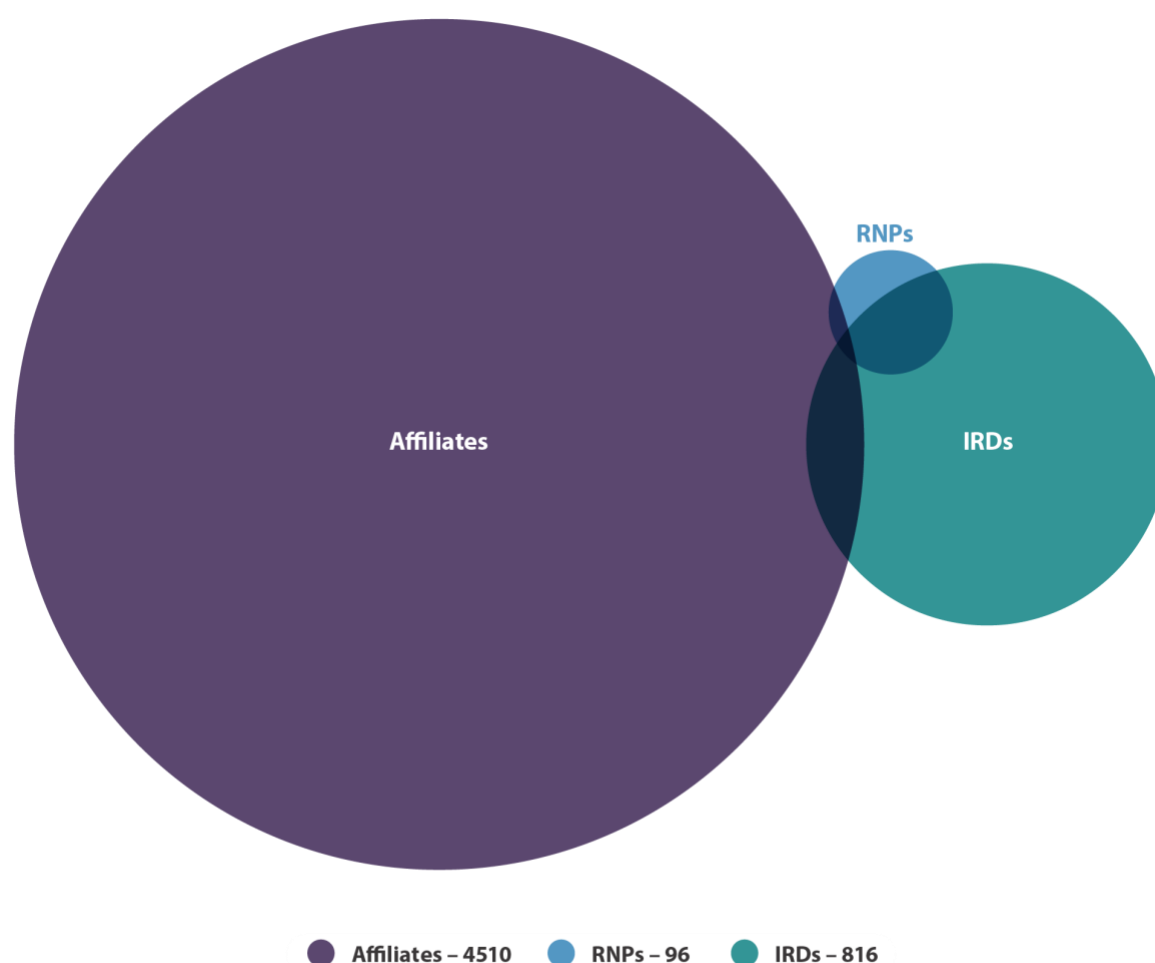


Figure 1: Number of registered remittance service providers in Australia during the reporting period

<sup>8</sup> This number was derived from analysis of IFTIs submitted by RNPs and affiliates in the reporting period. It is an approximation only.

<sup>9</sup> IBISWorld, *Industry at a Glance – OD5114 Money Transfer Agencies in Australia*, IBISWorld, January 2021, accessed 12 July 2021.

Under the provisions of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act), RNPs are required to maintain a compliant, risk-based AML/CTF program and report to AUSTRAC:

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

Reporting entities are also required to provide AUSTRAC with annual AML/CTF compliance reports.

Across the subsector, the characteristics and activities of individual businesses vary significantly. There is a high level of diversity in the size and scale of operations including the type and number of customers, the volume and value of transactions processed, and foreign jurisdictions serviced. Consequently, the ML/TF risks associated with individual businesses also vary.

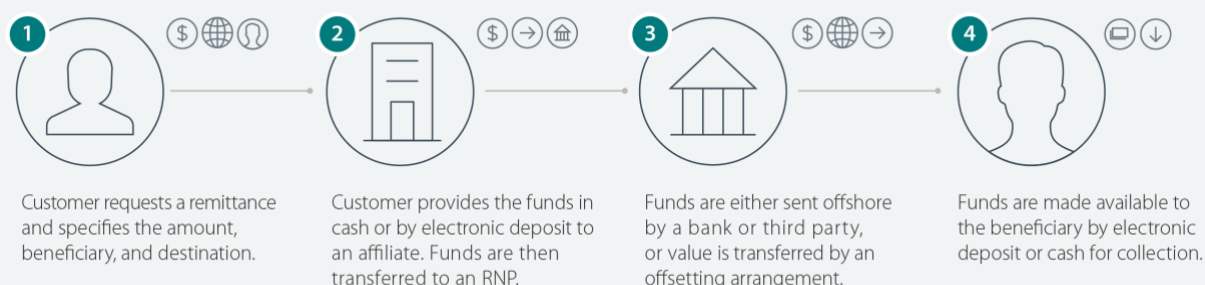
AUSTRAC acknowledges not all risks will be relevant for every reporting entity. In addition, some risks relate to the nature of remittance activity in general, and are not attributes specific to the subsector. The risk rating criteria used in this assessment is designed to capture an overall rating for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

## A TYPICAL REMITTANCE SERVICE

While specific procedures vary between reporting entities, transactions tend to follow a similar pattern. The following provides an overview for a typical outgoing transaction:

1. The customer contacts the affiliate in-person, via phone or online and requests a remittance transaction. They specify the value, beneficiary and jurisdiction details.
2. The customer provides the funds to the affiliate. Funds can be provided in cash or deposited electronically into the affiliate's bank account.
3. Depending on whether an affiliate has a bank account or not, funds will be transferred electronically via bank transfer or a third-party service provider to the RNP. The RNP then transfers the funds offshore via international bank transfer, agent or third-party service provider in the destination country, or the value will be transferred through an offsetting arrangement.
4. Funds are then deposited electronically into the beneficiary's account or made available for collection as cash from a local agent.

## A TYPICAL REMITTANCE SERVICE



## METHODOLOGY

The methodology used for this risk assessment draws on Financial Action Task Force (FATF) guidance that assessment of 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 individual businesses 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 are encouraged to 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 to criminal misuse.

Further information on methodology and how it was applied to the subsector is 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 a sample of 744 SMRs that the RNP subsector submitted between 1 April 2018 and 31 March 2019 (the **SMR sample**).<sup>10</sup> See the call-out box **Labelling the SMR sample** on page 14 for more details.
2. A comprehensive review of 1,100 AUSTRAC and partner agency intelligence reports produced between January 2017 and May 2020; 10 per cent of these reports related to the RNP subsector (the **IR review**).<sup>11</sup>
3. The results of data-matching (the **data-matching exercise**) of IFTIs, TTRs and SMRs submitted to AUSTRAC by the RNP subsector between 1 January 2019 and 31 December 2019 and criminal entities who were:
  - recorded as a member of a significant national or transnational criminal group as at May 2020
  - charged with a money laundering or proceeds of crime-related offence between 1 January 2017 and 31 December 2018
  - charged with a terrorism-related offence between 1 January 2014 and 31 December 2018.

<sup>10</sup> SMRs should be considered indicative of suspicious behaviour only and not conclusive in their own right. This is because reporting entities generally lack visibility of certain threat elements, for example how a customer generates suspected criminal proceeds. To ensure accuracy of ML/TF indicators (threats and vulnerabilities) outlined in the SMR sample, AUSTRAC officers manually reviewed and categorised each report.

<sup>11</sup> 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.



4. Open source information, including public-facing information produced by Commonwealth agencies, academic institutions, reporting entities and the media.
5. Feedback and professional insights offered during interviews and consultations with a range of partner agencies and reporting entity representatives, as well as industry experts and industry associations.

## LABELLING THE SMR SAMPLE

SMRs are indicative of suspicious behaviour only and are not conclusive evidence of criminal activity in their own right. For example, reporting entities often have no visibility of how a customer generates criminal proceeds. As a result, reporting entities are unable to include specific information regarding 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 jurisdictions.

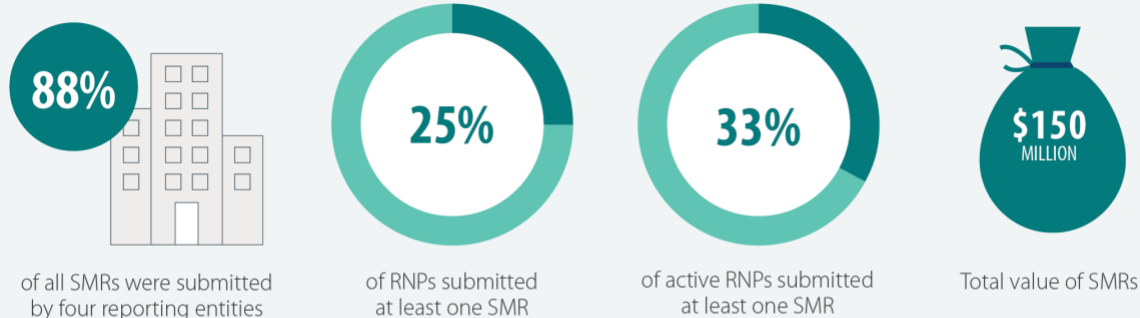
For example, a single SMR could be categorised with multiple labels as follows:

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

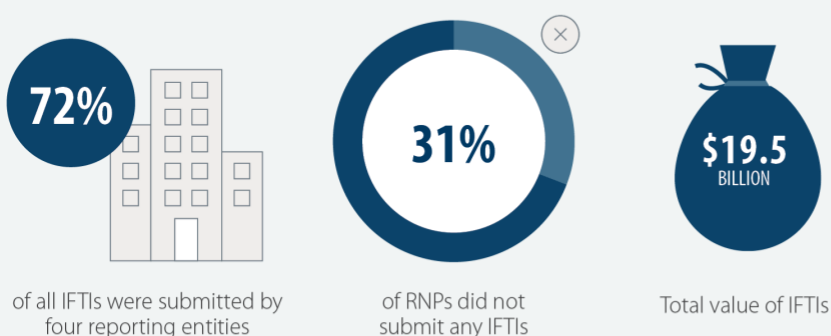
## REPORTING TO AUSTRAC

### REPORTS SUBMITTED BY THE SUBSECTOR BETWEEN 1 APRIL 2018 AND 31 MARCH 2019<sup>12 13</sup>

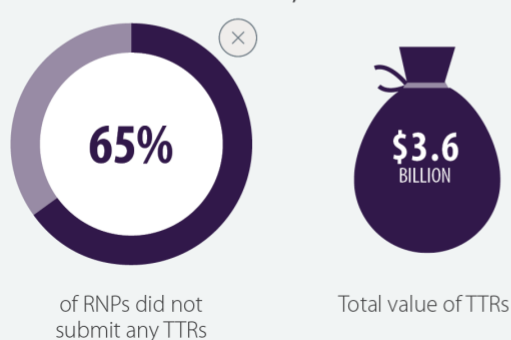
**SMRs** Number of SMRs: 19,142



**IFTIs** Number of IFTIs: 8.3 million



**TTRs** Number of TTRs: 54,332



<sup>12</sup> Caution should be exercised when interpreting the recorded value in SMRs. The recorded value may not necessarily relate to suspected criminal misuse or terrorism financing, and may include 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.

<sup>13</sup> 'Active RNPs' is defined as an RNP that has submitted at least one IFTI in the reporting period

## SMR SUBMISSIONS

Across the subsector SMR submissions are unevenly distributed and under- or non-reporting is common. Four RNPs accounted for 88 per cent of all SMR submissions in the reporting period, and most RNPs did not submit any SMRs in this timeframe. A concentration in SMR reporting is generally in line with the market concentration of the subsector, although SMR reporting is more highly concentrated in the top four RNPs than IFTI reporting.

In addition, one-third of SMRs lacked sufficient details to determine the nature of criminal threat. Refer to **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 6,000 users from more than 35 of AUSTRAC's partner agencies to inform their intelligence gathering efforts and investigations.

## IFTI SUBMISSIONS

IFTI submissions are concentrated in the largest RNPs, with the top four IFTI reporters accounting for almost three-quarters of all submissions. Almost a third of RNPs did not submit an IFTI during the reporting period, suggesting they were not actively providing remittance services during this period.

### Why are IFTIs important to AUSTRAC and its partner agencies?

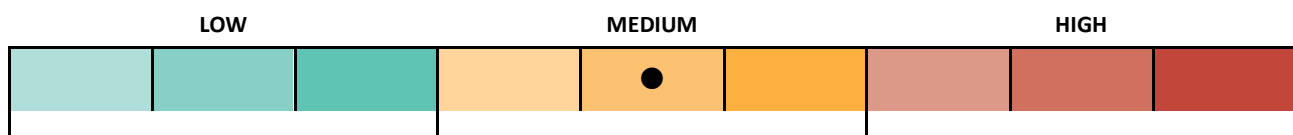
IFTI reporting drives a significant portion of AUSTRAC's intelligence work. The information in IFTI reports are an integral component of AUSTRAC's strategic and tactical intelligence outputs, and contributes to domestic and foreign partner agency investigations. IFTIs close a critical intelligence gap by capturing the overseas component of the money laundering cycle that transnational, serious and organised crime groups commonly exploit.

Reporting of IFTIs enables AUSTRAC and our partner agencies to follow funds flows into and out of Australia (including proceeds of crime). This critical financial intelligence enables AUSTRAC and its partners to 'connect the dots' and identify criminal syndicate members and their locations.

IFTI reporting contributes to investigations by Commonwealth, State and Territory law enforcement, revenue protection agencies, and national security and intelligence agencies into a range of criminal activities including but not limited to:

- fraud
- tax evasion
- illegal tobacco
- illegal firearms
- drug trafficking
- modern slavery
- cyber-enabled crime
- child sex exploitation
- bribery and corruption
- illegal trade in fauna and flora
- trade-based money laundering.

# CRIMINAL THREAT ENVIRONMENT

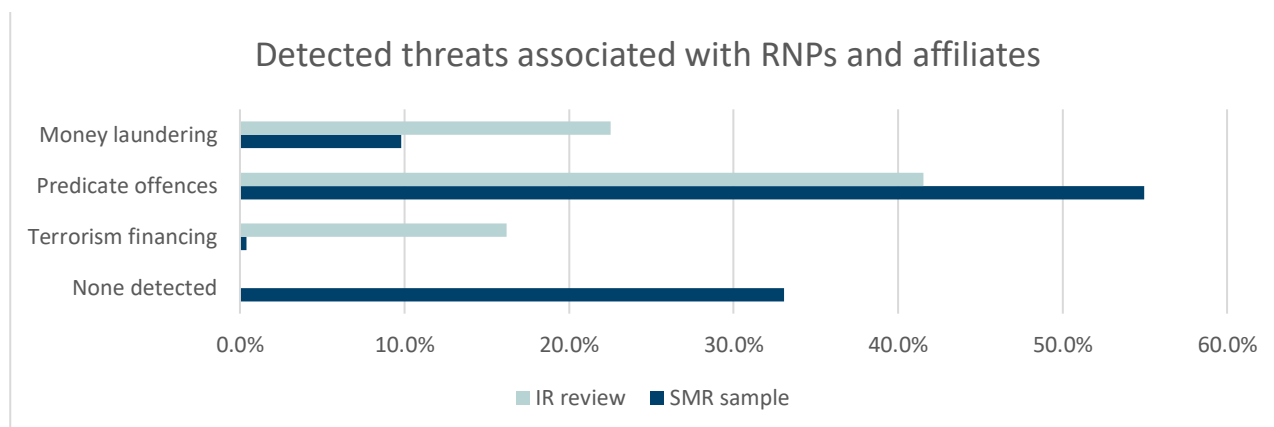


CRIMINAL THREAT ENVIRONMENT FACTOR	RATING
MONEY LAUNDERING	●
TERRORISM FINANCING	●
PREDICATE OFFENCES	●

AUSTRAC assesses the criminal threat environment facing the RNP subsector as **medium**.

The criminal threat environment refers to the nature and extent of ML, TF and predicate offences associated with the RNP subsector.





Fraud is the primary threat facing the subsector, followed by money laundering, scams, and child exploitation.

There is a medium risk of money laundering in the RNP subsector, some of which is sophisticated or linked to serious and organised crime groups. Values associated with suspected instance of money laundering were moderate. Some reporting entities are exploited by money launderers and members of serious and organised crime groups, particularly to move cash-based domestic criminal proceeds offshore.

The overall threat of terrorism financing in the RNP subsector has declined in recent years, however, the subsector continues to be moderately exposed to known and suspected cases of terrorism financing.

The subsector is also moderately exposed to a variety of predicate offences, most of which are opportunistic, largely unsophisticated and low in associated value. The key predicate offences impacting the subsector are frauds, scams, child exploitation and drug trafficking.

Under- and non-reporting of SMRs remains common in the subsector. While AUSTRAC has increased its guidance and outreach to the subsector in recent years, one-third of reports in the SMR sample did not provide sufficient details to determine a threat type. Given these gaps, the SMR sample likely understates the extent of criminal activity impacting the subsector. Findings from the IR review and consultations with industry representatives and partner agencies were therefore critical in informing the criminal threat picture.

## MONEY LAUNDERING

AUSTRAC assesses the nature and extent of money laundering threats facing the RNP subsector as **medium**.

Suspected money laundering was identified in 10 per cent of the SMR sample and 23 per cent of the IR review.<sup>14</sup> Associated values were generally moderate. The average value of money laundering-related reports in the SMR sample was \$16,000 and no SMRs exceeded \$1 million. Approximately 19 per cent of money-laundering-related intelligence reports identified aggregate transactions valued in excess of \$1 million.

Money laundering was the third most common threat among the SMR sample although AUSTRAC assesses this underrepresents the extent of activity in the subsector due to underreporting.

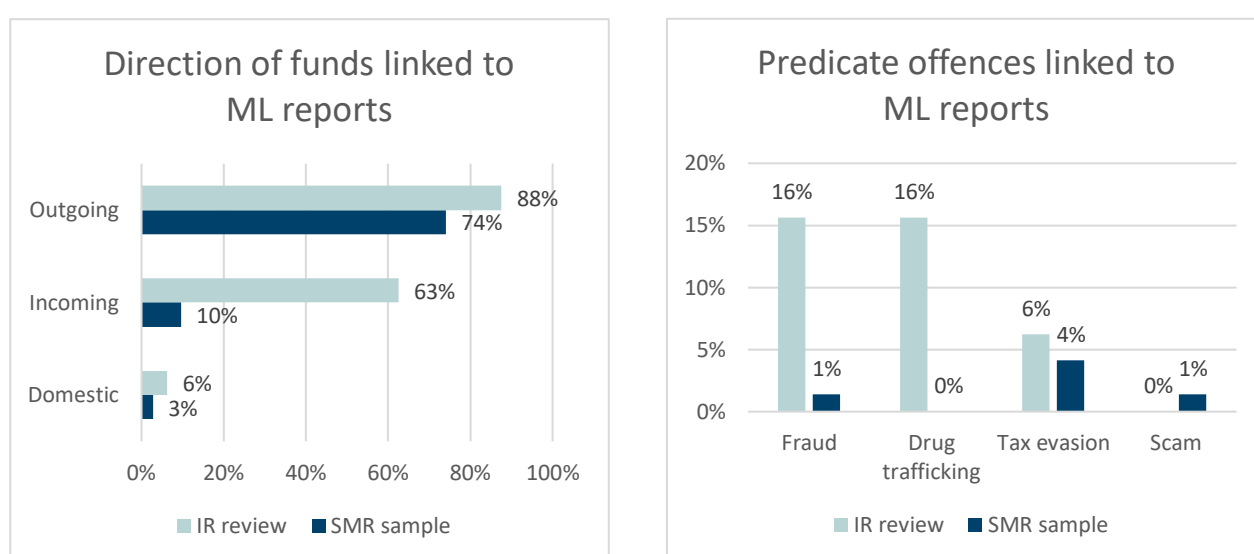
Partner agency information and the results of the data matching exercise indicate that money launderers and serious and organised crime groups use the subsector, particularly to move cash-based

<sup>14</sup> 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).

domestic criminal proceeds offshore. These reports indicate more sophisticated exploitation, with at least one report of a known member of a transnational money laundering organisation using the subsector to remit funds.

The RNP subsector is primarily exploited in the placement and layering phases of the money laundering process. This is because many RNPs and their affiliates accept cash and can move funds quickly and at low cost. A frequently identified method to try and obscure the source of funds or ultimate beneficiary of a remittance is conducting multiple transactions across a range of financial institutions, such as domestic and foreign banks, as well as currency exchanges.

Almost three-quarters of money laundering SMRs involved outgoing transactions. The most common foreign jurisdictions noted in the money laundering-related SMRs were Vietnam, the Philippines, India and Lebanon. Most suspected money laundering activities are linked to key proceeds-generating predicate offences in Australia such as frauds, drug trafficking and tax evasion. These are discussed in detail in the **Predicate offences** on page 24



Common indicators of suspected money laundering activity observed in the SMR sample and IR review include:

- unexplained source of funds
- structuring cash payments to avoid reporting thresholds
- funding remittances with multiple debit cards or cash payments
- remittances to jurisdictions inconsistent with a customer's profile
- remittances involving a higher-risk jurisdiction (see page 45 for more details)
- several customers opening accounts within a short period of time, in a seemingly coordinated manner
- a customer enquiring about transaction limits or requesting their name be omitted from the transaction
- separate individuals making remittances to the same recipient, with no apparent connection between the sender and recipient
- transactions that do not align with a customer's expected activity, for example high-value transactions by a customer supplying a backpacker hostel as a residential address.



Suspicious incoming international transactions were far more commonly observed in the IR review than were reported in the SMR sample (63 per cent versus 10 per cent). Reporting entities should ensure they apply appropriate risk mitigation strategies to overseas ordering customers – including robust CDD processes and tailored transaction monitoring – and report suspicious transactions to AUSTRAC.

## SUSPECTED LAUNDERING OF DRUG TRAFFICKING PROCEEDS

Over a four month period in 2018, several foreign nationals transferred a total of approximately \$100,000 from Australia to countries known for the production or transshipment of narcotics. The amounts were inconsistent with the senders' stated occupations (e.g. 'student') and were sent from different locations in a structured manner, often to common beneficiaries. This activity triggered transaction monitoring rules at two RNPs, which submitted SMRs that prompted further AUSTRAC analysis. This analysis identified a network of likely money mules who were laundering criminal proceeds.

## Cash-based money laundering

Partner agencies consider cash transactions to be one of the most significant money laundering-related risks to the subsector. This is because criminal proceeds are often derived in cash and the subsector generally accept cash. To some extent, this risk is moderated where reporting entities impose transaction limits because criminals generally prefer to make fewer, larger transactions – particularly when laundering large amounts of money.

Cash transactions were commonly observed in money laundering-related reports in the SMR sample (79 per cent) and IR review (84 per cent). Indicators of cash-based money laundering may include:

- large transactions
- unexplained wealth
- structured payments for remittances
- use of money mules and other third-parties
- multiple transactions with no apparent economic rationale.

## AFFILIATE'S AUSTRAC REGISTRATION CANCELLED

In 2021, AUSTRAC cancelled the registration of an affiliate after its director and owner was convicted of conducting structured deposits. The individual conducted six structured cash deposits valued at \$50,000 into the bank account of a student visa holder within a two hour period.



Reporting entities that facilitate cash transactions should remain vigilant of the associated risks and continue strengthening their systems and controls to mitigate the illicit use of cash.

## TERRORISM FINANCING

AUSTRAC assesses the nature and extent of terrorism financing threats facing the RNP subsector as **medium**.

This assessment is based on a low-to-moderate number of SMRs submitted by the subsector, a relatively high number of terrorism-financing related reports in the IR review, and consultations with intelligence partners.

This assessment is lower than determined in previous AUSTRAC assessments and reflects shifting terrorism financing behaviour. While historically some RNPs and their affiliates have been used to send funds to support terrorist organisations and foreign terrorist fighters, the current terrorism financing threat environment in Australia is dominated by self-funded activity, or attempted attacks that require little to no funding.

Despite the shifts in the terrorism financing environment, the RNP subsector is still exposed to terrorism financing. For example:

- The subsector were identified in 21 per cent of all terrorism financing intelligence reports assessed in the IR review.
- Terrorism financing was identified in 20 per cent of all intelligence reports linked to the subsector.
- The subsector submitted 66 terrorism financing-related SMRs.<sup>15</sup> This represents nine per cent of terrorism financing-related SMRs submitted by all reporting entities during this period.
- The data matching exercise identified a moderate number of customers of the subsector that have been charged with terrorism-related offences (see **Higher-risk customers** for further details).

Associated transaction values in the SMR sample and IR review were generally low, and terrorism financing methods were largely unsophisticated.<sup>16</sup> In most cases little effort was made to obfuscate the source or destination of funds.

Common themes of the SMR sample and IR review include:

- use of cash
- SMR transaction values under \$1,000
- remittances to higher-risk jurisdictions
- law enforcement enquiries or media reporting triggering suspicions
- using descriptions like 'family support' or 'charitable donation' for the remittance
- predominantly individual customers, however several non-profit organisations were also noted.

<sup>15</sup> Determined by keyword analysis of all AUSTRAC SMRs submitted between 1 April 2018 to 31 March 2019.

<sup>16</sup> The average associated value of reports in the SMR sample was \$11,500. However, almost all of these reports recorded the total cumulative sum of multiple transactions linked to the customer over a long period of time. In some instances, more than 100 transactions were recorded in a single SMR.

## 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 emergence of 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 lone actors or small groups. These actors and groups primarily conduct small-scale, low-cost terrorist attacks. 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 are likely to have limited the ability for foreign fighters to return to Australia. These restrictions also likely affected 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 also occur. Please refer to AUSTRAC's [ML/TF risk assessment of non-profit organisations](#) for more detail.

Although many RNPs and affiliates have stated they forbid transfers to conflict zones, neighbouring jurisdictions are often attractive alternative destinations. For example, a remittance may be sent to a location serviced by an RNP or affiliate, and the funds then physically smuggled across land or maritime borders into a nearby conflict zone.

Remittance transfers to regions adjoining conflict zones can also be difficult to distinguish from legitimate remittances intended to support displaced persons. Tactics such as diverting genuine charitable donations, or terrorist-affiliated organisations using funds for ostensibly benign reasons such as construction projects, further complicate the picture.

Common indicators of terrorism financing include:

- a customer remitting funds to multiple beneficiaries in a higher-risk jurisdiction
- multiple customers remitting funds to the same beneficiary, especially in jurisdictions deemed higher-risk for terrorism financing
- open source reporting that any parties to the transaction have links to known terrorist entities or activities.

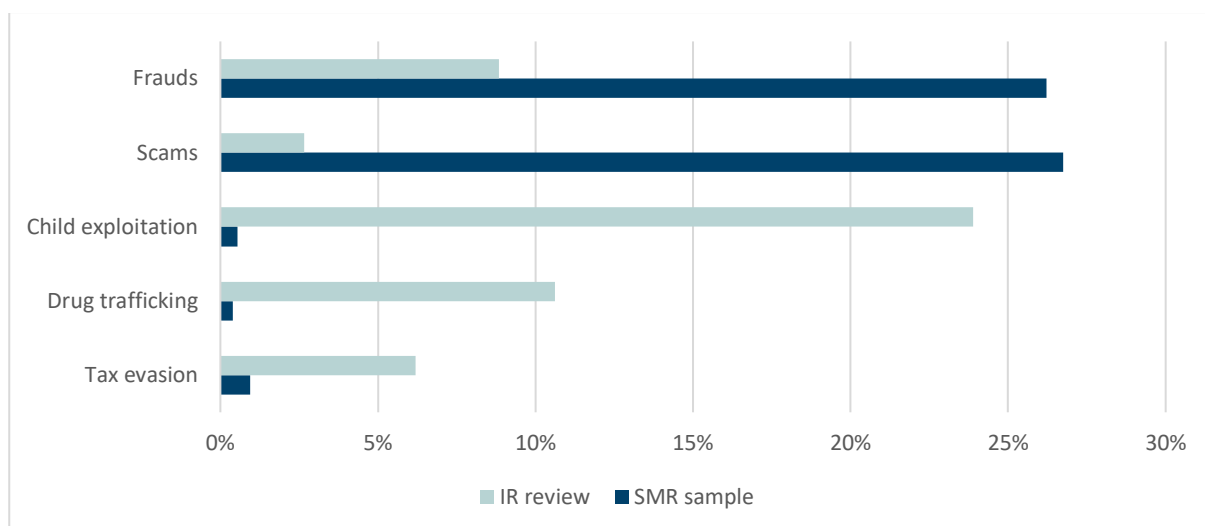


## PREDICATE OFFENCES

AUSTRAC assesses the nature and extent of threat posed by predicate offending involving RNPs as **medium**.

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

The key predicate offences impacting the subsector are frauds, scams, child exploitation and drug trafficking. To a lesser extent, the subsector is also exposed to tax evasion.



### IDENTIFYING PREDICATE OFFENCES – A CHALLENGE FOR REPORTING ENTITIES

The actual extent of predicate offences involving RNPs and affiliates is almost certainly higher than is represented in the SMR sample. Approximately one-third of all SMRs reviewed did not identify a discernible criminal offence – these were largely submitted because of suspicious transactional activity.

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 an RNP or affiliate to identify because it occurs outside of the remittance process altogether, unlike frauds, which often involve a remitter 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.

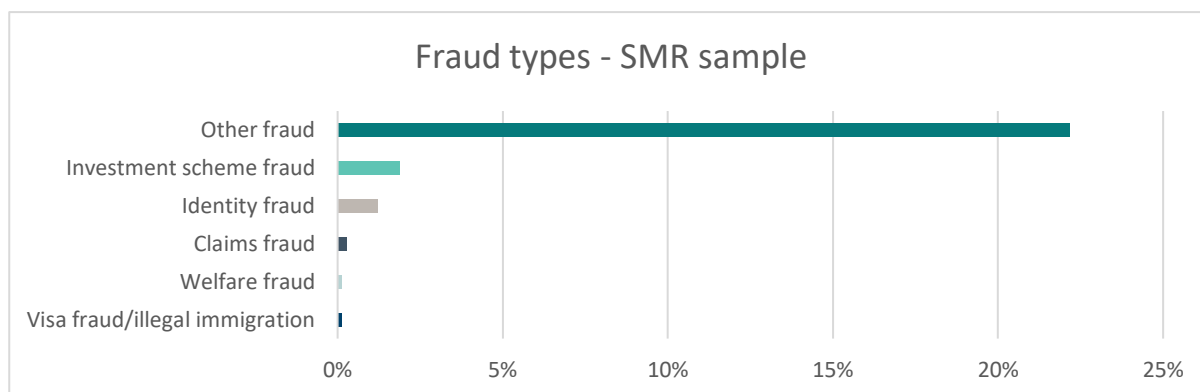


SMRs that do not identify a predicate offence can still contain important pieces of intelligence that form part of a bigger picture of offending. Reporting entities should remain vigilant of key criminal market trends in Australia and report any suspicions of related financial transactions to AUSTRAC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

## Frauds

Frauds were the second most commonly identified predicate offence in the SMR sample (26 per cent) and the third most common in the IR review (nine per cent).<sup>17</sup>

Most fraud-related SMRs did not contain enough detail to determine the type of fraud. Where fraud types were discernible, investment scheme fraud and identity fraud were most common. Most suspicious transactions involved the Philippines, Nigeria, USA, Ghana, and South Africa. Associated values were generally low-to-medium, averaging \$7,200.



Far fewer suspected frauds were observed in the IR review, likely because intelligence reports often highlight more serious criminality with higher associated values. For example, organised investment fraud schemes involving millions of dollars.

The subsector is attractive to fraudsters because offenders can receive cash payments at locations across Australia and the world which cannot be easily recovered once collected. The remittance sector may also be perceived as being subject to less scrutiny than other sectors, such as banks.

Reporting entities consulted for this report identified the following as common indicators of potential fraud:

- purchases made through split transactions
- transfers described as 'processing fees', 'shipping charges' or similar
- payments to supposedly Australian companies that are sent overseas
- multiple transfers from various Australian locations to one overseas agent
- customers who appear to be receiving instructions from a third party over the phone
- payment of purported fines or taxes via remittance rather than into a government account
- customers who cannot substantiate a relationship with the beneficiary, or do not appear to have ties to the jurisdiction.



Reporting entities consulted for this assessment say that some customers deny being a victim to fraud or scam activity, and it can be difficult to dissuade these customers from proceeding with a remittance. Some reporting entities will refuse to process the transaction, while others will proceed once they have explained their concerns to the customer. AUSTRAC reminds reporting entities to submit an SMR in these circumstances as they can provide valuable intelligence to partner agencies investigating frauds or scams.

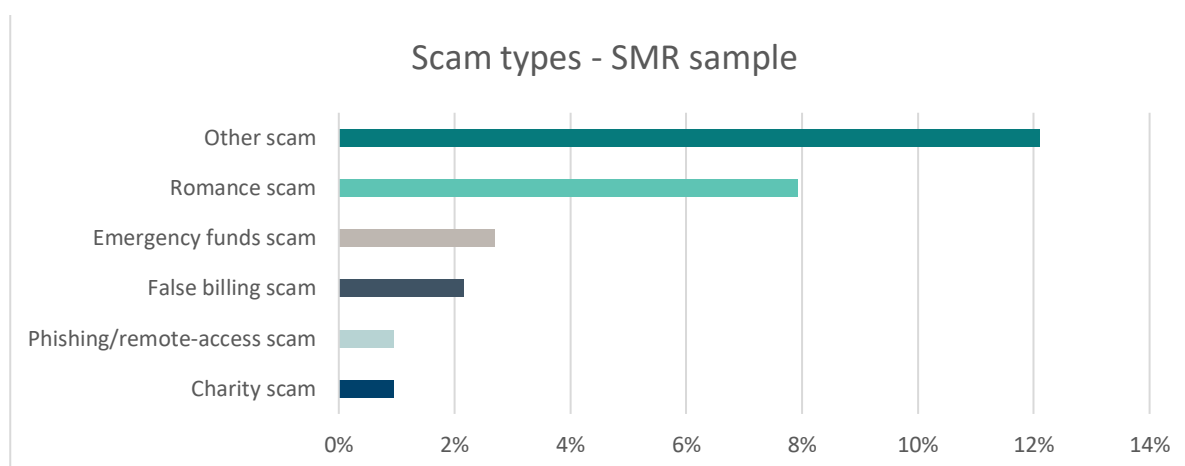
<sup>17</sup> The IR review understates the true extent of frauds impacting the subsector as intelligence reporting usually details serious or organised criminal offending only. Opportunistic, low-volume fraud activity generally is not reported.

## Scams

Scams were the most commonly identified predicate offence in the SMR sample (27 per cent) and the fifth most common in the IR review (three per cent).<sup>18</sup>

A significant number of SMRs did not contain enough detail to determine the actual type of scam. Where scam types were discernible, romance scams, emergency funds scams and false billing scams were most common. Most suspicious transactions involved Nigeria, USA, the Philippines, Ghana, and China. Associated values were generally low, averaging \$4,600.

Scam offenders usually provide victims with instructions to use a remitter to send funds offshore. The offender may instruct victims to make deposits into a domestic bank account that they control, which is then quickly remitted offshore.



### SCAMMER INSTRUCTS VICTIM BY PHONE

One reporting entity consulted for this report described an instance whereby a third party scammer instructed a customer to remit funds to an unknown recipient. The customer received a series of instructions via phone specifying the value, destination and ostensible purpose of the attempted remittance, as well as coaching on what to say to the reporting entity's staff.



While reporting entities may not always have details of the scam, where further details become known and a suspicion is formed, AUSTRAC reminds RNPs and their affiliates of their obligation to submit an SMR.

## Child exploitation

Child exploitation was identified in less than one per cent of the SMR sample but was the most common predicate offence in the IR review (25 per cent).

Intelligence from AUSTRAC and partner agencies also demonstrates that the RNP subsector is used to facilitate payments for access to child exploitation material, as well as to facilitate 'grooming' and child sex tourism. For example, the RNP subsector facilitated 36 per cent of transactions in a recent sample of outgoing offshore remittances linked to known child exploitation offenders in Australia.

<sup>18</sup> The IR review understates the true extent of scams impacting the subsector as intelligence reporting usually details serious or organised criminal offending only. Opportunistic, low-volume scam activity generally is not reported.

Remittance services allow rapid movement of funds to child exploitation facilitators who are frequently based in jurisdictions where remittance services are a prominent part of the financial system.



The potential harms associated with child exploitation are significant. Reporting entities must remain vigilant to key risk indicators of child exploitation activity and report suspicious transactions to AUSTRAC.

## IDENTIFYING CHILD EXPLOITATION ACTIVITY

Identifying transactions linked to child exploitation can be challenging as transaction values can appear legitimate or confused with potential fraud activity.

The following financial indicators are drawn from the 2019 Fintel Alliance paper [\*Combating the sexual exploitation of children for financial gain\*](#):

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

## Drug trafficking

Drug trafficking was identified in less than one per cent of the SMR sample but was the second most common predicate offence in the IR review (11 per cent).

Most partner agencies rank drug trafficking as one of the top predicate offences to money laundering in Australia. The ACIC estimates Australians spent almost \$13 billion on illicit drugs in 2020-21.<sup>19</sup>

The data-matching exercise identified approximately \$7 million in transactions linked to members of serious and organised crime groups, many of which are involved in drug trafficking. While this figure almost certainly includes legitimate transactions, it is likely an under-representation of the actual extent to which known and suspected criminals transact with the subsector.<sup>20</sup>

AUSTRAC acknowledges that without law enforcement information, it is very difficult for reporting entities to distinguish transactions linked to drug proceeds from other money laundering activities. This almost certainly accounts for the low number of SMRs indicating drug-related activity. SMRs that had a direct link to drug activity were usually based on low-level suspicious behaviour such as

<sup>19</sup> Australian Criminal Intelligence Commission (ACIC), *Estimating the costs of serious and organised crime in Australia, 2020–21*, ACIC, Australian Government, 2022, accessed March 25 2022.

<sup>20</sup> This is because the data matching exercise only included a sample of known or suspected criminals and reflects transactions that were subject to an SMR, TTR or IFTI submitted by the subsector. Given issues with the quality of reporting across the subsector (including false- and non-reporting), it is almost certain suspicious transactions linked to these entities were not identified.

references to drugs in transaction descriptions, or were triggered by law enforcement enquiries or adverse media reporting.

### **Tax evasion**

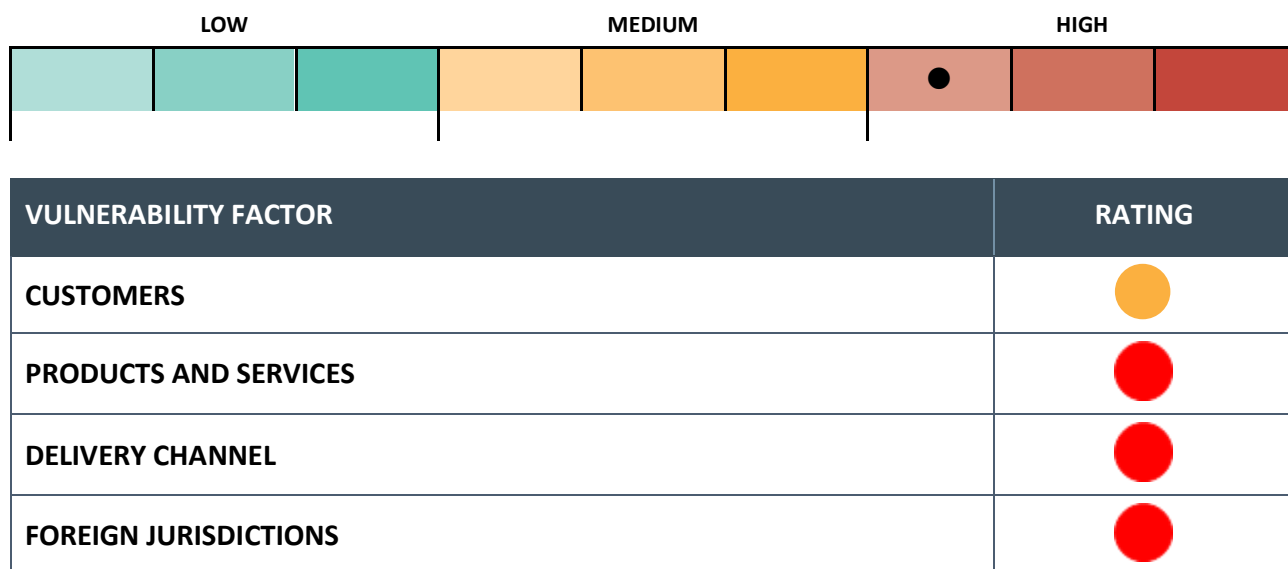
Tax evasion was the third most common predicate offences in the SMR sample (one per cent) and the fourth most identified in the IR review (six per cent).

Instances of suspected tax evasion were confined to personal income tax evasion in the SMR sample. This is consistent with the subsector's customer base, which is primarily individuals. Common themes of these SMRs include:

- structured cash deposits
- outgoing international transactions
- transactions to higher-risk jurisdictions
- customers being evasive or uncooperative when questioned about the purpose of the transaction

The majority of tax-related reports in the IR review, however, involved a company or business. This is likely because intelligence reporting usually details serious or sophisticated offending, which often involves the use of corporate structures.

# VULNERABILITIES



AUSTRAC assesses that the RNP subsector is are subject to a **high** level of inherent ML/TF vulnerability. Vulnerability refers to the characteristics of a subsector that make it susceptible to criminal exploitation.

AUSTRAC’s vulnerability assessment falls into four broad categories: customers, products and services, delivery channels, and exposure to foreign jurisdictions.

## CUSTOMERS

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

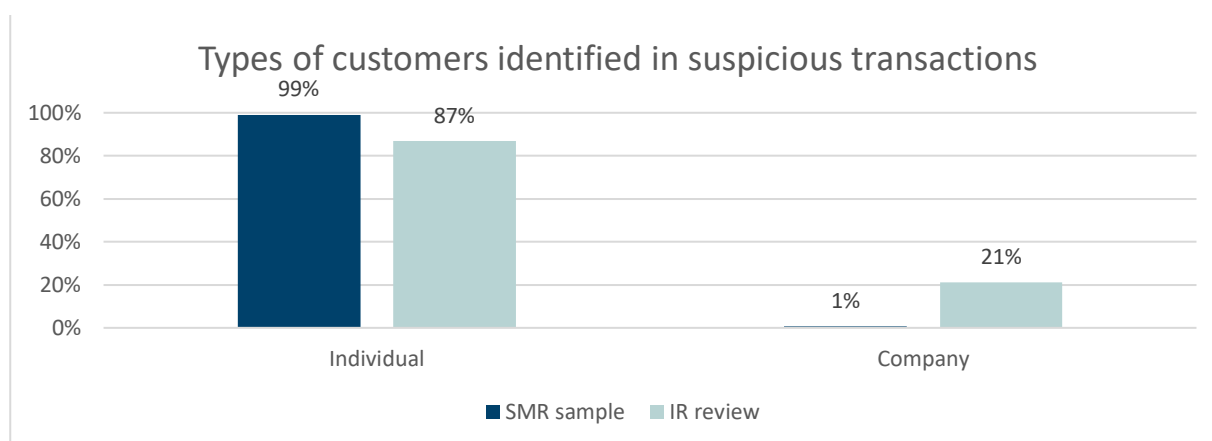
This vulnerability stems from a moderately-sized customer base and exposure to some higher-risk customers, including known and suspected criminals, overseas-based customers, and some companies, trusts and other legal entities.

### Size of the customer base

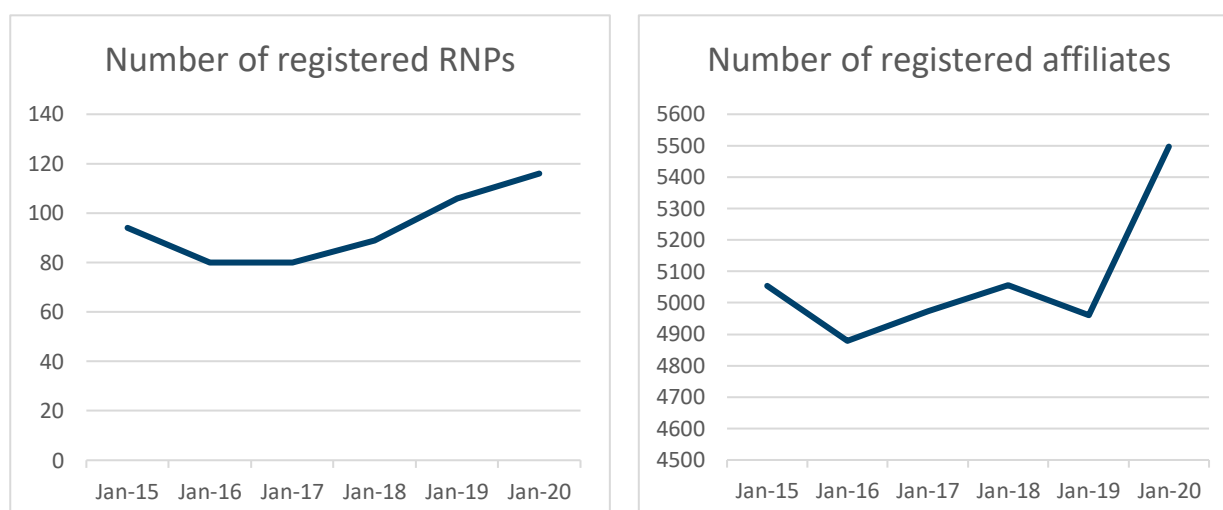
The RNP subsector has a moderately-sized customer base compared to other financial sectors regulated by AUSTRAC, serving an estimated 1.2 million customers.<sup>21</sup>

There is considerable diversity in the size of reporting entities' customer bases. Some large multi-national businesses may serve thousands of customers per day, while small affiliates may only serve a handful a month.

The subsector primarily services individual customers, although some reporting entities provide services to companies, trusts and other legal entities. Individual customers can pose a lower ML/TF vulnerability compared to corporate, trust or other legal entity customers. This is because these entities can more easily obscure beneficial ownership, the source of funds, or the purpose of transactions.



The number of registered RNPs increased by almost a quarter from 2015 to 2020. However, the number of registered affiliates has decreased by eight per cent.



<sup>21</sup> This number was derived from analysis of IFTIs submitted by RNPs and affiliates in the reporting period. It is an approximation only.



## IMPACT OF COVID-19 ON CUSTOMER NUMBERS

The COVID-19 pandemic led to a temporary decline in the subsector's customer numbers due to the closure of international borders, government-imposed lockdowns, and some migrant workers returning to their home countries.

Reporting entities that relied on face-to-face transacting were most likely to suffer customer losses as a result of the pandemic, either because they were forced to close their retail stores or because of customer reluctance to transact in-person.

Over the next five years, industry experts expect customer numbers and transaction volumes to recover and steadily grow. This growth is largely contingent on global containment of COVID-19 and open international borders. Growth will likely be driven by the registration of online businesses, which generally have lower operating costs and offer greater convenience to customers.<sup>22</sup>

## Higher-risk customers

AUSTRAC assesses the RNP subsector is exposed to a moderate number of higher-risk customers. This assessment is based on industry consultations, compliance report data, the SMR sample, the data-matching exercise and qualitative insights from partner agencies.

Higher-risk customers can present across several categories including:

- known or suspected criminals
- overseas-based customers
- companies, trusts and other legal entities
- politically exposed persons (PEPs).

## INDUSTRY CUSTOMER RISK RATINGS

Approximately 65 per cent of reporting entities that submitted a compliance report in 2020 advised they do not service high-risk customers. At the subsector level, RNPs and affiliates reported a moderate number of high-risk customers.



AUSTRAC acknowledges that reporting entities who service high-risk customers do sometimes apply risk treatment strategies. However, the sophistication and effectiveness of these strategies varies considerably. Unsophisticated approaches to assessing customer risk is likely to account for the high proportion of the subsector that reported not having any high-risk customers. Refer to **Risk mitigation strategies** for further details.

<sup>22</sup> IBISWorld, Industry at a Glance – OD5114 Money Transfer Agencies in Australia, January 2021, accessed 12 July 2021 <https://my.ibisworld.com/au/en/industry-specialized/od5114/industry-at-a-glance>.

**Known or suspected criminals**




	MEMBERS OF SERIOUS ORGANISED CRIME		ENTITIES CHARGED WITH ML OR PROCEEDS OF CRIME OFFENCE		ENTITIES CHARGED WITH TERRORISM OR TF RELATED OFFENCE	
	PROPORTION OF POIs	VALUE	PROPORTION OF POIs	VALUE	PROPORTION OF POIs	VALUE
DATA-MATCHING RESULTS TO RNPs		\$\$		\$\$		\$
<b>LEGEND</b> \$ = Low    \$\$ = Medium    \$\$\$ = High						

Table 1: Results of data-matching exercise: Transaction reports matched to known and suspected criminals

AUSTRAC assesses a number of known or suspected criminals present a high inherent ML/TF vulnerability to the subsector. This assessment is based on the results of data-matching that identified the proportion of customers who were either:<sup>23</sup>

- recorded as a member of a serious and organised crime group as at May 2020
- charged with a money laundering or proceeds of crime-related offence between 1 January 2017 and 31 December 2018<sup>24</sup>
- charged with a terrorism-related offence between 1 January 2014 and 31 December 2018.<sup>25</sup>

Data matching identified:

- A high proportion of individuals charged with a money laundering-related offence were customers of the subsector. These individuals were linked to transaction reports totalling approximately \$140,000 during the reporting period.
- A moderate proportion of individuals charged with a terrorism-related offence were customers of the subsector. These individuals were linked to transaction reports totalling approximately \$300,000 during the reporting period.
- A low proportion of members of serious and organised crime groups were customers of the subsector. Those customers that were identified were linked to almost 2,000 transaction reports totalling approximately \$6.8 million during the reporting period.

Criminal entities are known to monitor the regulatory landscape and target businesses they perceive to be more vulnerable to ML/TF. This can include:

- avoiding businesses that have been subject to AUSTRAC regulatory action or adverse media
- avoiding businesses that employ robust customer screening and transaction monitoring
- targeting businesses perceived as likely to aid criminal activity or have weak AML/CTF controls.

<sup>23</sup> This analysis was completed on all IFTIs, TTRs and SMRs submitted by RNPs and affiliates between 1 January 2019 and 31 December 2019. A high, medium, or low rating reflects the number of individuals identified as customers of each subsector taken as a proportion of the total number of individuals in each category.

<sup>24</sup> Includes persons charged under Division 400 of the *Criminal Code* (Cth) and/or sections 81 and 82 of the *Proceeds of Crimes Act 2002* (Cth).

<sup>25</sup> Includes persons charged with a 'Terrorism offence' in section three of the *Crimes Act 1914* (Cth) and/or offences contrary to the *Crimes (Foreign Incursion and Recruitment) Act 1978* (Cth).

While the RNP subsector will remain attractive for criminal misuse because of the speed, reliability and global reach of transactions, and acceptance of cash, smaller reporting entities or those with weaker AML/CTF controls may be increasingly targeted by criminals.

### ***Overseas-based ordering customers***

Overseas-based ordering customers can pose higher inherent ML/TF vulnerability to reporting entities processing incoming international transactions. AUSTRAC estimates that incoming IFTIs accounted for approximately 12 per cent of IFTIs.<sup>26</sup>

The most significant vulnerabilities relate to on-boarding because Australian reporting entities rely on their foreign correspondents to conduct CDD and ECDD checks such as verifying identities and the source of funds. These processes can vary in effectiveness from one correspondent to another.

In addition, offshore-based customers may expose the subsector to criminal risks relevant to the threat environment in the customer's home jurisdiction. For example, transactions originating from a jurisdiction considered high-risk for drug trafficking may alter the risk profile of a customer sending funds from the jurisdiction.



AUSTRAC expects reporting entities who service overseas-based customers to understand and assess associated ML/TF risks and implement appropriate risk-based systems and controls to manage and mitigate these identified risks. This includes:

- ensuring CDD and ECDD procedures of overseas counterparts are robust
- considering risks associated with a customer's location, such as whether that jurisdiction presents a higher risk for ML/TF or other criminal offences, or lacks a robust AML/CTF regime.

### ***Companies, trusts and other legal entities***

Companies, trusts and other legal entities can expose a reporting entity to higher inherent ML/TF vulnerability. The extent of vulnerability depends on multiple factors including the industry, business-type, 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 or an offshore nexus. Entities that operate in sectors deemed more vulnerable to ML/TF – such as gambling, natural resource extraction, or DNFBPs – also pose higher risks to reporting entities.

Across the subsector, the overall number of non-individual customers is significantly lower than the number of individual customers. There is also wide variation in customer types among reporting entities. For example, some reporting entities do not provide services to non-individuals, while others provide services exclusively to non-individual customers.

Companies, trusts and other legal entity customers were not commonly observed in the SMR sample. However, they were observed in 41 per cent of money laundering-related intelligence reports and 21 per cent of predicate offence-related intelligence reports in the IR review. This suggests reporting entities are not identifying and reporting suspicious transactions linked to non-individuals. This aligns with information provided by some reporting entities during consultations for this report that transaction monitoring programs were often not optimised for non-individual customers (see **Risk mitigation strategies** for more detail).

<sup>26</sup> Statistics related to IFTI value are estimated accounting for errors in the reported source and destination jurisdictions. The uncertainty in estimated proportions is typically in the range 0.5 to 1 percentage points but can be as large as 5.

Customers that were companies, trusts or other legal entities were identified in just one per cent of the SMR sample and 20 per cent of the IR review.<sup>27</sup> Common themes observed in these reports include:

- high-value transactions
- complex or rapid transactions indicative of a fraud or scam
- false invoice scams committed against corporate customers
- lack of supporting documents to substantiate overseas business activity
- customers making purchases with no discernible relevance or connection to the business.

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.
- 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.
- When a criminal organisation own or control multiple entities, they can be used to under-invoice, over-invoice or double-invoice to transfer value. This method of trade-based money laundering can be used to move illicit money across borders undetected and to evade taxes.

Company shareholders are also typically legally protected from criminal liability through 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.



AUSTRAC expects RNPs and affiliate’s to continue strengthening their risk-based systems and controls to increase transparency and oversight of their customers’ beneficial owners and mitigate the inherent vulnerabilities of corporate customers and other legal entities. When a suspicion is formed because of obscure beneficial ownership or an unknown source of funds, AUSTRAC expects reporting entities to submit detailed SMRs.

### ***Politically exposed persons (PEPs)***

A PEP is an individual who holds a prominent public position or role in a government body or international organisation, either in Australia or overseas.<sup>28</sup> PEPs can be an attractive target for bribery and corruption given their capacity to influence government spending and budgets, procurement processes, development approvals, and grants.

<sup>27</sup> The discrepancy between figures from the SMR sample and IR review suggests reporting entities may not be identifying and reporting suspicious transactions linked to corporate customers. This aligns with information some reporting entities provided during consultations for this report that transaction monitoring programs were often not optimised for non-individual customers (see **Risk mitigation strategies**).

<sup>28</sup> Part 1.2.1 of 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. Further information on PEPs can be found on the AUSTRAC [website](#).

Overall, PEPs pose a low ML/TF risk to the subsector. No PEPs were identified in the SMR sample and a very low number were identified in the IR review (0.9 per cent). Just 11 per cent of reporting entities that submitted a compliance report in 2020 said they had PEP customers, with the subsector reporting approximately 200 PEPs in total.



AUSTRAC assesses the subsector is not widely exposed to PEPs. Nonetheless, reporting entities should remain vigilant to the ML/TF risk that PEPs can pose, and ensure risk-based procedures are in place to identify whether an individual customer or beneficial owner is a PEP. Reporting entities should do this before providing a customer with a designated service (or as soon as possible afterwards). See AUSTRAC's website for further guidance on identifying PEPs.

## PRODUCTS AND SERVICES

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

Vulnerability stems from the subsector's high exposure to cash, and products and services that are designed to move funds quickly and efficiently.

### Use of cash

#### TTRS AND CASH-RELATED SMRS BETWEEN 1 APRIL 2018 AND 31 MARCH 2019

Total number of TTRs submitted to AUSTRAC: **54,332**

Sum of TTRs: **\$3.6 billion**

Total SMRs submitted featuring cash: **77 per cent**

Sum of SMRs featuring cash: **\$198 million**

The number of SMRs containing a suspicious cash transaction increased from 64 per cent in 2015 to 91 per cent in 2019.

While overall cash use in Australia is declining, the RNP subsector continues to have a high exposure to cash. Consultations with reporting entities suggests there are a combination of reasons for this, for example:

- elderly customers may be more familiar with cash than online alternatives
- some culturally and linguistically diverse communities may prefer to deal in cash rather than bank transactions
- cash wage payments remain prevalent in some sectors of the economy, and customers seeking to remit funds often prefer to directly remit a portion of their cash income.

Acceptance of cash transactions provides convenience for some customers and access to the financial system for various segments of the Australian community, particularly the elderly and culturally or linguistically diverse communities.

Cash transactions also increase the subsector's exposure to the proceeds of crime – which are often derived in cash – and cash-based money laundering (see **Criminal threat environment** on page 21). Because of the anonymity associated with cash transactions they are also associated with the shadow economy and tax-related crimes (See **Tax evasion** on page 28).

Across the subsector, the extent of cash exposure for individual reporting entities varies (see figure 2). While some reporting entities are abandoning cash in favour of electronic payment methods, others operate exclusively in cash.

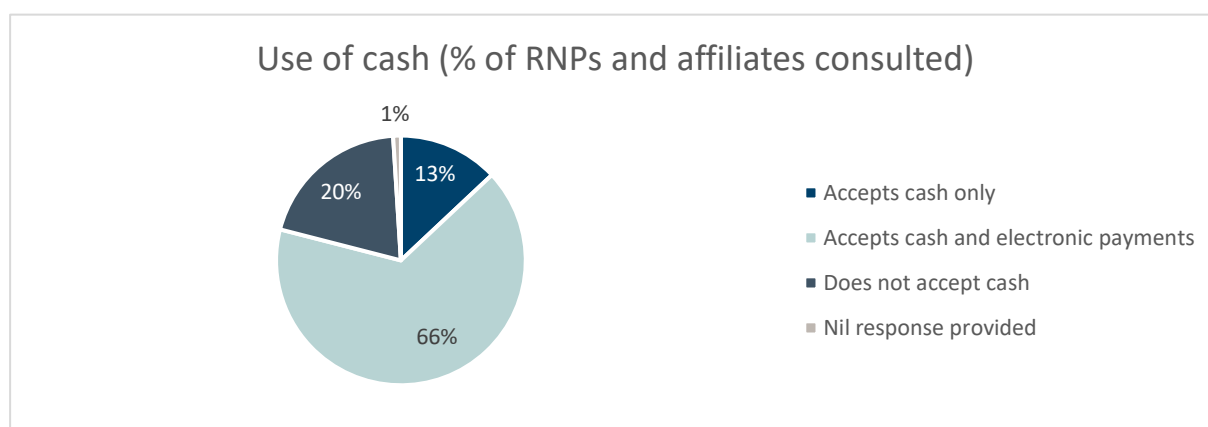


Figure 2: Most RNPs and affiliates consulted for this assessment accept cash to fund remittances.

### Ability to store and move funds

By their nature, the subsector's products and services facilitate the rapid movement of funds. Such activity makes these 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. On the other hand, the subsector's products and services are not generally designed to store funds and customers are unlikely to use the subsector for this purpose.<sup>29</sup>

Inherent ML/TF vulnerability is primarily concentrated in remittance services, followed by foreign currency exchange. This is consistent with the how many entities subsector provide these services (see figure 3). A very small number of reporting entities offer other services that carry specific inherent ML/TF vulnerability, such as traveller's cheques, stored value cards and bullion services. These services are not discussed in detail in this report because their scale across the subsector is very limited. Reporting entities can refer to AUSTRAC's ML/TF risk assessments of [traveller's cheques](#) and [stored value cards](#) for information on ML/TF vulnerabilities associated with these services.

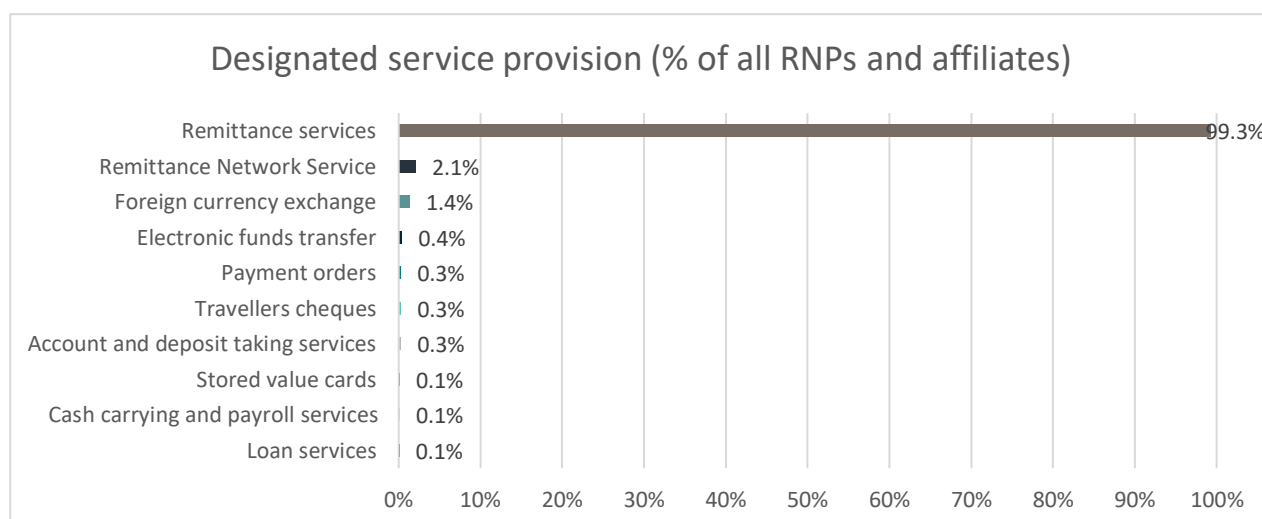


Figure 3: Proportion of the subsector that is registered with AUSTRAC to provide each designated service

<sup>29</sup> With respect to remittance accounts, transaction monitoring alerts may prompt compliance personnel to engage with a customer if funds are left in an account unused.

SMRs submitted by the subsector during the reporting period generally reflect the concentration of products and services offered. During the reporting period, 79 per cent of SMRs identified suspicious activity involving remittance services, while three per cent identified foreign currency exchange (see figure 4).

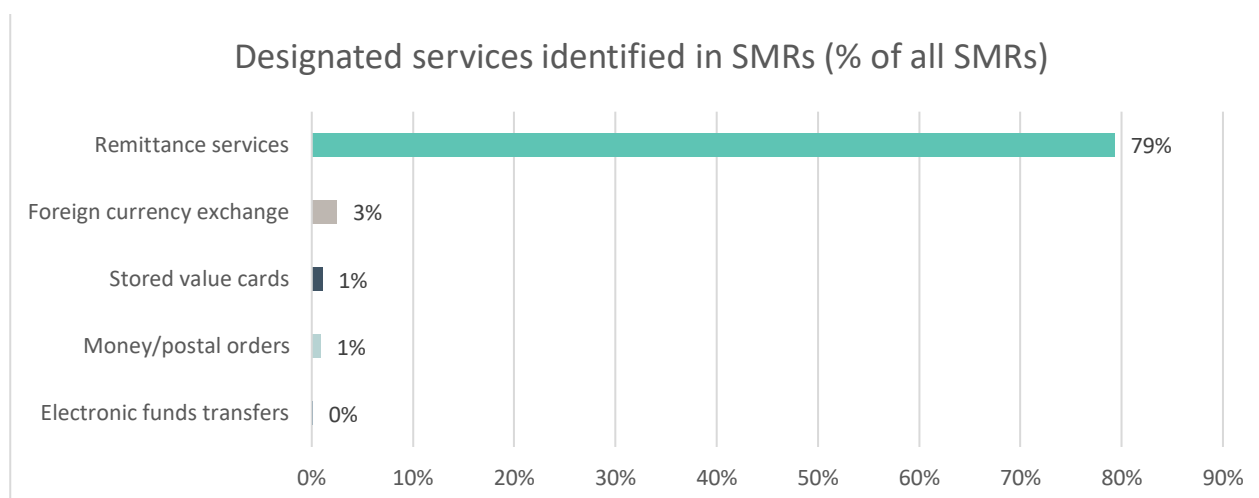


Figure 4: Remittance services dominate SMRs submitted by RNPs and affiliates during the reporting period

### Remittance services

Remittance services enable fast and effective movement of funds domestically and internationally. This exposes the subsector to a range of inherent ML/TF vulnerabilities including layering of criminal proceeds, financing or support of terrorist activity, and foreign jurisdiction risk (**Foreign jurisdiction risk** is discussed on page 44).

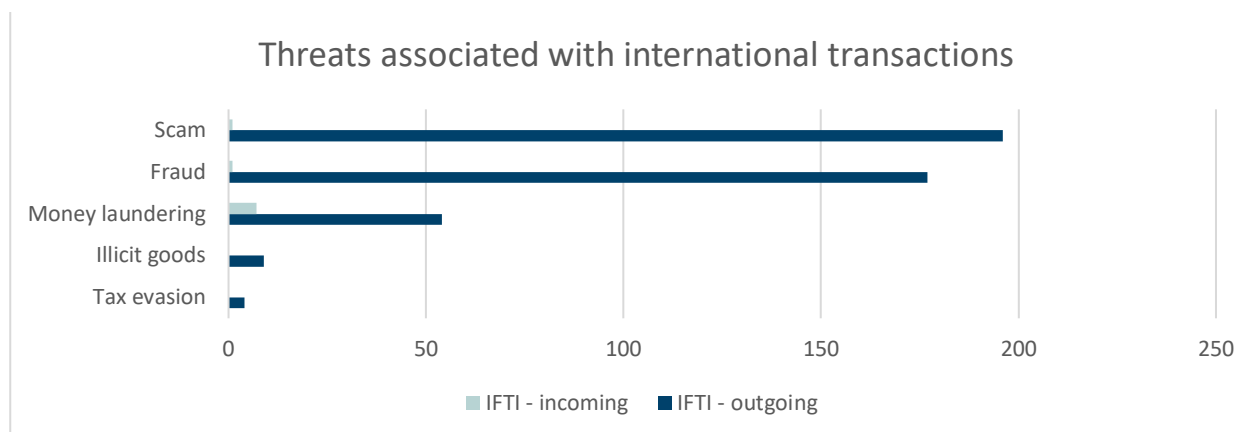
During the reporting period, the RNP subsector submitted over eight million IFTIs with a total value of \$19.5 billion. The total value associated with remittance services is likely to be higher because domestic remittances do not need to be reported to AUSTRAC. The vast volume and value of remittance transactions can help mask illegal funds movements and complicate detection of money laundering activity.

Criminals may seek to exploit specific perceived or actual vulnerabilities associated with remittance services including:

- the speed and global reach of remittances services
- a perception that remittance services may be less regulated compared to other financial sectors
- a perception that customers are more able to conceal their identity and the source of funds compared to other financial sectors.

Remittance services were identified in 88 per cent of the SMR sample, with outgoing remittances making up 97 per cent of remittance-related SMRs. The average value of outgoing remittance SMRs was moderate, at \$7,000. The most common threats associated with outgoing remittances related to suspected scams, frauds, and money laundering activity.





### **Foreign currency exchange**

Foreign currency exchange services are vulnerable to ML/TF because criminals can quickly exchange criminal proceeds into different currencies. Once exchanged, the original source of criminal proceeds can be difficult to trace. Reporting entities that provide foreign currency exchange may be exposed to both domestic and foreign criminal proceeds. Criminals can also use foreign currency exchange services to exchange smaller denominations into larger foreign currency denominations, making it easier to conceal or transport their funds.

Foreign currency exchange services were identified in five per cent of the SMR sample. Most reports related to suspected money laundering or fraud activity with a moderate-to high average value of \$21,000.

The number of foreign currency exchange transactions over \$10,000 declined by 89 per cent between 2019 and 2020, almost certainly as a result of COVID-19 restrictions.<sup>30</sup> This has reduced the subsector's exposure to ML/TF risk from foreign currency exchange services. It is likely that the number of transactions will increase when international visitors return to Australia in greater numbers.

<sup>30</sup> The number of TTRs submitted by the subsector where 'currency exchange services' was identified as the designated service fell by 89 per cent during the January and December 2020 period compared to the same time in 2019.

## DELIVERY CHANNELS

AUSTRAC assesses the delivery channels through which the RNP subsector offers its products and services present a **high** inherent ML/TF vulnerability.

While some remote product delivery arrangements exist in the subsector, such as automated kiosks, face-to-face interactions continue to be the primary means of customer contact.

The subsector is also exposed to ML/TF vulnerability related to outsourced product delivery arrangements, including super-agents, as well as the practice of offsetting.

### Level of customer contact

Reporting entities use a range of delivery channels to provide their products and services to customers. These include in-person, phone, online, and through third-party arrangements.

The RNP-affiliate business model means that the majority of reporting entities interact with customers face-to-face. Where a customer deals with an RNP directly online, this interaction is captured under that reporting entity's independent remittance dealer registration. Readers can refer to AUSTRAC's [ML/TF risk assessment of independent remittance dealers](#) for information about associated ML/TF vulnerabilities.

### IMPACT OF COVID-19 ON CUSTOMER CONTACT

The onset of COVID-19 and resulting government restrictions have impacted the subsector's interaction with customers, which has increasingly shifted to more remote delivery channels.

While some reporting entities were not able to open their physical shopfronts during lockdown restrictions, a number of affiliates were able to remain open because they also operated essential businesses, such as post offices, newsagents and pharmacies. Despite this, reporting entities and industry experts reported a drop in face-to-face customer interactions following the onset of the pandemic.

Over the medium-to-long-term it is likely these changes will accelerate the trend away from face-to-face product delivery and towards online channels.

### *Face-to-face transactions*

The majority of RNPs and affiliates continue to offer face-to-face transactions. 70 per cent of respondents to the compliance report said they offered in-person transactions in 2020, and 16 per cent indicated they only offered in-person transactions.

The level of face-to-face customer interaction varies among reporting entities. During consultations for this report, industry representatives stated in-person contact may occur for each transaction or at on-boarding only.<sup>31</sup>

Face-to-face transactions generally provide reporting entities with more opportunity to identify and respond to suspicious behaviour if necessary, including by:

- refusing to process a transaction
- advising a customer they may be a victim of fraud
- examining identification documents to ensure they are genuine, or have not been tampered with

<sup>31</sup> Refer to **Risk mitigation strategies** for an overview of CDD procedures applied at on-boarding across the subsector, and subsequent ML/TF vulnerabilities.

- enquiring about the purpose of a remittance and the customer's relationship with the beneficiary.

Face-to-face CDD checks or service delivery may also deter some criminals who prefer the perceived anonymity that online services offer.

### KIOSK USE AMONG RNPs

Some RNPs have expanded their network by placing automated kiosks in commercial premises, notably convenience stores and service stations. Kiosk systems are often implemented with the help of third party compliance technology providers.

Typically, an established customer will enter details of the remittance transaction through the kiosk interface, including the value, destination, and nature of the remittance. Once details are entered, a docket is generated which the customer presents to the retail staff, who are required to verify the customer's identification and details of the transfer prior to approving the transaction.

The kiosks are supported by face-to-face identity verification and automate elements of the remittance transaction process. The physical inspection of customer documents makes it easier to detect altered or mismatching forms of identification. However, industry experts consulted for this report said that staff responsible for identity verification sometimes lack training or are distracted by their sales clerk duties. Commercial third party verification services are often used to support identity verification.

### Complexity of product delivery arrangements

By design, the RNP-affiliate operational structure lengthens the supply chain and thus increases ML/TF vulnerability. In most instances, outgoing international transactions are sent from the customer to the affiliate and then to the RNP, before being sent offshore. Affiliates that exercise poor AML/CTF controls – particularly affiliates that are part of multiple RNP networks – pose a significant ML/TF risk to their RNP and the subsector as a whole.

The RNP subsector is also exposed to ML/TF vulnerability related to outsourced product delivery arrangements. This includes the use of correspondent institutions and third-party service providers to fulfil transactions in foreign jurisdictions.

In addition, some reporting entities use offsetting arrangements to effect remittance transactions. Offsetting can expose reporting entities to increased ML/TF risk, particularly if record-keeping is limited. Offsetting can also enable criminally complicit business to avoid reporting requirements and facilitate criminal activity.

#### **Outsourcing**

##### **Correspondent institutions and third party service providers**

Some RNPs rely on overseas correspondent institutions to fulfil transactions involving foreign jurisdictions without the need to operate in these jurisdictions. Reporting entities also often rely on other third-party service providers to provide additional services to customers, such as accepting card or online payments without having to establish their own merchant facility. Payment platforms are often integrated with the RNP's own website.

Outsourced product delivery arrangements can expose the subsector to increased inherent ML/TF vulnerability. This is because outsourcing lengthens and complicates the product delivery chain, making it harder for RNPs and affiliates to detect and act on suspicious activity. Poor governance arrangements can further exacerbate these vulnerabilities.



RNPs must conduct a thorough risk assessment before starting a business relationship with any third-party service providers they are using to facilitate remittance services. Initial assessments concerning the suitability of a commercial institution should reflect the RNP's transaction volumes, operating jurisdictions and existing risk mitigation strategies.

### Super-agents

A super-agent is any intermediary which provides a range of administrative and support services to a group of affiliates. This can include compliance training, affiliate on-boarding, managing contractual arrangements, optimising the use of an RNP's proprietary remittance platform, and ensuring affiliates are implementing the RNP's AML/CTF program effectively. Some super-agents also provide cash collection and deposit services, as well as remittance services, for affiliate customers.<sup>32</sup>



Super-agents offering purely administrative services are not subject to the AML/CTF Act and are not required to register with AUSTRAC. The private commercial arrangement with the RNP or affiliate defines their mandate and responsibilities.

A super-agent providing remittance services directly to customers must register with AUSTRAC.

A super-agent providing cash collection and deposit services for affiliates must register with AUSTRAC if the services are considered to be a remittance service.

For more information please refer to [Guidance note 12/03](#).

It is difficult to determine the true number of super-agents providing services in the RNP subsector. This is because:

- there is no central register of super-agents operating in Australia
- some super-agents are not required to register or enrol with AUSTRAC
- some super-agents deliberately avoid registration.

This lack of transparency poses an inherent ML/TF risk in itself. Super-agents can also increase inherent ML/TF risk exposure to the subsector by:

- providing poor affiliate AML/CTF training and program implementation, either wittingly or unwittingly
- pooling cash collections and deposits, which can obscure the actual value of funds received from an individual affiliate
- depositing pooled funds into their own personal bank account, then transferring funds to the RNP, thus adding an additional transactional layer and complicating detection of suspicious funds flows
- using cash deposit facilities that limit transaction oversight, such as ATMs or business express deposit boxes<sup>33</sup>
- failing to correctly register with or correctly report transactions to AUSTRAC.

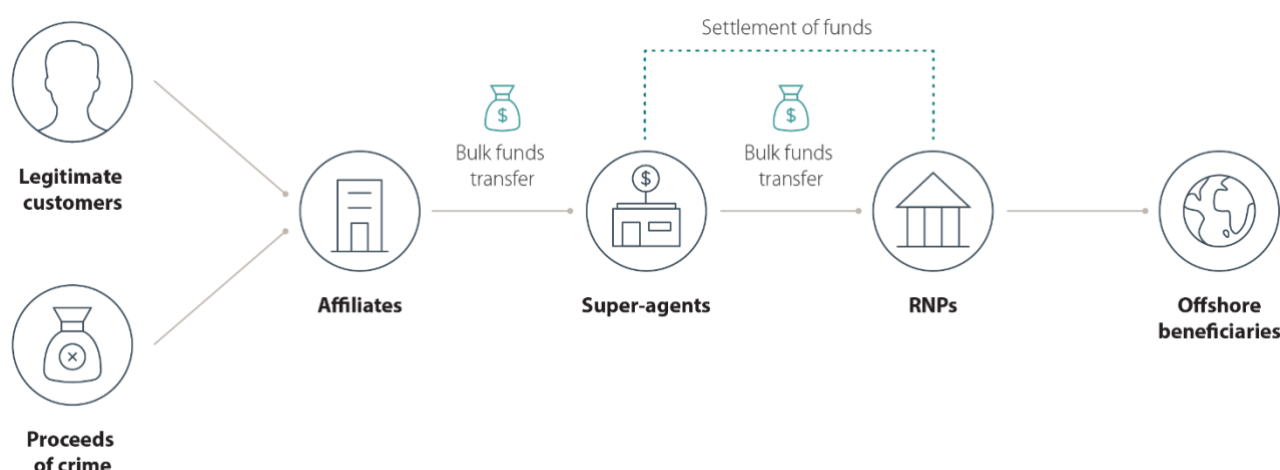
<sup>32</sup> De-banking has driven use of super-agents because they provide affiliates that do not hold a bank account with a method of transferring cash remittances to their RNP.

<sup>33</sup> Business express deposit facilities allow individuals to deposit large amounts of cash into a chute or other receptacle that is generally available 24/7. The individual making the deposit is exempt from providing identification under the AML/CTF Act.

## SUPER-AGENTS AND CASH REMITTANCES

Some affiliates will organise for a super-agents to collect bulk cash amounts to reconcile them with the RNP. After collection, the super-agent will either:

- deposit the cash into its own bank account and conduct an electronic funds transfer to the RNP account; or
- deposit the cash directly into the RNP account.



### Offsetting

Offsetting is a method of exchanging value internationally that relies on business-to-business relationships instead of established banking arrangements.<sup>34</sup> In its simplest form, a customer will ask an Australia-based reporting entity to send money to a jurisdiction where the reporting entity has a correspondent operator. The Australia-based reporting entity will then inform the overseas correspondent of the transaction, which will then release funds to the nominated beneficiary abroad. The Australia-based reporting entity and its overseas counterpart will settle their balance of payments at a later date.<sup>35</sup>

Offsetting can be a fast and effective method for transferring value overseas and is a legitimate business practice that many types of businesses use, such as commercial entities reconciling business accounts with overseas entities. For some reporting entities offsetting is a viable alternative to using formal banking channels. For example, when transferring value to jurisdictions that lack adequate banking infrastructure, or to avoid expensive foreign exchange fees charged by banks and therefore increase profit margins. In other situations, reporting entities may use offsetting if they have been de-banked. Large multinational reporting entities may also find offsetting arrangements more convenient for transferring value between their businesses.

While offsetting is often part of legitimate business practices, it is also highly attractive to criminals as a means of moving domestically-generated proceeds of crime offshore. Given the informal nature of many offsetting arrangements, customers can be afforded greater anonymity and transactions are often subject to less scrutiny, particularly if the reporting entity has poor or limited record-keeping practices.

<sup>34</sup> Other common names for offsetting include hawala, hundi, chit and fei chi'en.

<sup>35</sup> Common methods of settlement include periodic cross-border movement of cash, under/over-invoicing goods, and later-date wire transfers between stakeholders removed from the original customer's transaction.

Offsetting also increases the ability of a criminally complicit business to avoid reporting requirements and facilitate criminal activity. For example, when a reporting entity facilitates a remittance transaction using a bank, AUSTRAC receives an IFTI from both the reporting entity and the bank. However, in an offset transaction AUSTRAC only receives the reporting entity's IFTI. If this is not submitted, AUSTRAC has no record of the transaction taking place.



Reporting entities must still submit relevant reports to AUSTRAC when using offsetting arrangements. AUSTRAC expects the RNP subsector to know and understand their AML/CTF reporting obligations when using offsetting arrangements.

## DE-BANKING AND THE REMITTANCE SECTOR

Many reporting entities consulted for this report highlight de-banking as a significant and ongoing concern for the subsector. De-banking occurs when a financial institution closes a customer's account, usually because of perceived or actual ML/TF risk posed by the customer AUSTRAC published a [statement on de-banking](#) in October 2021.

De-banking is likely to increase the subsector's reliance on third-party service providers to process payments, which allows reporting entities to bypass the need to acquire merchant facilities from a bank. Therefore, de-banking may indirectly increase ML/TF vulnerabilities associated with outsourcing.

De-banking of RNPs and affiliates is also likely to increase the use of offsetting arrangements. This is because offsetting can bypass an entity's reliance on bank transactions to effect remittance transactions, therefore enabling reporting entities to continue operating when they have been de-banked. As discussed below, offsetting exposes the subsector to ML/TF vulnerabilities.

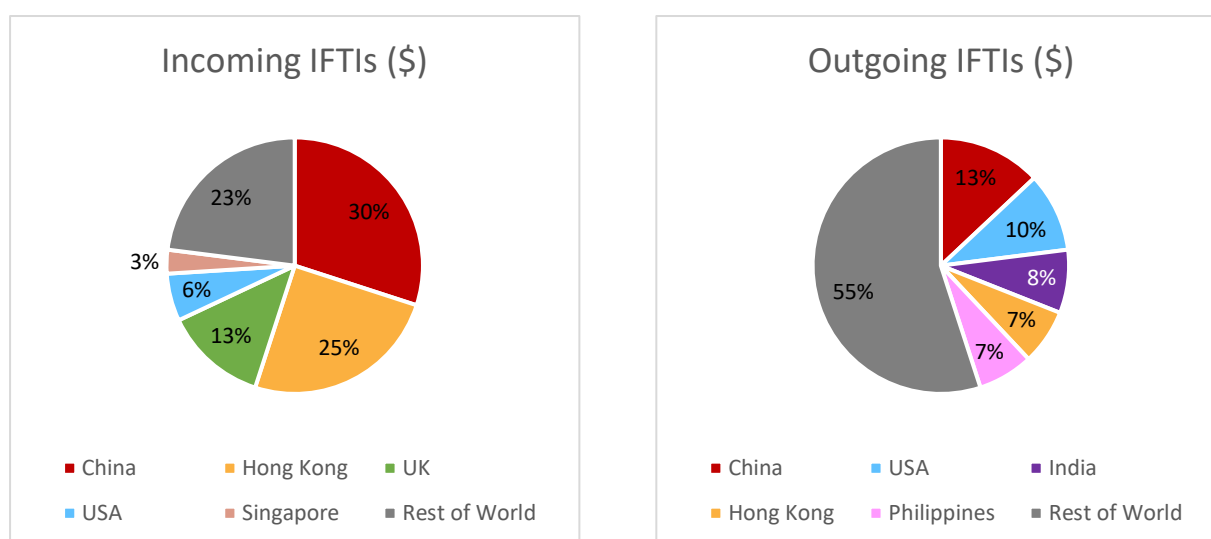
## FOREIGN JURISDICTIONS

AUSTRAC assesses the RNP subsector has a **high** inherent ML/TF vulnerability to foreign jurisdictions.

The RNP subsector has substantial and ongoing exposure to foreign jurisdictions, including higher-risk jurisdictions, because of the nature of their business operations.

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

### Movement of funds or value internationally<sup>36</sup>



In the reporting period, the subsector submitted approximately 8.3 million IFTIs with a total value of \$19.5 billion. Almost three quarters of the value of IFTIs were outgoing transactions (74 per cent).<sup>37</sup> The average value of incoming IFTIs was almost three times greater than outgoing. This is likely a reflection of the purpose of these transfers. Funds remitted offshore often comprise a portion of the customer's income to support family overseas. Incoming transfers are often payment for investments or financial support for international students, which are generally higher value transactions.

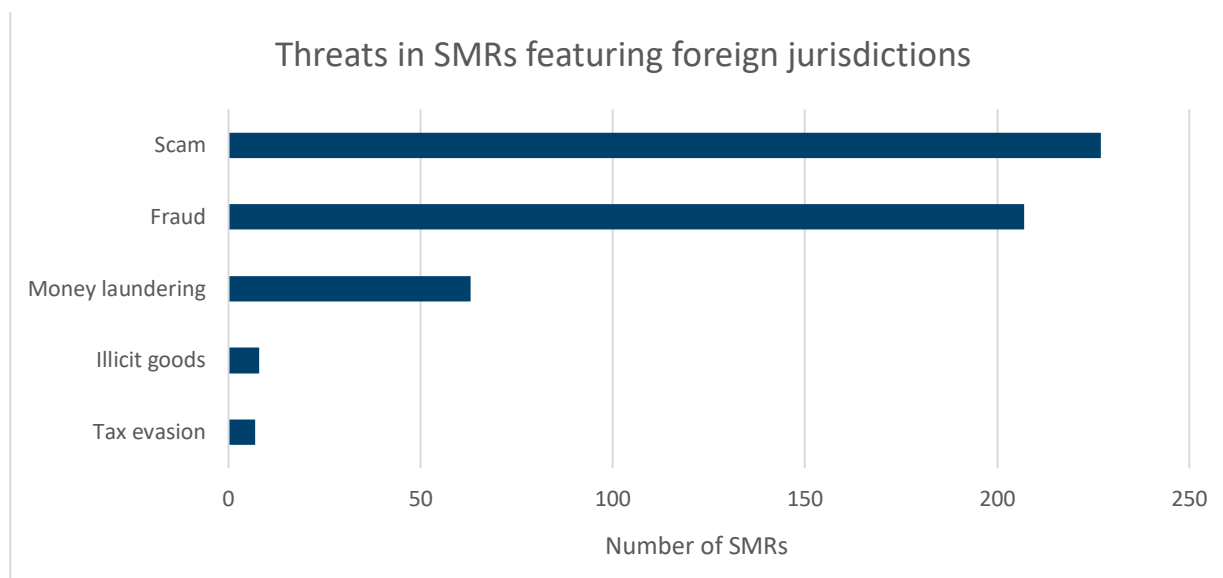
International transactions were identified in 89 per cent of the SMR sample. The top five jurisdictions identified in the SMR sample were the Philippines, Nigeria, Vietnam, USA and India. Three of these jurisdictions (Philippines, USA, and India) rank in the top five source or destination jurisdictions for IFTIs the subsector submitted. This suggests suspicious activity from the Philippines, Nigeria and Vietnam is over-represented relative to the value of transactions with these jurisdictions.

Scams, frauds and money laundering were the primary threats in SMRs where a foreign jurisdiction was present.

<sup>36</sup> Statistics related to IFTI value are estimated accounting for errors in the reported source and destination jurisdictions. The uncertainty in estimated proportions is typically in the range 0.5 to 1 percentage points but can be as large as 5.

<sup>37</sup> Industry IFTI submissions include data quality issues surrounding incomplete or inaccurate inputs. Caution should be applied when interpreting IFTI source and destination countries.





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.

### Transactions with higher-risk jurisdictions

The RNP subsector frequently transacts with higher-risk jurisdictions. 64 per cent of all IFTIs by value involved transactions with higher-risk jurisdictions.<sup>38</sup> This includes a moderate value of funds flowing to or from global financial centres.<sup>39</sup> More than three-quarters of transactions with higher-risk jurisdictions were outgoing (83 per cent).<sup>40</sup>



AUSTRAC recognises that the majority of funds flows with higher-risk jurisdictions are for legitimate reasons, particularly in the context of financial inclusion. Some higher-risk countries have limited or no banking infrastructure, and funds remitted from abroad can be a vital means of support for those facing socio-economic hardship. It is critical reporting entities understand the purpose of their customers' transactions with higher-risk countries to assess their risk exposure and detect criminal behaviour.

<sup>38</sup> This finding was made by data matching the source or destination of IFTIs with a list of foreign jurisdictions considered higher risk for money laundering, terrorism financing, tax evasion and child exploitation. These higher-risk jurisdiction lists were compiled with the assistance of expert advice from international institutions, non-profit organisations and partner agencies.

<sup>39</sup> Global financial centres are hubs of financial trade and house the headquarters of many large corporations. This report considers the following countries as global financial centres: Hong Kong SAR, Singapore, UK and USA in line with the Global Financial Centres Index [https://www.longfinance.net/media/documents/GFCI\\_26\\_Report\\_2019.09.19\\_v1.4.pdf](https://www.longfinance.net/media/documents/GFCI_26_Report_2019.09.19_v1.4.pdf)

<sup>40</sup> Statistics related to IFTI value are estimated accounting for errors in the reported source and destination jurisdictions. The uncertainty in estimated proportions is typically in the range 0.5 to 1 percentage points but can be as large as 5.

## 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.

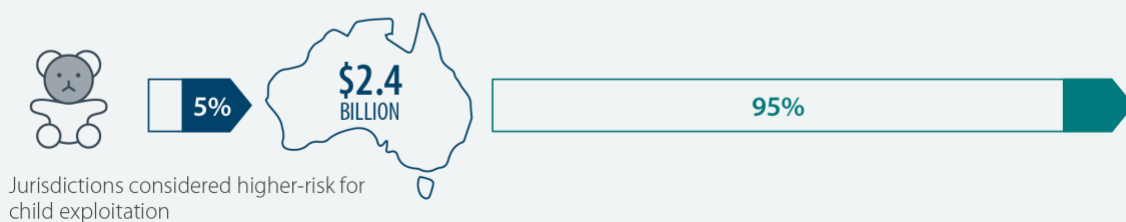
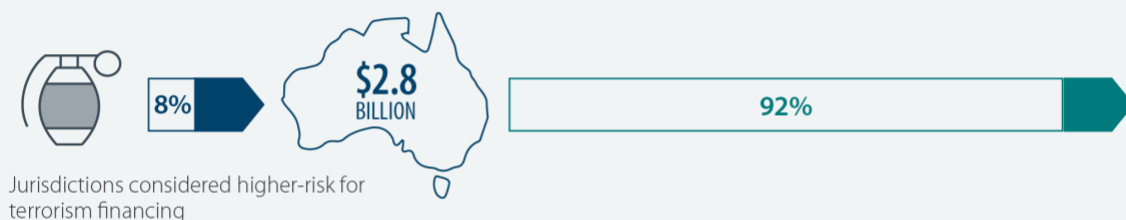
AUSTRAC has made its own determination about which jurisdictions are considered higher-risk for this report. This takes into account Australia-specific factors, such as top source or destination jurisdictions for higher-risk financial flows, as well as global factors, such as the strength or weakness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

- the European Union list of non-cooperative jurisdiction in taxation matters
- the European Union's high-risk third countries with strategic deficiencies in their AML/CFT regimes
- 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 WITH HIGHER-RISK JURISDICTIONS<sup>41</sup>

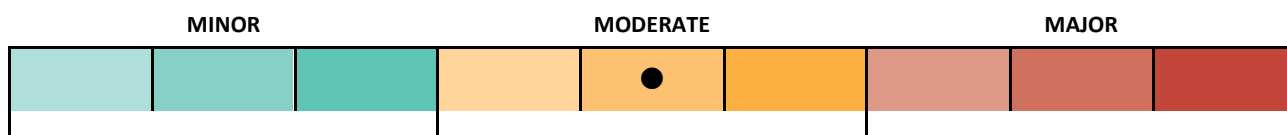
## Incoming value

## Outgoing value



<sup>41</sup> Statistics related to IFTI value are estimated accounting for errors in the reported source and destination jurisdictions. The uncertainty in estimated proportions is typically in the range 0.5 to 1 percentage points but can be as large as 4.

# CONSEQUENCES



CONSEQUENCES FACTOR	RATING
CUSTOMERS	●
INDIVIDUAL BUSINESSES AND THE SUBSECTOR	●
THE AUSTRALIAN FINANCIAL SYSTEM AND COMMUNITY	●
NATIONAL AND INTERNATIONAL SECURITY	●

AUSTRAC assesses that the consequences of criminal activity in the RNP subsector are **moderate**. Consequences include the potential impact or harm that ML/TF and other financial crimes may cause. Financial crime that impacts the RNP subsector has consequences for customers, individual reporting entities, the subsector as a whole, and the broader Australian and international community. Where the subsector is used to finance terrorism or serious transnational crime, exploitation can have significant consequences for national and international security.

## CUSTOMERS

AUSTRAC assesses that ML/TF and predicate offences involving the RNP subsector have **moderate** consequences for customers of the subsector.

The subsector reports impacts that criminal activity can have on their customers. Frauds and scams may have a higher financial and emotional impact on individual customers as opposed to corporate entities, which may be able to absorb the financial impact more readily. Victims are often reluctant to admit a scammer has deceived them, and will insist on continuing a transaction against advice provided by a reporting entity. This can prolong the duration and harm of scams.

The impact of criminal activity on customers can include:

- financial loss and emotional distress from fraud and identity theft
- distress and potential legal repercussions for customers targeted by fraudsters and scammers (e.g. those used as money mules)
- increased compliance costs for reporting entities driving increased costs for customers using remittance services
- where a reporting entity is de-banked, subsequent money transfer options could cause hardship for communities overseas that are supported through remittances
- market competition may be reduced where de-banked remitters are forced out of business. This may drive up prices for remittance services.

## INDIVIDUAL REPORTING ENTITIES AND THE SUBSECTOR

AUSTRAC assesses that ML/TF and predicate offences involving the RNP subsector have **moderate** consequences for individual reporting entities and the subsector as a whole.

The perceived or actual threat of criminal activity in the remittance sector poses reputational risks to RNPs and affiliates. In some instances this can lead to de-banking, particularly of smaller RNPs which may be perceived as having less sophisticated risk mitigation strategies. De-banking constrains the operations of reporting entities and may force some out of business.

The subsector may also be increasingly targeted by criminals if they identify certain RNPs or affiliates with poor AML/CTF controls.

The impact of criminal activity on individual reporting entities and the RNP subsector as a whole can include:

- loss of revenue and increased insurance premiums
- more stringent regulatory oversight, creating additional costs for businesses
- difficulty continuing or establishing relationships with domestic and overseas financial institutions
- enforcement or legal action and associated civil or criminal penalties in the event of serious non-compliance
- loss of earnings as a result of criminal exploitation (e.g. customers taking business elsewhere due to negative experience)
- reputational damage to individual business, the subsector and the remittance sector more broadly, leading to loss of customers, de-banking and possible business closures.

## AUSTRALIAN FINANCIAL SYSTEM AND COMMUNITY

AUSTRAC assesses that ML/TF and predicate offences involving the RNP subsector have **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 as having a stable and secure financial sector. This harm is moderated by the relatively modest financial footprint of the RNP subsector, as well as the concentration of activity in a small number of products and services.

The speed and capacity the subsector possess to move funds internationally may attract criminals seeking to launder the proceeds of crime or finance new crimes. This poses harms to the Australian community, including societal harms associated with predicate offences such as child exploitation and drug trafficking

The impact of criminal activity on the Australian financial system and the community can include:

- increased difficulty combatting crime if crucial financial intelligence is not reported to law enforcement
- reduced government revenue due to tax evasion, impacting on the delivery of critical government services.
- physical and psychological injury inflicted upon non-customers through offences such as child exploitation and drug trafficking
- money laundering resulting in the preservation of illicit assets, the financing of new crimes and the corruption of public officials and private enterprise<sup>42</sup>
- a loss of confidence in the RNP subsector as a legitimate method of sending funds internationally. This could reduce competition in the remittance sector and result in more expensive international funds movements

## NATIONAL AND INTERNATIONAL SECURITY

AUSTRAC assesses that ML/TF and predicate offences involving the RNP subsector have **moderate** consequences for national and international security.

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

- gang-related violence can threaten domestic security (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 violence).

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

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

<sup>42</sup> D Chaikin, *Effectiveness of anti-money laundering obligations in combating organised crime with particular reference to the professions*, Australian Institute of Criminology, Australian Government, 2018.



# RISK MITIGATION STRATEGIES

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

The level of sophistication and implementation of risk mitigation strategies varies significantly across the subsector. Some reporting entities have substantial data and technological capabilities and human resources to apply risk mitigation strategies consistently and robustly. In these instances, risk mitigation strategies generally include CDD and ECDD procedures, transaction monitoring, AML/CTF experts conducting annual audits, introductory and ongoing training for staff and affiliates, risk rating processes for customers and foreign jurisdictions, and sanction and PEP screening.

However, some reporting entities do not adequately resource or employ a strong AML/CTF program, or have a very limited understanding of their AML/CTF obligations. Some reporting entities consider the cost of implementing a robust AML/CTF program as prohibitive. These entities often use low-cost 'off the shelf' programs that are not tailored to their business requirements, which can expose them to ML/TF risk. Criminals are known to target reporting entities who they suspect employ weak CDD procedures.

Across the subsector, improvements could be made to ensure:

- CDD processes are optimised to meet compliance requirements for corporate customers, not just individual customers
- proof of customer source of funds is sought for all unusual and suspicious remittance requests, not just high-value transactions
- RNPs provide their affiliates with a robust and tailored AML/CTF program and the capacity to understand and effectively implement it



- all reportable transactions are submitted to AUSTRAC in a timely manner and to a high standard.

Improvements to the quality and quantity of SMR submissions can also be made across the subsector (see page 56).



## GUIDANCE RESOURCES FOR RNPs AND AFFILIATES

IRDs are encouraged to access guidance and other materials developed specifically for remittance service providers that are available on the [AUSTRAC website](#). These include:

- [Guide to developing an AML/CTF program](#)
- [Risk management methodology fact sheet](#)
- [Identifying individual customers fact sheet](#)

This information is [available in other languages](#) including Arabic, Chinese, Dari, Farsi, Swahili, Urdu, and Vietnamese.

Reporting entities can also access [general guidance on how to comply with their obligations and report to AUSTRAC](#).

## CUSTOMER DUE DILIGENCE

All reporting entities consulted for this assessment stated they apply CDD measures as part of their customer on-boarding procedures. These processes varied from very simple – for example, where a customer provides only their name, address and occupation – to the use of comprehensive customer questionnaires.

### Corporate customers

Reporting entities who primarily service corporate customers acknowledge the risks associated with complex corporate structures and the challenges in identifying beneficial ownership. Generally, only a few RNPs have the capacity, risk appetite or resources to adequately service both individual and corporate customers. A number of reporting entities consulted for this assessment highlight their systems and procedures are better optimised for individual customers, and indicate they would need a significant uplift to be able to serve corporate customers.



Reporting entities must identify beneficial owners of corporate customers and assess the ML/TF risks those customers pose to their business. [Further information about beneficial owner obligations](#) is available on AUSTRAC's website.

## PEP and sanctions screening

Reporting entities describe using a mix of automated and manual screening via commercial third-party databases, official watch lists, media scanning and other open source searches.

Some reporting entities are better resourced to implement thorough and tailored PEP and sanctions screening. Reporting entities who use a single source to detect PEPs or sanctioned entities need to be aware of the shortcomings of this approach. Some databases rely on methodologies to determine PEP status that differ from the AML/CTF Act definition. In addition, spelling and translation errors can compromise name matching and, in some cases, certain PEP categories are not included for screening.



Reporting entities should adopt comprehensive screening practices and ensure all customers are subject to PEP and sanctions screening. AUSTRAC's website contains further guidance about [identifying and assessing the ML/TF risk of PEPs](#).

The Department of Foreign Affairs and Trade (DFAT) is the primary department responsible for sanctions. Further information about Australian sanctions can also be found on the [Department of Foreign Affairs and Trade website](#).

## Source of funds/source of wealth

AUSTRAC considers the ability and willingness of some reporting entities to confirm customers' source of funds or source of wealth as limited. Although RNPs frequently require customers to specify and provide proof of their occupation during customer on-boarding, a number of reporting entities do not normally seek source of funds documentation for smaller remittance transactions (usually those under \$1,000). RNPs normally create customer profiles based on the usual value, frequency and destination of transfers, and will generally attempt to verify source of funds or wealth only when the customer departs from these patterns or requests a larger than usual remittance transaction. Documents accepted as source of funds or wealth verification include pay slips, bank statements and, where appropriate, proof of asset sales (e.g. property deeds).

Verifying funding sources for corporate customers presents further challenges owing to the variety and complexity of business structures and a range of purported commercial explanations for funds used in transactions. The inability of some reporting entities to implement adequate CDD policies for corporate customers compounds these challenges.



Reporting entities are strongly encouraged to review and be familiar with [source of funds and source of wealth considerations](#), available on the AUSTRAC website.

## Affiliate due diligence: initial and ongoing

RNPs must conduct due diligence when on-boarding an affiliate, and ongoing due diligence to identify any material changes in compliance with the AML/CTF Act. RNPs must also develop and deliver training for affiliates on compliance procedures and reporting obligations. RNPs should regularly monitor their affiliate network to ensure compliance obligations are being met.

Consultations with industry experts and reporting entities for this assessment identified some gaps in the RNP-affiliate relationship regarding communication, AML/CTF compliance and systems training, and guidance when errors occur. These gaps can expose businesses to criminal misuse stemming from a breakdown in communication, an understanding of risk appetites, or AML/CTF reporting responsibilities and procedures.

## Correspondent institutions and third-party service providers

RNPs must conduct a thorough risk assessment before starting a business relationship with any commercial institution they are using to facilitate remittance services. Initial assessments concerning the suitability of a commercial institution should match the profile of the RNP business, transaction volumes, jurisdiction, and other risk mitigation strategies.

Considerations for initial assessments can include:

- Assessing the bank or third party service provider's products and customer base.
- Assessing the existence and quality of any AML/CTF regulation in the entity's domicile country.

- Assessing the existence and adequacy of the correspondent institution's AML/CTF controls and internal compliance practices.
- Assessing the ownership, control and management structures of the correspondent institution and any parent company.
- Ensuring key personnel in management and ownership structure are checked against reputable and updated sanctions and PEP watch lists.
- Where changes occur to the ownership structure, operations or the correspondent's key principals, further due diligence should be initiated.

## TRANSACTION MONITORING

Transaction monitoring is the capacity to analyse transactions in order to detect suspicious activity, including investigating high risk cases flagged by transaction monitoring software. Effective transaction monitoring requires up-to-date threat typologies that define indicators of criminal activity, which are used to create software rules that identify and trigger automated alerts. Threat typologies can be based on a range of internal and external sources, including law enforcement information.

Reporting entities consulted for this report described transaction monitoring capabilities that varied in sophistication. The largest RNPs generally have the most sophisticated transaction monitoring capabilities, as their operations mean they have both the need and resources to develop and maintain the required systems and procedures. These RNPs and their affiliates process a very high number of transactions, sometimes as many as 30 per second. The sheer volume of transactions means they cannot rely solely on frontline CDD procedures to prevent criminal misuse of their system or exploitation of their customers.

Some RNPs also maintain in-house financial intelligence units responsible for developing threat typologies. RNPs that process fewer transactions have traditionally relied more upon front line CDD procedures to detect criminal misuse. However, an AML/CTF expert has estimated that roughly 80 per cent of their RNP clients now perform some form of post-transaction analysis, due to the growing availability of suitable software.

Industry feedback revealed RNPs and affiliates use several methods to escalate suspicious matters internally. These included verbal reporting to the RNP, alongside email, online and paper methods. Less than one per cent stated they still rely upon hard copy forms, which may impair their ability to submit SMRs within the necessary timeframes.

## TRANSACTION LIMITS

Imposing limitations on the value and frequency of transactions, and limiting the number of jurisdictions serviced is a relatively common risk mitigation strategy that RNPs and affiliates use.

Many reporting entities consulted by AUSTRAC indicated they impose limits on the total value and/or number of remittance transactions per customer in a given time period. Limits varied depending on the risk associated with the jurisdiction involved. These limits enable businesses to manage their ML/TF exposure in relation to high-value or high-volume remittance transactions which are inconsistent with a customer's profile or their usual remittance activity.



Strategies that reduce the rapid or complex movements of funds offshore can help minimise the subsector's exposure to ML/TF risks. AUSTRAC encourages RNPs and affiliates to consider how transaction limits may reduce their business's ML/TF exposure and review existing limits on a regular basis.

## RISK ASSESSMENTS

RNPs are required to assess the ML/TF risks associated with their businesses across the four key elements of customers, products, delivery channels and foreign jurisdictions. RNPs consulted outlined various risk assessment processes across these elements which vary in their sophistication. In the past, AUSTRAC has identified some shortcomings in the risk assessment processes of some RNPs.



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 RNPs and their business operations.

In addition to being business-specific, risk assessments need to be regularly updated to ensure changes in risk profiles and systems, as well as products or delivery channels, are addressed in a timely and effective way.

## INDEPENDENT REVIEWS

RNPs and their affiliates are required to have their risk management frameworks independently reviewed on a regular basis. Reviews should be scheduled periodically, and should also take place in response to events that may impact the risks a reporting entity faces. These reviews must be conducted by operationally independent, appropriately trained and competent persons. AML/CTF policies and programs dealing with material risks are also expected to be included in the independent reviews. This provides an objective mechanism to assess whether AML/CTF programs are appropriate and effective in detecting criminal misuse.

## EMPLOYEE DUE DILIGENCE AND TRAINING

While criminal misuse of the subsector is generally considered an external threat, staff actions may also inadvertently increase ML/TF risks. Some reporting entities conduct regular scheduled or new-starter training programs, as well as initial and ongoing staff due diligence such as police and reference checks, PEP and sanctions screening, and open source or social media searches. However, some reporting entities have limited time or resources to undertake these checks.

Partner agency reporting indicates some reporting entities employ non-resident foreign nationals in violation of their visa conditions. This offence may make the businesses in question susceptible to criminal coercion through blackmail. Unintentional employment of non-residents without work rights would indicate serious shortcomings in employee screening.

## TRUSTED INSIDERS – ENABLERS OF CRIME IN AUSTRALIA’S FINANCIAL SYSTEM

The trusted insider is an individual with legitimate or indirect access to a business’s privileged information, techniques, technology, assets or premises, and whose access can facilitate harm.

Serious and organised crime groups will continually seek opportunities to exploit trusted insiders across Australia’s financial sectors. Criminals may specifically target RNPs and affiliates to facilitate money laundering and the movement of funds internationally.



Appropriate initial and ongoing employee training is critical for all businesses regulated under the AML/CTF Act. Regular refresher training is essential to ensure experienced staff do not become complacent or unaware of emerging ML/TF methodologies, threats and trends.

Ensuring employee probity and integrity – both before they commence processing remittance transactions and throughout their tenure – is an important ML/TF risk mitigation strategy.

AUSTRAC expects RNPs and affiliates to report any suspicions of professional facilitators or enabling parties to illicit activity, and encourages mature risk mitigation strategies for limiting insider threats.

## SUSPICIOUS MATTER REPORTING TO AUSTRAC

A significant proportion of RNPs submit limited or no SMRs to AUSTRAC. This may be because an RNP is inactive or has no affiliates. Low or no reporting may also be attributable to differences between reporting entities' scale of operations, their customer base, or remittance transactions with lower-risk foreign jurisdictions. However, low SMR reporting often reflects varied levels of:

- understanding of reporting obligations
- effectiveness of CDD, ECDD and transaction monitoring processes
- understanding of ML/TF risks, including a lack of appropriate staff training.

AUSTRAC also considers the content of SMR submissions could be improved. For example:

- **Including a more detailed grounds for suspicion.** This information-rich section provides valuable intelligence for AUSTRAC and its partner agencies. Reporting entities are encouraged to explain what aspects of the transaction(s) or customer behaviour was suspicious and include all information from ECDD activities and financial investigations in the grounds for suspicion.
- **Avoiding trigger-based reporting.** Trigger-based reporting is a practice in which a reporting entity submits a SMR solely on the basis of a trigger generated by their transaction monitoring system without conducting further investigation to form suspicion on reasonable grounds. Similarly, template reporting where there is little unique detail in the grounds for suspicion. Such reports provide little intelligence value.
- **Summarising suspicions** by including a short summary at the top of the grounds for suspicion section of the SMR. This would help expedite review and assessment of reports by AUSTRAC and partner agencies.
- **Including documents that provide additional context.** If relevant, include identity verification documents or any other materials which may be available to provide AUSTRAC analysts with a more detailed and complete picture of suspicious transactions.

RNPs should have policies and procedures to assist staff identify and report suspicious matters.



## FURTHER RESOURCES ON SUSPICIOUS MATTER REPORTING

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

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

## APPENDIX A: GLOSSARY

<b>Affiliate</b>	Members of a remittance network provider's (RNP) network that use that network's brand, products, platforms or systems to provide the remittance service, and are required to comply with the AML/CTF program of the RNP.
<b>AML/CTF</b>	Anti-money laundering and counter-terrorism financing.
<b>AML/CTF program</b>	A document that sets out how a reporting entity meets its AML/CTF compliance obligations.
<b>Beneficial owner</b>	An individual who owns 25 per cent or more of, or otherwise controls the business of an entity.
<b>Customer due diligence (CDD)</b>	Customer due diligence (CDD) is the process where pertinent information of a customer's profile is collected and evaluated for potential ML/TF risks.
<b>Designated business group</b>	A designated business group (DBG) is a group of two or more reporting entities who join together to share the administration of some or all of their anti-money laundering and counter-terrorism financing obligations.
<b>Designated non-financial businesses and professions (DNFBP)</b>	The Financial Action Task Force (FATF) Recommendations defines Designated Non-Financial Businesses and Professions (DNFBPs) as casinos, real estate agents, precious metal/precious stone dealers, lawyers, notaries, other independent professionals, accountants, as well as trust and company service providers.
<b>Enhanced customer due diligence (ECDD)</b>	Enhanced customer due diligence (ECDD) is the process of undertaking additional customer identification and verification measures in certain circumstances deemed to be high risk.
<b>Financial Action Task Force (FATF)</b>	The Financial Action Task Force is an inter-governmental body focused on fighting money laundering, terrorism financing and other related threats to the integrity of the international financial system, by ensuring the effective implementation of legal, regulatory and operational measures.
<b>Global financial centres</b>	For the purposes of this report, global financial centres refer to the jurisdictions that are home to the top four cities in the Global Financial Centres Index 26
<b>Independent remittance dealer (IRD)</b>	A remittance service provider that uses its own products, platforms or systems to provide remittance services to customers. An independent remittance dealer may own or control a number of branches.
<b>Inherent risk</b>	Inherent risk represents the amount of risk that exists in the absence of the reporting entity implementing AML/CTF controls.
<b>Integration</b>	The final stage of the money laundering cycle, in which illicit funds or assets are invested in further criminal activity, 'legitimate' business or used to purchase assets or goods. At this stage, the funds are in the mainstream financial system and appear to be legitimate.
<b>International financial transaction instruction – designated remittance agreement (IFTI-DRA)</b>	<p>A money service business instruction to transfer funds or property to or from another country where either:</p> <ul style="list-style-type: none"> <li>the entity accepting the instruction from the customer or</li> <li>the entity making the money or property available</li> </ul> <p>is not a financial institution.</p>
<b>Know your customer (KYC)</b>	'Know Your Customer': an initial and ongoing process whereby a business determines and verifies the real identity of a customer and their transaction activities. Confirming

	this information allows businesses to identify aberrations to a customer's normal behaviour which may form a suspicion for criminal activity.
<b>Layering</b>	The second stage of the money laundering cycle, which involves moving, dispersing or disguising illegal funds or assets to conceal their true origin.
<b>ML/TF</b>	Money laundering and terrorism financing.
<b>Mules</b>	Third parties used to transfer illicit funds between locations or accounts.
<b>Permanent establishment</b>	<p>The place where an entity carries on any activity or business in Australia or another country. You operate at or through a permanent establishment in a country if you or your agent:</p> <ul style="list-style-type: none"> <li>• have physical offices or business premises in that country</li> <li>• carry on your business in that country (even without a physical office).</li> </ul>
<b>Placement</b>	The first stage of the money laundering cycle, in which illicit funds first enter the formal financial system.
<b>Politically exposed person (PEP)</b>	<p>A politically exposed person (PEP) is an individual who holds a prominent public position or role in a government body or international organisation, either in Australia or overseas. Immediate family members and/or close associates of these individuals are also considered PEPs. PEPs often have power over government spending and budgets, procurement processes, development approvals and grants.</p> <p>The AML/CTF Act identifies three types of PEPs.</p> <ul style="list-style-type: none"> <li>• Domestic PEP – someone who holds a prominent public position or role in an Australian government body.</li> <li>• Foreign PEP – someone who holds a prominent public position or role with a government body in a country other than Australia.</li> <li>• International organisation PEP – someone who holds a prominent public position or role in an international organisation, such as the United Nations (UN), the World Trade Organisation (WTO) or the North Atlantic Treaty Organisation (NATO).</li> </ul>
<b>Predicate offence</b>	For the purpose of this risk assessment, a predicate offence is any offence which generates proceeds of crime.
<b>Refining</b>	The process of exchanging lower denomination bills into higher denominations. Can occur using foreign exchange which provides further distance from funds' origin.
<b>Remittance network provider (RNP)</b>	A remittance business structure that allows a network of affiliates to use its brand, products, platforms or systems to provide remittance services to customers.
<b>Remittance service</b>	A service for transferring money or property offered by a remittance service provider. The remittance service must involve either accepting an instruction for the transfer of money or property, or making money or property available to the intended payee, or both. In addition, the remittance service must be provided at or through a permanent establishment of the remittance service provider in Australia.
<b>Remittance service provider (RSP)</b>	An individual, business or organisation that accepts instructions from customers to transfer money or property to a recipient. Remittance service providers are also known as money transfer businesses.
<b>Residual risk</b>	Residual risk is the amount of risk that remains after a reporting entity's AML/CTF controls are accounted for.
<b>Source of funds</b>	A customer's source of funds refers to the origin of the particular funds or other assets involved in one or more transactions between you and the customer.



<b>Source of wealth</b>	A customer's source of wealth refers to the origin of their entire wealth including the volume of wealth the customer would be expected to have accumulated and how the customer acquired that wealth.
<b>Structuring</b>	Where a person deliberately: <ul style="list-style-type: none"> <li>• splits cash transactions to avoid a single large transaction being reported in threshold transaction reports</li> <li>• travels with cash amounts in a way that avoids declaring cross border movements of the cash</li> </ul>
<b>Suspicious matter report (SMR)</b>	A report that 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.
<b>Third party service providers</b>	Services that businesses often use to facilitate the final payment to a beneficiary.
<b>Threshold transaction report (TTR)</b>	A report that must be submitted to AUSTRAC when a designated service provided to a customer involves a transfer of physical currency of \$10,000 or more, or the foreign currency equivalent.
<b>Transaction monitoring program</b>	Part A of a reporting entity's AML/CTF program must include a risk-based transaction monitoring program that comprises of appropriate systems and controls to monitor the transactions of customers and identify suspicious transactions.
<b>Trigger-based reporting</b>	Where a reporting entity submits a suspicious matter report to AUSTRAC solely on the basis of a trigger generated by their transaction monitoring system without conducting further investigation.
<b>Unregistered remittance dealers</b>	A person or entity providing remittance services (also known as money transfer) in Australia without being registered with AUSTRAC. It is against the law to provide remittance services in Australia without being registered.

## APPENDIX B: RISK ASSESSMENT METHODOLOGY

The methodology used for this risk assessment follows Financial Action Task Force 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 these 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.

CRIMINAL THREAT ENVIRONMENT		
LOW	MEDIUM	HIGH
Minimal variety of money laundering methodologies. There is a low level of involvement by serious organised crime groups and other higher-risk entities.	Money laundering methodologies are moderately varied. There is a medium level of involvement by serious organised crime groups and other higher-risk entities.	Money laundering methodologies are highly varied. There is a high level of involvement by serious organised crime groups 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 serious organised crime groups and other higher-risk actors.	Predicate offences are moderately varied. There is a medium level of involvement by serious organised crime groups and other higher-risk actors.	Predicate offences are highly varied. There is a high level of involvement by serious organised crime groups and other higher-risk actors.
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
Few higher-risk customers	A moderate number of higher-risk customers	A high number of higher-risk customers
Subsector has a small customer base.	Subsector has a medium customer base.	Subsector has a large customer base.
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

