



Australian Government

AUSTRAC

FIGHTING
FINANCIAL
CRIME
TOGETHER



INDEPENDENT REMITTANCE DEALERS 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).

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

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



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

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

CONTACT US

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

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

CONTENTS

EXECUTIVE SUMMARY	4
PURPOSE.....	9
BACKGROUND	10
METHODOLOGY	13
REPORTING TO AUSTRAC.....	15
CRIMINAL THREAT ENVIRONMENT	18
Money laundering	20
Terrorism financing.....	25
Predicate offences	27
VULNERABILITIES	34
Customers	35
Products and services	40
Delivery channels	44
Foreign jurisdictions	48
CONSEQUENCES.....	52
Customers	53
Individual reporting entities and the subsector	53
Australian financial system and the community	54
National and international security	54
RISK MITIGATION STRATEGIES.....	55
APPENDIX A: GLOSSARY	61
APPENDIX B: RISK ASSESSMENT METHODOLOGY	64

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.¹ Remittance services are a crucial component of global financial inclusion, for example by enabling customers to send money to locations that traditional banking infrastructure may not service.

Independent remittance dealers (IRDs) operating in Australia are remittance service providers that use their own products, platforms or systems to provide remittance services directly to customers. IRDs can be registered as a single entity operating independently, or own and operate multiple branches.

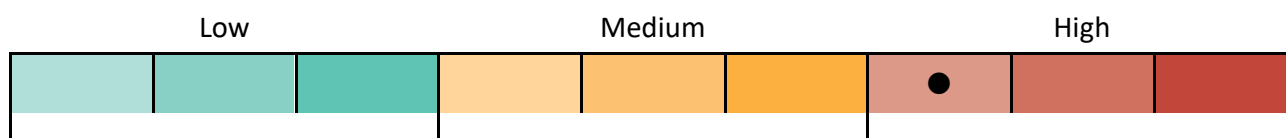
Based on AUSTRAC's Remittance Sector Register, 816 IRDs were considered in-scope for this risk assessment and these entities provide services to approximately 2.2 million customers. For the purpose of this report, this cohort of remittance service providers is referred to as **IRDs**, the **IRD subsector** or the **subsector**.

The characteristics and activities of individual IRDs vary significantly and range from very large reporting entities (**major IRDs**) to very small operators that conduct few remittance transactions during the reporting period.² 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.

¹ Remittance service providers are also known globally as 'money transfer businesses'.

² For the purposes of this report 'major IRDs' are defined as reporting entities with an IRD registration that submitted more than \$500 million worth of IFTIs in 2019. Of the 816 IRDs in-scope for this report, 25 are considered to be major IRDs.

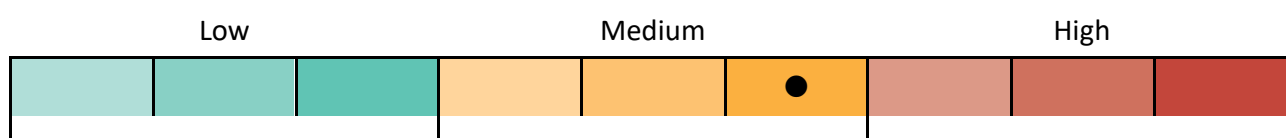
OVERALL RISK RATING



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

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

CRIMINAL THREAT ENVIRONMENT



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

The criminal threat environment facing IRDs is varied and encompasses simple schemes by opportunistic criminals as well as instances of more sophisticated activity by serious and organised crime. While most instances of suspected exploitation involve low-to-moderate value transactions, there are also instances that involve high-value exploitation.

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

A small number of major IRDs dominate suspicious matter reports (SMR) submitted to AUSTRAC; major IRDs submitted 88 per cent of the subsector's SMRs in the reporting period. It is highly likely this is due to considerable diversity across the subsector. Many major IRDs have sophisticated systems and controls designed to detect a wide variety of crime types, and large customer bases that send funds to multiple jurisdictions. On the other hand, smaller IRDs may only provide remittance services to a small group of customers from a shared cultural background, and that only remit funds to a single jurisdiction. Just under a 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 IRDs.

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 threats facing the IRD subsector is assessed as **high**.

Money laundering was the most common threat impacting the subsector. Most instances of suspected money laundering had moderate associated values, although there were instances of high-value exploitation. AUSTRAC and partner agency intelligence indicates a small number of IRDs likely have links to serious and organised crime groups, indicating sophisticated exploitation of the subsector.

IRDs are primarily exploited in the placement and layering phases of the money laundering process.³ This is because many IRDs accept cash transactions and specialise in moving funds quickly and at low

³ The money laundering process involves three stages: placement, layering and integration. These terms are defined in the **Glossary** at **Appendix A**.

cost, making the subsector an efficient means to place and layer criminal proceeds. Criminals wishing to launder funds often seek out reporting entities they perceive to have poor or inconsistent record-keeping practices.

Terrorism financing

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

While the overall terrorism financing threat to the IRDs has declined in recent years, the subsector continues to be exposed to terrorism financing. IRDs submitted 26 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 per cent of all terrorism financing intelligence reports assessed for this report were linked to IRDs.

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 IRDs is assessed as **medium**.⁴

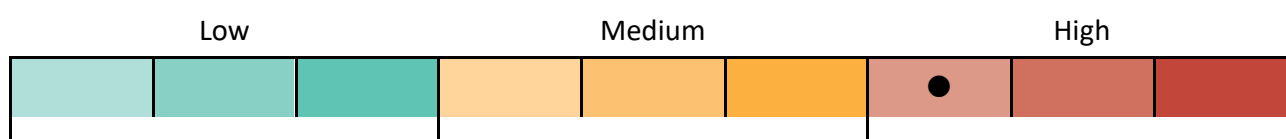
The IRD subsector is exposed to a variety of predicate offences. Most offending appears to be opportunistic, largely unsophisticated and low in associated value. However, some sophisticated and high-value offending has also been observed.

The key predicate offences impacting the subsector are frauds, scams, child exploitation and drug trafficking. To a lesser extent IRDs are also exposed to tax evasion.⁵

More than half of all predicate offences identified by IRDs were frauds and scams. Identity fraud was the most common type of fraud, followed by 'other fraud' and investment fraud.⁶ The most common scam types were romance scams, false billing scams and remote access scams.

Major IRDs were linked to the overwhelming majority of suspected predicate offending. This is highly likely due to the cohort's dominance of the subsector and a reflection of major IRDs having more sophisticated anti-money laundering and counter-terrorism financing (AML/CTF) systems and controls, which lead to more detections and reporting of suspicious activities.

VULNERABILITIES



AUSTRAC assesses the IRD 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:

⁴ 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.

⁵ 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.

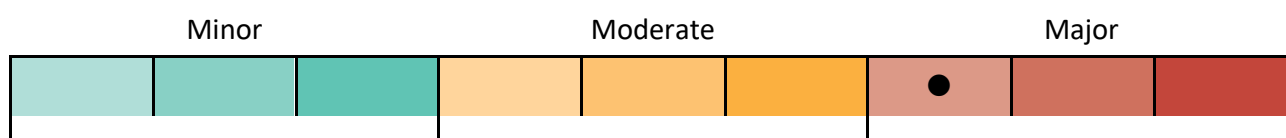
⁶ SMRs were categorised as 'other fraud' by AUSTRAC analysts when the underlying type of fraudulent activity could not be identified.

- outsourcing, which lengthens the product delivery chain and reduces the level of oversight a reporting entity might have over customers and transactions
- use of offsetting arrangements, which can help mask the ultimate beneficiary and complicate detection of illicit funds flows⁷
- high exposure to foreign jurisdictions, including higher-risk jurisdictions.

Other features that can 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, overseas-based ordering customers, and some companies, trusts and other legal entities⁸
- a declining level of face-to-face customer contact in favour of remote service delivery channels, particularly online services and the use of third parties. These channels can offer criminals anonymity, such as through the use of mule accounts created using stolen identities.

CONSEQUENCES



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

Customers

Criminal activity can have **moderate** consequences for customers of IRDs. 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 **major** financial, reputational or operational consequences for IRDs and the subsector. This includes de-banking of non-major IRDs, which may be perceived as having less sophisticated risk mitigation strategies than major IRDs. De-banking has constrained the operations of some reporting entities and forced others out of business. In some instances, it has also increased the cost of doing business because impacted IRDs must find a way to operate without access to banking infrastructure.

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 IRDs can have **major** consequences for national and international security. Serious and organised crime groups are likely to be linked to a small number of IRDs. Successful money laundering through the subsector can result in the preservation of illicit assets and help finance new

⁷ Offsetting is a method of value transfer using reciprocal debit and credit arrangements between businesses.

⁸ 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.

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.

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

Implementation of risk mitigation strategies varies significantly across the subsector. Reporting entities surveyed for this report advised they have implemented risk mitigation strategies such as customer due diligence (CDD) procedures, customer risk rating tools, product controls, and transaction limits.

However, some entities have mixed approaches to their CDD obligations, deliver limited (or no) AML/CTF training to their employees, or generally lack an 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.

Other factors that may exacerbate ML/TF risk include:

- CDD processes, including ongoing and enhanced CDD procedures, which are designed for natural persons and may be inadequate for complex corporate customers
- the lack of understanding of and failure to properly consider the difference between customers' source of funds and source of wealth
- the absence of comprehensive enterprise-wide ML/TF risk assessments, or failure to conduct regular independent reviews of risk management frameworks.

PURPOSE

This assessment provides specific information to the IRD subsector on the ML/TF risks it faces at the national level. Its primary aim is to assist IRDs 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 IRDs 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 extreme diversity across the subsector and recommends this assessment be considered according to each business' 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 remittance network providers and their affiliates. 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

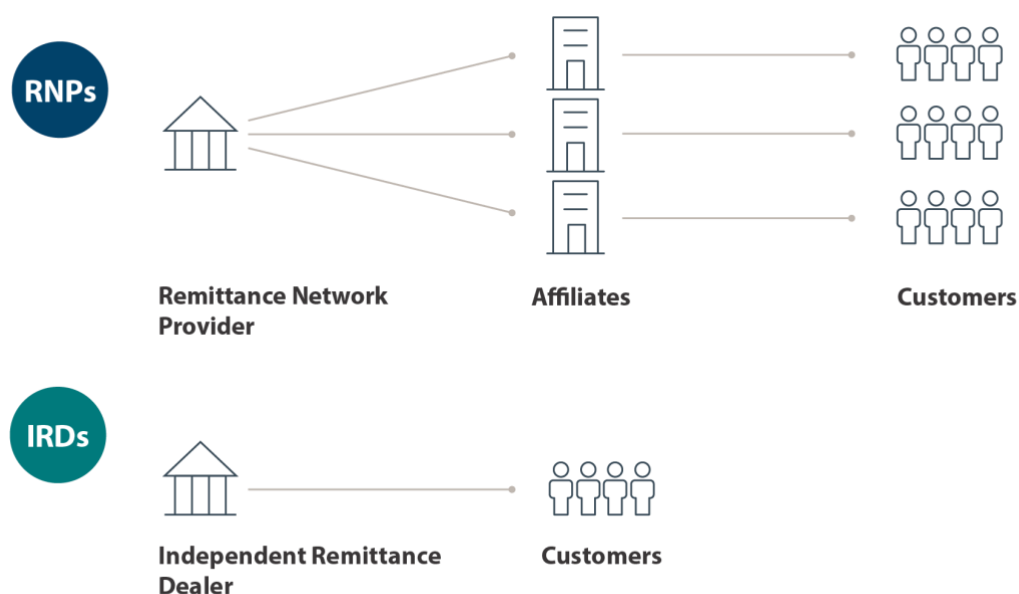
Remittance service providers operating in Australia offer fast and relatively low-cost methods of transferring funds domestically and overseas. These services are particularly important for migrant communities and expatriate workers supporting families in their countries of origin.

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 IRD, a remittance network provider, or an affiliate.

- **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.
- A **remittance network provider (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. Please refer to AUSTRAC's [ML/TF risk assessment of remittance network providers and affiliates](#) for further information regarding the risks specific to these businesses.
- 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.

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.



IRD SUBSECTOR

During the reporting period there were 816 IRDs operating in Australia, of which 25 are considered major IRDs. The subsector provided services to an estimated 2.2 million customers.⁹

The number of registered IRDs increased by a third from 2015 to 2020. IRDs consulted for this report indicate the subsector will likely continue expanding over the next five years, although growth could be hampered by COVID-19-related impacts on customer numbers and IRD 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.¹⁰ These trends are further discussed in the **Customers** section on page 35.

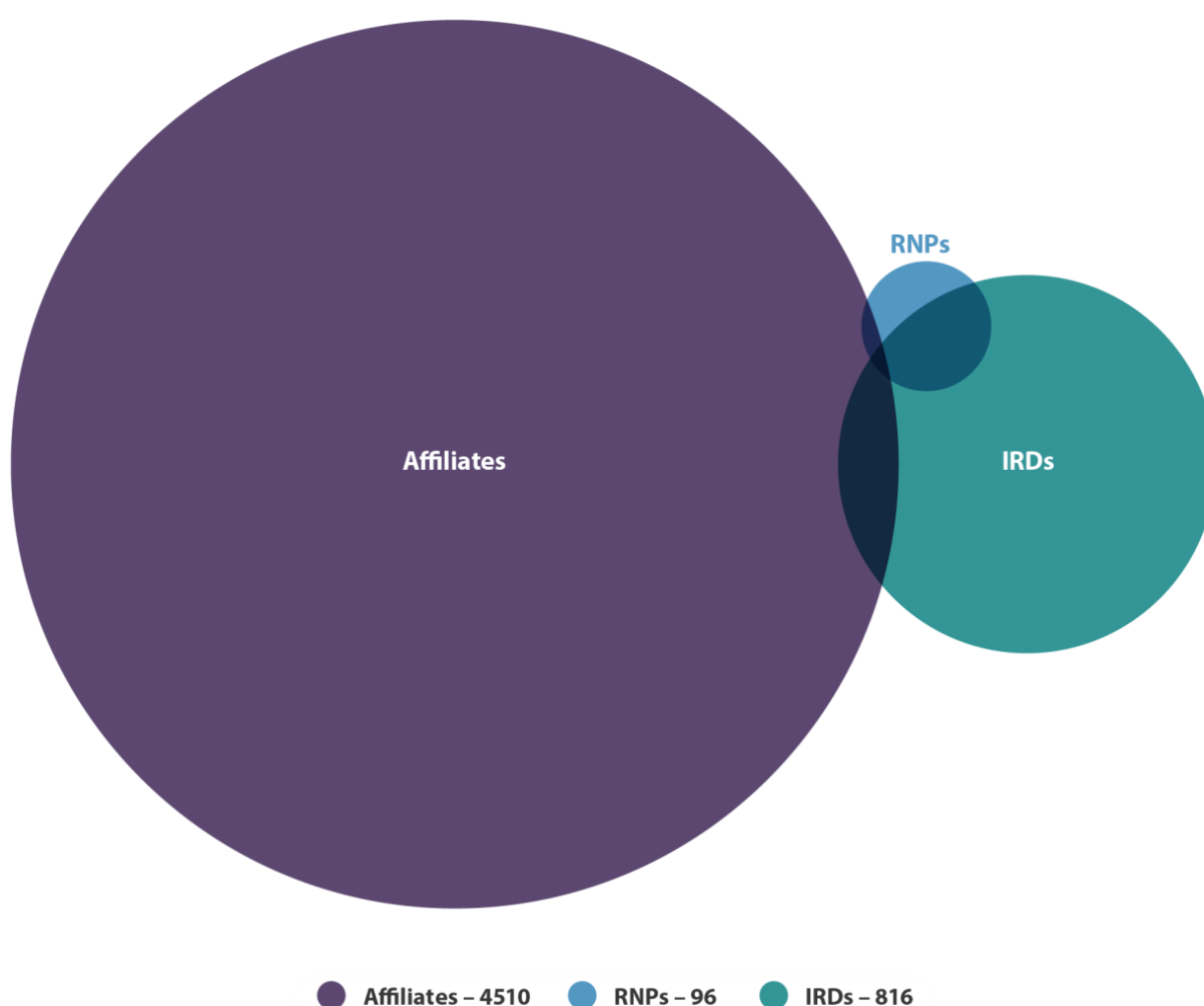


Figure 1: Number of registered remittance service providers in Australia during the reporting period

⁹ This number was derived from analysis of IFTIs submitted by IRDs in the reporting period. It is an approximation only.

¹⁰ 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), IRDs are required to maintain a compliant 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 IRDs vary significantly. There is extreme diversity between IRDs, including the size of commercial activity, foreign jurisdictions serviced, and the number of customers served. The subsector includes large corporations that offer services to a wide array of jurisdictions, as well as small businesses that provide remittance services to specific communities or remittance corridors. Consequently, the ML/TF risks associated with individual businesses can vary significantly.

This risk assessment isolates findings associated with ‘major IRDs’ where possible. For the purposes of this report, ‘major IRDs’ are defined as reporting entities with an IRD registration that submitted more than \$500 million worth of IFTIs in 2019.

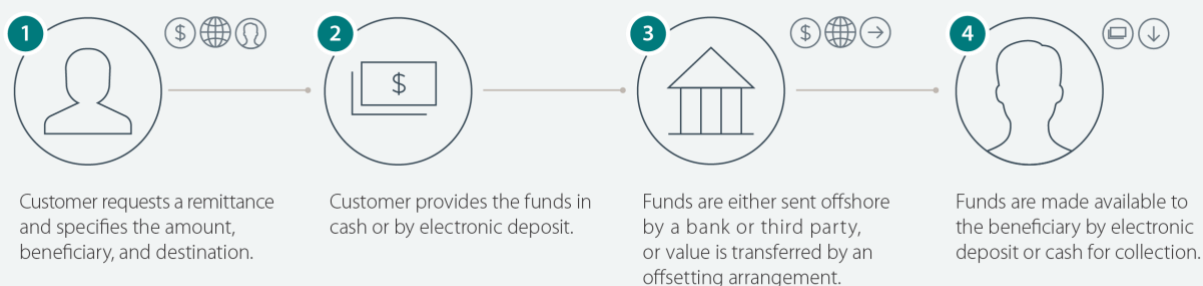
AUSTRAC acknowledges not all risks will be relevant for every reporting entity. In addition, some risks relate to the nature of remittance activity in general, and are not attributes specific to IRDs. The risk rating criteria used in this assessment is designed to capture an overall rating for the subsector.

A TYPICAL REMITTANCE SERVICE

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

1. The customer contacts the IRD 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 IRD. Funds can be provided in cash or deposited electronically to the IRD’s bank account.
3. Depending on whether an IRD has a bank account or not, funds will be sent 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, which states that ML/TF risk can be seen as a function of criminal threat, vulnerability and consequence. In this assessment:

- **Criminal threat environment** refers to the nature and extent of ML/TF and relevant predicate offences in the IRD subsector.
- **Vulnerability** refers to the characteristics of IRDs 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 1,298 SMRs that IRDs submitted between 1 January 2019 and 31 December 2019 (the **SMR sample**).¹¹ See the **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; 13 per cent of these reports relate to IRDs (the **IR review**).¹²
3. The results of data-matching (the **data-matching exercise**) of IFTIs, TTRs and SMRs submitted to AUSTRAC by IRDs between 1 January 2019 and 31 December 2019 and criminal entities who were:
 - recorded as a member of serious organised crime 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.

¹¹ 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.

¹² 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 government agencies, academic institutions, reporting entities and the media.
5. Feedback and professional insights offered during interviews, surveys and consultations with a range of partner agencies and IRD representatives, as well as industry experts and industry associations. This includes survey responses from 69 IRDs (the **IRD survey**).

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

REPORTING TO AUSTRAC

REPORTS SUBMITTED BY IRDs BETWEEN 1 JANUARY 2019 AND 31 DECEMBER 2019^{13 14}

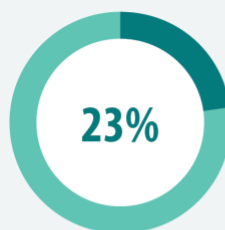
SMRs Number of SMRs: 17,183



of all SMRs were submitted by major IRDs



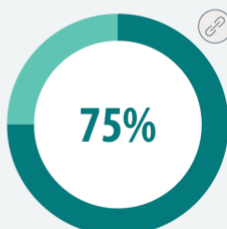
of IRDs submitted at least one SMR



of active IRDs submitted at least one SMR



Total value of SMRs

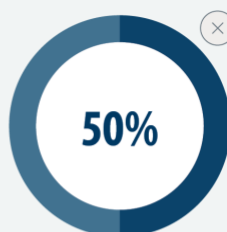


of the total value of SMRs was linked to major IRDs

IFTIs Number of IFTIs: 18.8 million



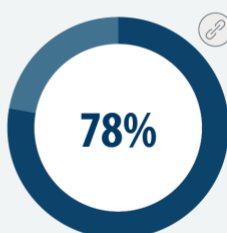
of all IFTIs were submitted by major IRDs



of IRDs did not submit any IFTIs



Total value of IFTIs

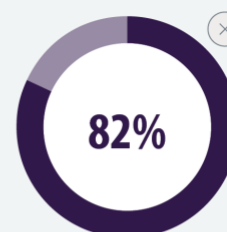


of the total value of IFTIs was linked to major IRDs

TTRs Number of TTRs: 58,913



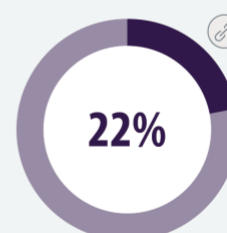
of all TTRs were submitted by major IRDs



of IRDs did not submit any TTRs



Total value of TTRs



of the total value of TTRs was linked to major IRDs

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

¹⁴ 'Active IRDs' is defined as an IRD that has submitted at least one IFTI in the reporting period

SMR SUBMISSIONS

Across the subsector, the value and volume of SMR submissions during the reporting period was unevenly distributed. Major IRDs were responsible for 88 per cent of all SMRs submissions, and 75 per cent of the total SMR dollar value during the reporting period. On the other hand, 87 per cent of registered IRDs did not submit an SMR during this period, suggesting under-reporting occurs across the subsector.

In addition, 35 per cent of reports 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 major IRDs, which account for more than three-quarters of all IFTIs submitted in the reporting period. Half of IRDs did not submit an IFTI, suggesting they were not actively providing remittance services during this period.

Why are IFTIs important to AUSTRAC and its partner agencies?

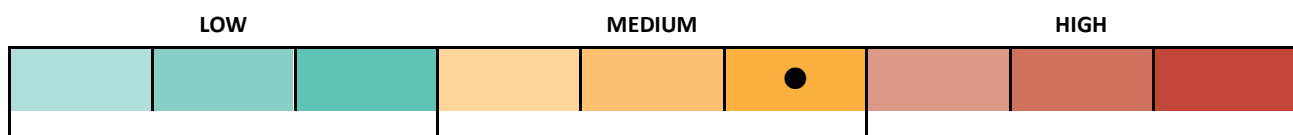
IFTI reporting drives a significant portion of AUSTRAC's intelligence work. The information in IFTI reports are an integral component of AUSTRAC's strategic and tactical intelligence outputs, and contributes to domestic and foreign partner agency investigations. IFTIs close a critical intelligence gap 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 firearms
- illegal tobacco
- drug trafficking
- modern slavery
- cyber-enabled crime
- child sex exploitation
- bribery and corruption
- illegal trade in fauna and flora
- trade-based money laundering.

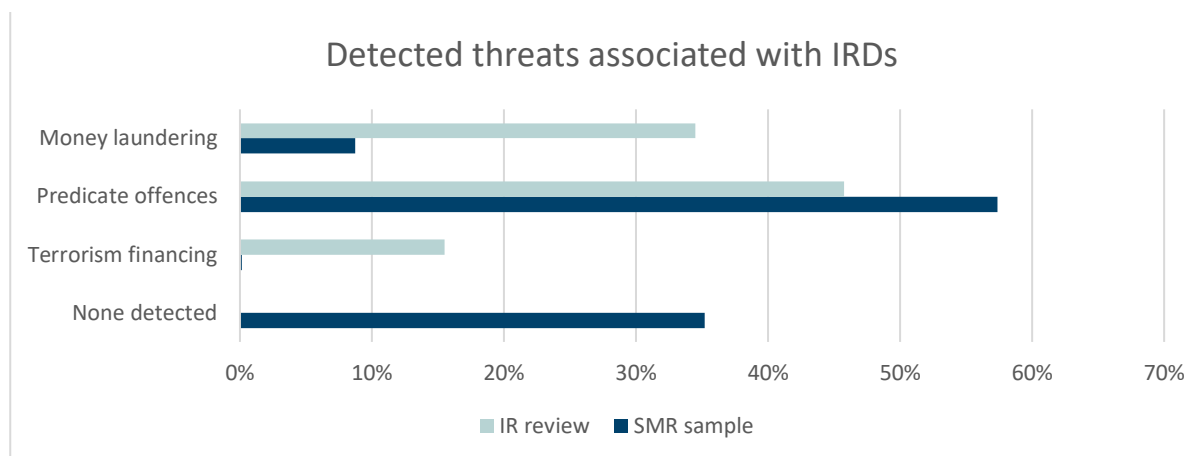
CRIMINAL THREAT ENVIRONMENT



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

AUSTRAC assess the criminal threat environment facing the IRD subsector as **medium**.

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



The IRD subsector faces a high risk of money laundering, with instances of sophisticated methods and actors identified exploiting the sector. AUSTRAC and partner agency intelligence indicates that some IRDs are likely linked to criminal actors, including members of serious and organised crime groups.

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

IRDs are also moderately exposed to a variety of predicate offences, which range in sophistication from opportunistic offending to complex schemes. The key predicate offences impacting IRDs are frauds, scams, child exploitation and drug trafficking.

The nature and extent of threats associated with major IRDs are different from those associated with non-major IRDs. Suspected instances of terrorism financing and predicate offences are concentrated in major IRDs, however, instances of money laundering are more evenly distributed between the two cohorts (see figures 2 and 3). In recognition of this variance, this report will distinguish the findings of the SMR sample and IR review linked to major IRDs from those linked to non-major IRDs.

It is highly likely that some IRDs under-report SMRs to AUSTRAC. During the reporting period, 87 per cent of in-scope IRDs did not submit an SMR. While AUSTRAC has increased its guidance and outreach to the subsector in recent years, 35 per cent of 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.

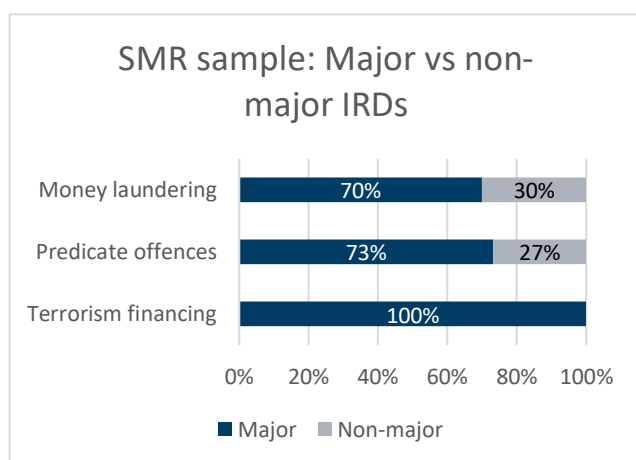


Figure 2: Threat groups associated with IRDs from the SMR sample

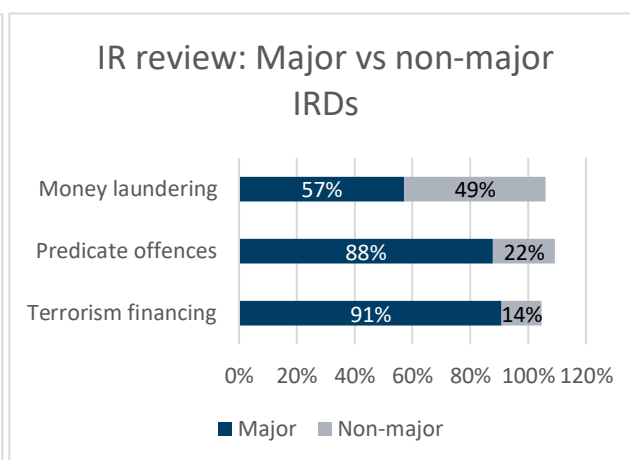


Figure 3: Threat groups associated with IRDs in intelligence reports. Values add up to more than 100 per cent because an intelligence report can relate to multiple reporting entities.

MONEY LAUNDERING

AUSTRAC assesses the nature and extent of money laundering threats facing the IRD subsector as **high**.

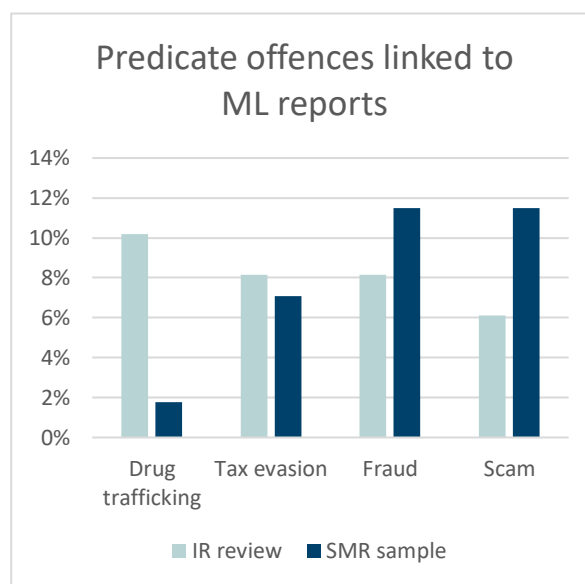
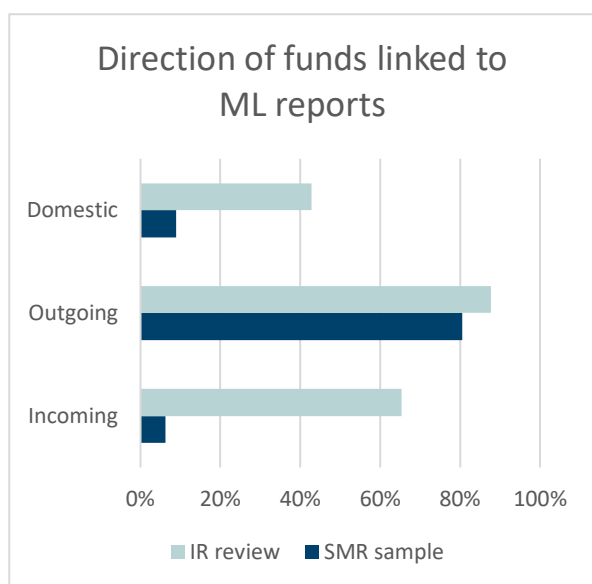
Suspected money laundering instances were identified in nine per cent of the SMR sample and 35 per cent of the IR review. Associated values were moderate-to-high.¹⁵ The average value of money laundering-related reports in the SMR sample was \$38,000, with several SMRs exceeding \$1 million. A third of 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 under-reporting. Major IRDs submitted 70 per cent of the SMRs in the sample that identified suspected money laundering.

Partner agency intelligence indicates a high level of criminal exploitation of a small number of IRDs, including some with likely links to serious and organised crime groups. Of intelligence reports linking the subsector to suspected money laundering, 57 per cent related to major IRDs and 49 per cent related to non-major IRDs.¹⁶ This indicates money laundering activity is more evenly spread between major IRDs and their non-major counterparts than is the case with terrorism financing or predicate offences (see figure 3). This trend is partly attributable to a number of intelligence reports of non-major IRDs potentially linked to serious and organised crime (see page 22).

The subsector is primarily exploited in the placement and layering phases of the money laundering process. This is because many IRDs accept cash and specialise in moving funds quickly and at low cost. Conducting multiple transactions across a range of financial institutions – such as domestic and foreign banks, as well as currency exchanges – was a frequently identified money laundering method, which is designed to obscure the source of funds or ultimate beneficiary of a remittance.

More than 80 per cent of money laundering SMRs involved outgoing transactions. The most common foreign jurisdictions noted in the money laundering-related SMRs were China, Nigeria, USA, and the UK. Most suspected money laundering activities are linked to key proceeds-generating predicate offences in Australia such as frauds, scams, drug trafficking, and tax evasion. These are discussed in detail in the **Predicate offences** on page 27.



¹⁵ 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).

¹⁶ These figures add up to more than 100 per cent because some intelligence reports identified suspected money laundering activities in both major and non-major IRDs.

The actual extent of exploitation of IRDs is almost certainly higher than indicated in the SMR sample. This is likely due to under-reporting of suspected money laundering, varying levels of sophistication and capacity in AML/CTF responses, and concerns that some IRDs are likely linked to criminal entities (see page 22).

Common indicators of suspected money laundering activity identified in the SMR sample include:

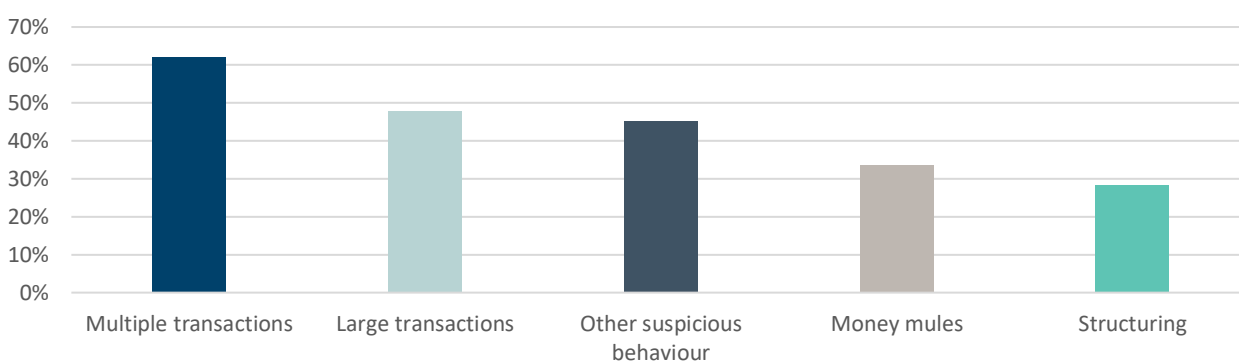
- unexplained source of funds
- using multiple debit cards or cash payments to fund remittances
- remittances to jurisdictions inconsistent with a customer's profile
- funding remittances with structured cash deposits to avoid reporting thresholds
- several customers opening accounts within a short period of time, in a seemingly coordinated manner
- a customer enquiring about transaction limits or requesting their name be omitted from the transaction.
- multiple remittances to the same recipient from multiple individuals, with no apparent connection between the sender and recipient.

LAUNDERING OF SCAM PROCEEDS THROUGH MULE ACCOUNTS

In a suspected tax impersonation scam, victims were contacted by phone and told they owed unpaid taxes to the ATO. Victims were instructed to make ATM cash deposits into various bank accounts held and operated by Australia-based foreign national money mules. Once they received the funds, the money mules used an IRD to remit the funds to the same beneficiary located overseas. The amount lost per victim ranged from \$1,000 to \$7,000. Most money mules were holders of temporary Australian visas and were complicit in the scam.

Criminals exploit existing bank and remittance accounts belonging to foreign students or migrants to provide a veneer of legitimacy to their money laundering activities. This is because it is not unusual for these customers to conduct low value and semi-frequent outbound transactions.

Methods linked to ML-related SMRs



The data-matching exercise indicates the subsector is exposed to a high proportion of individuals charged with money laundering offences. These individuals were collectively linked to moderate associated values (refer to **Higher-risk customers** on page 36). While some transactions linked to these individuals are likely to be legitimate, their use of the subsector exposes it to a high risk of money laundering. AUSTRAC assesses the actual number of criminal entities exploiting the subsector is likely

higher than reflected in the data matching exercise results. This is because criminal entities use ‘cleanskins’ or money mules to conduct transactions on their behalf, and some reporting entities likely under-report to AUSTRAC, which would impact the data-matching results.¹⁷

AUSTRAC and partner agency intelligence indicates that it is likely a small number of IRDs facilitate money laundering activities for serious and organised crime groups, including acting as a location to securely store cash for professional money laundering organisations. These IRDs are likely to be part of a larger, sometimes global, network of companies that is exploited to layer criminal proceeds through international remittances. Complicit remittance service providers facilitating this type of activity helps to mask the true source and destination of funds, and significantly complicates partner agency detection efforts.

Where IRDs are suspected of facilitating money laundering activities, observed methods include:

- co-mingling legitimate business earnings with criminal proceeds
- under-reporting or non-reporting to AUSTRAC. This can include pooling multiple transactions into one IFTI, or failing to declare cross-border movements of large amounts of cash.
- use of offsetting arrangements, particularly when the IRD perceives this channel to be subject to less regulatory or law enforcement scrutiny. Offsetting arrangements can circumvent international funds transfer reporting requirements and facilitate both incoming and outgoing money laundering activities (see **Offsetting** on page 47).

Sophisticated criminals and serious organised crime groups reportedly 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 more likely to aid criminal activity or employ weak AML/CTF controls.

¹⁷ A ‘cleanskin’ is a person without a criminal history nor identifiable links to criminals who acts on behalf of a criminal entity in order to provide a veneer of legitimacy to such activities.

IRDs USE CUCKOO SMURFING, OFFSETTING TO MOVE CRIMINAL PROCEEDS OFFSHORE

AUSTRAC partnered with a law enforcement agency on an investigation to target the drug supply and money laundering networks of serious organised crime entities.

During the investigation a law enforcement partner located approximately \$1 million cash at the residential premises of an AUSTRAC registered remitter (Remitter A) that was likely proceeds of crime. A number of money transfer receipts, issued by other registered remittance businesses (Remitter B and Remitter C), were also located.

Remitter A claimed the money was for legitimate remittance; however analysis by AUSTRAC of holdings showed Remitter A had reported small incoming and outgoing IFTIs to AUSTRAC in the two years since registration (approximately \$800,000 both ways). This showed that Remitter A's business did not deal in large funds, so the \$1 million was not likely to be from legitimate business.

Using additional intelligence and data, AUSTRAC undertook further analysis, which led to the discovery of a small number of AUSTRAC registered remitters using a number of methodologies, including cuckoo smurfing and offsetting, to launder illicit funds. This involved Remitter A collecting the illicit funds from organised crime groups and providing it to Remitter B and Remitter C, which had outstanding IFTI obligations. Remitter B and Remitter C would subsequently deposit the illicit cash into the domestic accounts of the customers who were expecting the money from overseas. This would result in a threshold transaction report being submitted to AUSTRAC by the bank when the cash was deposited.

Remitter B and Remitter C would then provide a receipt to Remitter A. This receipt was the equivalent of money owed to Remitter A by an offshore money service business. These details would then be provided to offshore crime groups who would collect the funds from the offshore money service business.

By doing this, the illicit funds were disposed of onshore, the customer expecting funds from overseas received the expected money into their bank account, the Australian based crime group paid the offshore crime group, and no money physically moved across the border.

In the absence of the money transfer receipts and the TTRs, this activity would be invisible. AUSTRAC was able to use the indicators observed in the TTRs, and apply these to create filters to proactively identify and target similar activity in the future.

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 largely because criminal proceeds are often derived in cash and many IRDs 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. Half of respondents to the IRD survey indicated that they no longer accept cash (see **Use of cash** on page 40), which also mitigates the risk of cash-based money laundering in the subsector.

Suspicious cash transactions were identified in 27 per cent of money laundering-related reports in the SMR sample and 88 per cent in the IR review. Common methods and themes may include:

- large transactions
- unexplained wealth
- use of foreign currency exchange services
- use of money mules and other third-party depositors
- multiple transactions with no apparent economic rationale
- structured cash deposits for remittance transactions with no apparent economic rationale.



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

TERRORISM FINANCING

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

This assessment is based on a low number of terrorism financing-related SMRs submitted by IRDs, 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 IRDs 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, IRDs are still exposed to exploitation to facilitate or support terrorism financing. For example:

- IRDs were identified in 20 per cent of all terrorism financing-related intelligence reports assessed in the IR review.¹⁸
- Terrorism financing was identified in 15 per cent of all intelligence reports linked to IRDs. Of these, 91 per cent were linked to major IRDs and 14 per cent were linked to non-major IRDs.¹⁹
- IRDs submitted 26 terrorism financing-related SMRs during the reporting period.²⁰ This represents four per cent of all terrorism financing-related SMRs that reporting entities submitted during this period. Major IRDs submitted all 26 SMRs.
- No individuals charged with terror-related offences were identified as customers of IRDs during the reporting period. This finding is inconsistent with the significant level of intelligence reports linking the subsector to suspected terrorism financing and is likely a result of intelligence reports that detailed suspicions but did not lead to individuals being charged.

Associated transaction values in the SMR sample and IR review were generally low, and terrorism financing methods were largely unsophisticated.²¹ 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 customer types, however several non-profit organisations were also noted.

¹⁸ These intelligence reports were often based on IFTIs rather than SMRs. This explains why IRDs were identified in 20 per cent of terrorism financing-related intelligence reports but just four per cent of terrorism financing-related SMRs.

¹⁹ Values add up to more than 100 per cent because an intelligence report can relate to multiple reporting entities (e.g. can involve both a major IRD and non-major IRD)

²⁰ Determined by keyword analysis of all AUSTRAC SMRs submitted between 1 January 2019 to 31 December 2019.

²¹ The average associated value of reports in the SMR sample was \$58,000. 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 IRDs 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 IRD, 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:

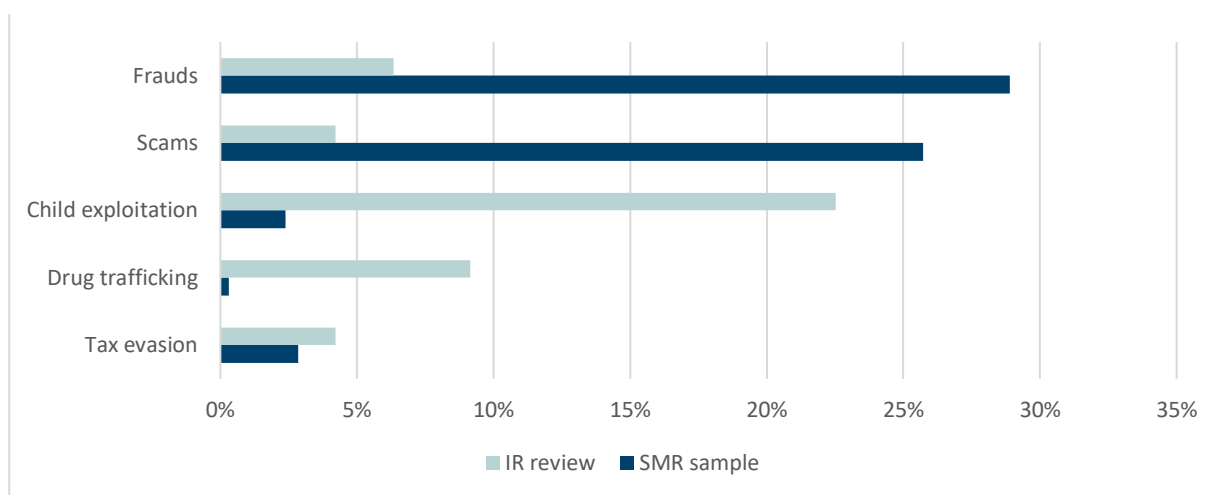
- a customer remitting funds to multiple beneficiaries in a higher-risk jurisdiction
- multiple customers remitting funds to the same beneficiary, especially in jurisdictions deemed higher-risk for terrorism financing
- open source reporting that any parties to the transaction have links to known terrorist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

PREDICATE OFFENCES

AUSTRAC assesses the nature and extent of threat posed by predicate offending involving IRDs 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, IRDs are also exposed to tax evasion.



Major IRDs were linked to the overwhelming majority of reporting that identified a predicate offence. This is highly likely a result of their dominance of the subsector in terms of customers, transactions, and foreign jurisdictions serviced. It is also likely that major IRDs have more sophisticated AML/CTF systems and controls, leading to more detections and reporting of suspicious activities.

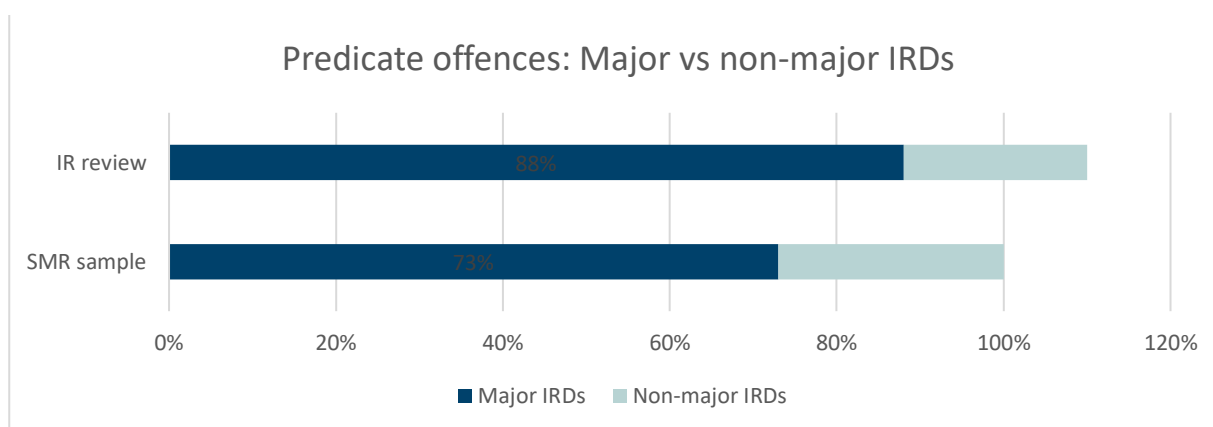


Figure 1: Values add up to more than 100 per cent because an intelligence report can relate to multiple reporting entities.

IDENTIFYING PREDICATE OFFENCES – A CHALLENGE FOR REPORTING ENTITIES

The actual extent of predicate offences involving IRDs is almost certainly higher than is represented in the SMR sample. Thirty-five per cent 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 IRD to identify because it occurs outside of the remittance process, 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.

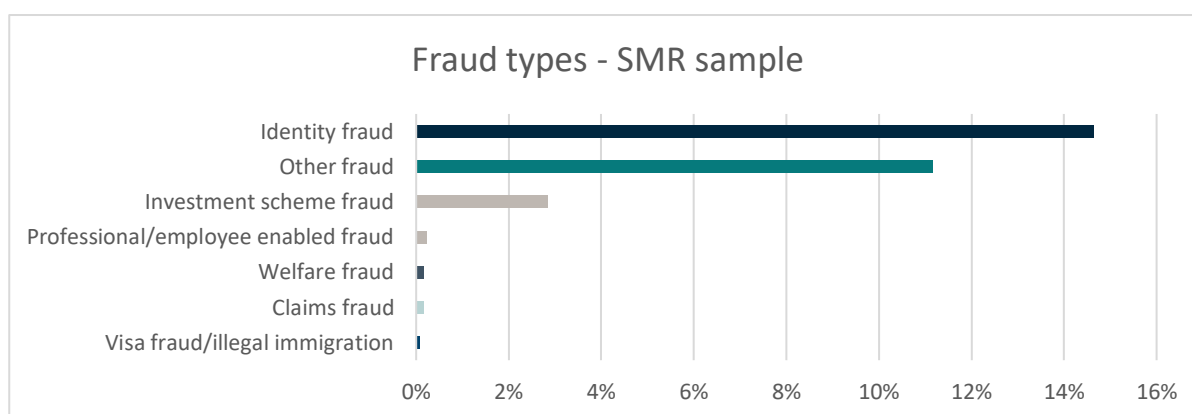


SMRs that do not identify a predicate offence can still contain important pieces of intelligence that form part of a bigger picture of offending. Reporting entities should remain vigilant of key criminal market trends in Australia and report any suspicions of related financial transactions to AUSTRAC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

Frauds

Frauds were the most commonly identified predicate offence in the SMR sample (29 per cent) and the third most common identified in the IR review (six per cent).²² Of these, 61 per cent of SMRs and 78 per cent of intelligence reports were linked to major IRDs.

The primary fraud-type was identity fraud (15 per cent), although 11 per cent of SMRs were categorised as 'other fraud' because the underlying type of fraudulent activity could not be identified. Investment fraud was the next most common type of fraud, with three per cent of the SMR sample.



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.

Major IRDs were most commonly linked to suspected fraudulent activity. Criminals likely target these IRDs because their global reach maximises options for both payment and collection of criminal proceeds. Using a global IRD may also lend credibility to the fraud if the offenders are impersonating a well-known company or government department. In addition, major IRDs often have more

²² Intelligence reports generally identify serious criminal activity so they likely under-represent the overall volume of frauds and scams impacting the subsector

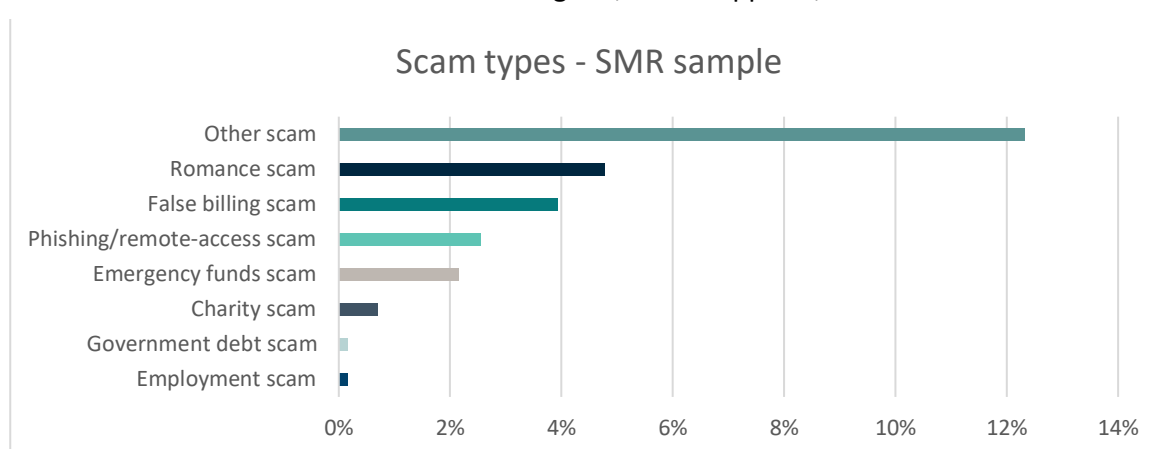
sophisticated AML/CTF strategies, which almost certainly result in more frauds being detected and reported to AUSTRAC.

Scams

Scams were the second most commonly identified predicate offence in the SMR sample (26 per cent) and the equal fourth most common identified in the IR review (four per cent). Of these, 92 per cent of SMRs and 67 per cent of intelligence reports were linked to major IRDs.

The most common scam types were romance scams, false billing scams and remote access scams. However, a significant portion of scam-related SMRs were categorised as 'other scam' because the exact nature of the underlying scam activity was difficult to determine.

The majority of reports had associated values under \$5,000. The top three foreign jurisdictions associated with scam-related SMRs were Nigeria, the Philippines, and the USA.



Almost all scam-related SMRs involved outgoing transactions. Offshore scammers often request funds be sent through larger IRDs, which are likely favoured for their large international footprint and a perception that lower values will get lost in the large volume of transactions.

Consultations with IRDs confirmed that victims will rarely admit that scammers have deceived them. It can therefore be difficult to dissuade them from proceeding with transactions that could be a scam. Some IRDs will not process transactions they suspect are part of a scam as a matter of policy, while others will process a transaction only after discussing their concerns with a customer.

OVERSEAS SCAMMERS TARGETING IRD CUSTOMERS

During 2019, an IRD customer received an unsolicited scratch card in the mail. The card instructed the customer to send an 'administration fee' to an overseas entity in order to claim a 'prize', which never arrived. The IRD reviewed transactions with similar amounts, currencies, dates and destinations and determined that the same entity had defrauded a number of customers.

All customers registered with the IRD at approximately the same time and sent funds to the same country. Several customers also sent funds to the same beneficiary. One beneficiary used multiple bank accounts, likely in an attempt to disperse the funds or evade suspicious transaction monitoring triggers. Some customers believed they were sending funds for investments, despite the payments being directed to individuals rather than companies. These transactions formed the basis of several SMRs submitted to AUSTRAC and details of the beneficiaries were added to the IRD's internal watch list.



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

IRDs USED TO MOVE INTERNATIONAL INVESTMENT SCAM PROCEEDS OFFSHORE

In 2019, a partner agency identified several IRDs being exploited in an attempt to launder the proceeds of an investment scam. The scam involved unwitting victims receiving cold calls from a representative of an Australian-registered company promoting investment opportunities. Once deceived, victims would send funds to domestic bank accounts which they were led to believe are affiliated with the company.

These accounts were typically opened by money mules linked to the scam and belonged to international visitors on temporary visas who were part of the scheme. Although some of the funds were accessed in Australia through ATM withdrawals, the scammers used IRDs to send the majority of funds offshore – to the value of \$1.6 million.

Child exploitation

Child exploitation was identified in two per cent of the SMR sample but was the most commonly identified predicate offence in the IR review (23 per cent). Of these, 71 per cent of SMRs and 100 per cent of intelligence reports were linked to major IRDs.

Recent AUSTRAC reporting indicates IRDs have been used to send payments for online child exploitation and to facilitate 'grooming' and child sex tourism. Remittance services allow rapid movement of funds to child exploitation facilitators (notably for 'pay per view' scenarios), who are frequently based in jurisdictions where remittance services are a prominent part of the financial system.

Twenty SMRs sampled for this assessment cited child exploitation as the grounds for suspicion. Three reported transactions in response to law enforcement enquiries, while seven flagged potential child exploitation concerns based upon jurisdictional risk. In each case, it was post-transaction analysis that led to the reporting entity submitting an SMR.



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. In several SMRs reviewed for this assessment, IRDs were unable to judge whether the customer was more likely to be engaged in child exploitation or a victim of a romance scam.

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 identified in the IR review (nine per cent). Of these, half the SMRs and 85 per cent of intelligence reports were linked to major IRDs.

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 2020-21.²³

The IR review indicates the subsector is likely exploited for small-scale drug trafficking activities, such as purchases of relatively small quantities of drugs or payments for drug transportation. This may be because many reporting entities in the subsector impose transaction limits.

²³ 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.

LOW-VALUE REMITTANCES LIKELY USED TO FUND DRUG SUPPLY

AUSTRAC analysis identified a suspected transnational drug trafficking syndicate using several foreign nationals in Australia to remit criminal proceeds overseas. Collectively, the individuals made a large number of low-value remittances and used the following methods in attempt to avoid attracting suspicion from the IRD:

- omitted the reason for the remittance
- used various IRDs in an attempt to obfuscate activity
- sent the remittances to various beneficiaries located in multiple foreign jurisdictions.

On the other hand, it is likely that a small number of IRDs with links to serious and organised crime are used to move large amounts of drug proceeds offshore (see **Money laundering** on page 22).

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 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 (three per cent) and the equal fourth most identified in the IR review (four per cent). Of these, 44 per cent of SMRs and 33 per cent of intelligence reports were linked to major IRDs.

Instances of suspected personal tax evasion were as common as suspected corporate tax evasion in the SMR sample. Because the subsector mostly services individual customers, this suggests that corporate tax evasion is overrepresented relative to the size of the corporate customer base. The average value of corporate tax evasion-related SMRs was also six times larger than personal tax evasion SMRs. Therefore the associated harm of corporate tax evasion through the subsector is likely higher.

Common themes of tax evasion-related SMRs include:

- unexplained wealth
- outgoing international transactions
- similar or identical sender and beneficiary details
- reluctance or refusal to provide tax or business documents
- transaction values were large or not proportionate with customer's stated personal income
- invoices for services rendered where the value and profile do not match a business or sector
- requests for transaction descriptions to include mislabelled business or tax-related descriptions for perceived future tax advantages.

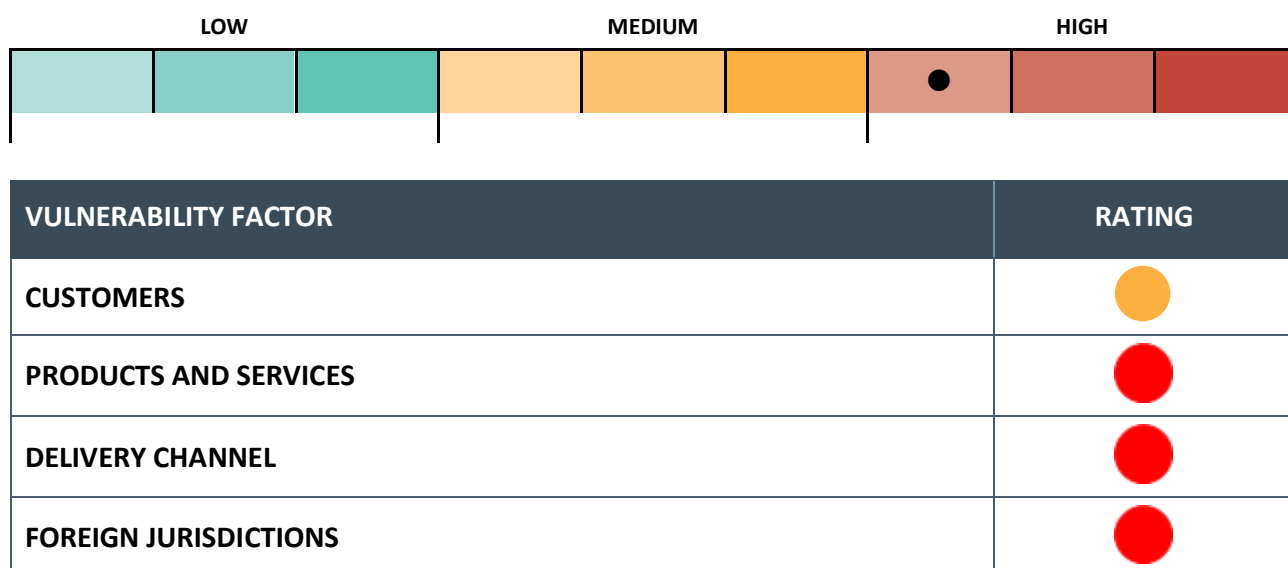
IRDs AND THE SHADOW ECONOMY

The shadow economy covers economic activities that take place outside the tax and regulatory systems. Examples include not reporting or under-reporting income, paying for work cash-in-hand, phoenixing, or bypassing visa restrictions.²⁴

A number of SMRs and intelligence reports involved the use of IRDs to remit funds that were likely generated in Australia's shadow economy. These reports frequently featured temporary visa holders that were suspected of working in breach of their visa conditions. Cash transactions were commonly associated with this type of activity and the subsector's high exposure to cash increases the risk it will be exploited to launder the proceeds of shadow economy (see **Use of cash** on page 40).

²⁴ The Treasury, *Black Economy Taskforce Final Report*, The Treasury, Australian Government, 2017, accessed 9 February 2022.

VULNERABILITIES



AUSTRAC assesses that the IRD subsector is subject to a **high** level of inherent ML/TF vulnerability.

Vulnerability refers to the characteristics of a sector 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 IRD 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 a significant number of higher-risk customers, including known and suspected criminals, overseas-based customers, and companies, trusts or other legal entities.

Size of the customer base

The IRD subsector has a moderately-sized customer base compared to other financial sectors that AUSTRAC regulates, serving an estimated 2.2 million customers.²⁵

There is extreme diversity in the size of reporting entities' customer bases. Major IRDs may serve thousands of customers per day, while small IRDs may serve a handful a month or less.

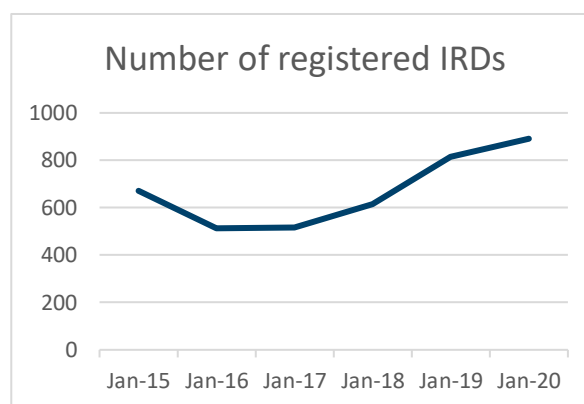
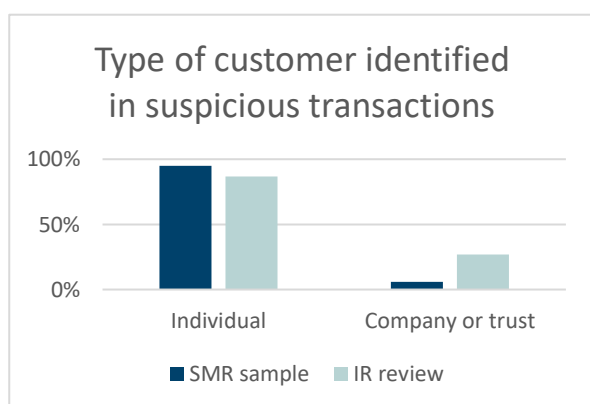
The subsector's customer base is predominantly composed of individuals, with nearly half of reporting entities surveyed indicating they service individual customers only. Many IRDs serve particular ethnic communities for reasons such as family support, funding community projects or charitable donations following natural disasters.

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 IRDs increased by one-third from 2015 to 2020. IRDs consulted for this report indicate the subsector will likely continue expanding over the coming years, although could be hampered by the impacts of COVID-19.

INCREASED REGULATORY OUTREACH

Since 2019, AUSTRAC and partner agencies have increased regulatory outreach to IRDs. This has involved publishing [guidance on how businesses can protect their operations from crime](#), including in [seven languages other than English](#) (see **Risk mitigation strategies**), as well as combatting unregistered remittance activity. This regulatory outreach is likely to have contributed to the increase of registered IRDs since 2019.



²⁵ This number was derived from analysis of IFTIs submitted by IRDs 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 IRD customer numbers due to the closure of international borders, government-imposed lockdowns, and some migrant workers returning to their home countries.

IRDs that relied on face-to-face transacting were most likely to suffer customer losses as a result of the pandemic, while some IRDs offering remittance services online have reported an increase in transactions and revenues.

Over the next five years, industry experts expect customer numbers and transaction volumes to 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.²⁶

Higher-risk customers

AUSTRAC assesses the IRD 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 present across a range of customer categories, including:

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

INDUSTRY CUSTOMER RISK RATINGS

Approximately 75 per cent of IRDs that submitted a compliance report in 2020 advised they do not service high-risk customers. At the subsector level, IRDs reported having a significant number of high-risk customers, which were overwhelmingly concentrated in major IRDs.



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.

²⁶ IBISWorld, *Industry at a Glance – OD5114 Money Transfer Agencies in Australia*, IBISWorld, January 2021, accessed 12 July 2021.

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 IRDs		\$\$		\$\$		\$
LEGEND \$ = 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:²⁷

- 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 2018²⁸
- charged with a terrorism-related offence between 1 January 2014 and 31 December 2018.²⁹

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 \$5.2 million during the reporting period.
- No individuals charged with a terrorism-related offence were customers of the subsector.
- A low proportion of members of serious and organised crime groups were customers of the subsector.
 - While the proportion of individuals on these lists is low, the actual number of individuals is significant, with more than 400 individuals linked to 2,400 transaction reports valued at approximately \$5.5 million. AUSTRAC assesses the actual number of serious and organised criminal entities is almost certainly higher due to under- or non-reporting within the subsector (see **Money laundering** on page 22).

Overseas-based ordering customers

Overseas-based ordering customers can pose higher inherent ML/TF vulnerability to IRDs processing incoming international transactions. AUSTRAC estimates that incoming IFTIs accounted for approximately 24 per cent of the value of IFTIs.³⁰

The most significant vulnerabilities relate to onboarding because Australian IRDs 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 jurisdiction to jurisdiction and many IRDs do not

²⁷ This analysis was completed on all IFTIs, TTRs and SMRs submitted by IRDs 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.

²⁸ 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).

²⁹ 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).

³⁰ 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.

conduct due diligence on their foreign correspondents – particularly where that correspondent is another remittance service provider.

In addition, offshore-based customers may expose IRDs 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 based in 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 and well-supervised 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 – can also pose higher risks to reporting entities.



Companies, trust and legal entities customers are non-natural persons. They can be public companies, incorporated or unincorporated partnerships, incorporated or unincorporated associations or entities using trust structures. There are many legitimate reasons for a corporate customer to send and receive funds internationally using an IRD. For example, transfers between linked entities of a multinational company or to pay suppliers. In some instances, corporate customers may prefer to use IRDs to process these transactions due to lower pricing and convenience.

Two-thirds of the IRDs that responded to the compliance report said they provide services to companies, trusts and other legal entities. A small number of reporting entities consulted for this report indicated companies were their primary customer type and ranged in size from small businesses to larger commercial institutions. In addition, industry representatives indicate IRDs are more willing to service corporate customers than RNPs and their affiliates.

Customers that were companies, trusts or other legal entities were identified in six per cent of the SMR sample and 26 per cent of the IR review.³¹ Common themes observed in these reports include:

- false invoice scams using corporate customers
- lack of supporting documents to substantiate overseas business activity
- corporate customers making purchases with no discernible relevance to their business

³¹ 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**).

- complex or rapid transactions through corporate customer accounts potentially indicating a fraud or scam.

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



AUSTRAC expects IRDs 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.³² 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.

Overall, PEPs pose a low ML/TF risk to the subsector. A very low number of PEP customers were identified in the SMR sample (0.3 per cent) and IR review (0.7 per cent). Just nine per cent of IRDs that submitted a compliance report in 2020 said they had PEP customers, with the subsector reporting approximately 1,700 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 a 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.

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

PRODUCTS AND SERVICES

AUSTRAC assesses the nature and extent of the products and services offered by the IRD 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 JANUARY 2019 AND 31 JANUARY 2019

Total number of TTRs submitted to AUSTRAC: **58,913**

Sum of TTRs: **\$3.8 billion**

Total SMRs submitted featuring cash: **78 per cent**

Sum of SMRs featuring cash: **\$106 million**

The number of SMRs containing a suspicious cash transaction declined from 93 per cent in 2015 to 78 per cent in 2019.

While overall cash use in Australia is declining, the IRD 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
- de-banked IRDs may be increasingly reliant on cash transactions to continue operating (see **Offsetting** on page 47)
- 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 has been identified in the subsector (see **Criminal threat environment** on page 23). 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 32).

Although cash exposure remains high among the subsector generally, some industry representatives and reporting entities consulted for this report indicated an increasing aversion to cash transactions. Over half (52 per cent) of respondents in the IRD survey say they no longer accept cash. Instead, many IRDs prefer to use other delivery channels such electronic funds transfer into their bank account, credit card payments or third-party biller payments (see **Level of customer contact** on page 44).

Almost all respondents to the IRD survey noted cash as a key indicator of ML/TF risk. Suspicious cash transactions were observed in 42 per cent of the SMR sample. Key themes observed include:

- cash payments from undeclared wealth
- cash deposits followed by rapid movement of funds

- multiple low-value transaction without commercial or business explanation (i.e. structuring).



During industry consultations one IRD said they prefer electronic funds transfers into their bank account because their bank's CDD procedures supplement their own risk mitigation strategies.

IRDs that ask customers to deposit funds directly into their bank account to reduce their cash exposure should ensure their banks understand the reason for these third-party deposits.

IRDs that continue accepting cash can mitigate ML/TF risks by:

- requesting evidence of the source of funds
- limiting the amount customers can send to higher-risk jurisdictions
- limiting the amount a customer can remit in one day or one transaction
- applying ECDD processes for large cash transactions to identify the beneficiary and purpose of the transaction.

Ability to store and move funds

By their nature, the products and services IRDs offer 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, IRD products and services are not generally designed to store funds and customers are unlikely to use the subsector for this purpose.³³

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 4). A small number of reporting entities offer other services. These services are not discussed in detail in this report because their scale across the subsector is limited. Refer to AUSTRAC's ML/TF risk assessment on stored value cards and bullion dealers for information on the ML/TF risks and vulnerabilities of these services.

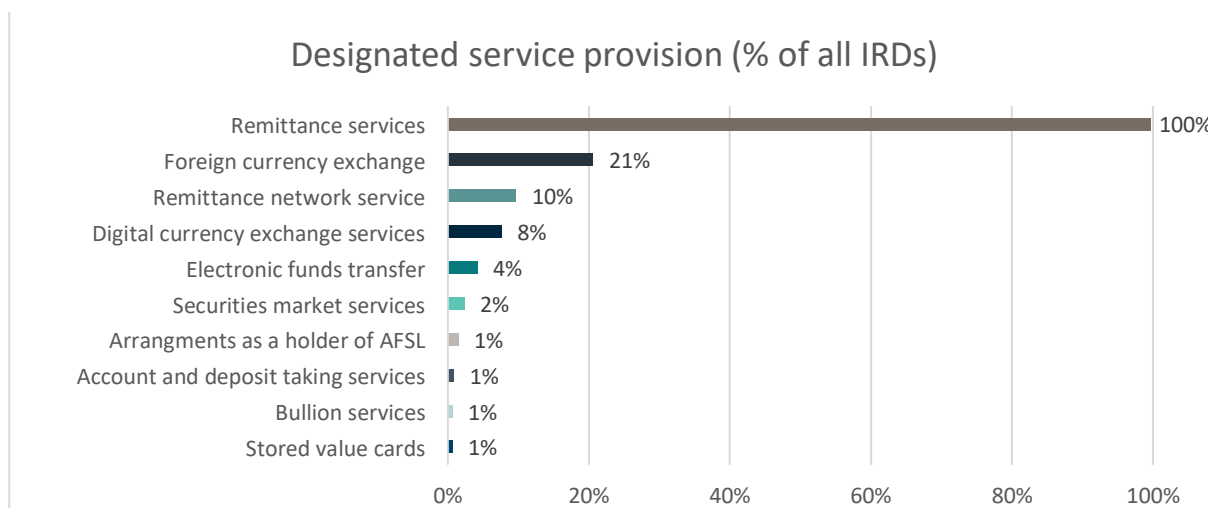
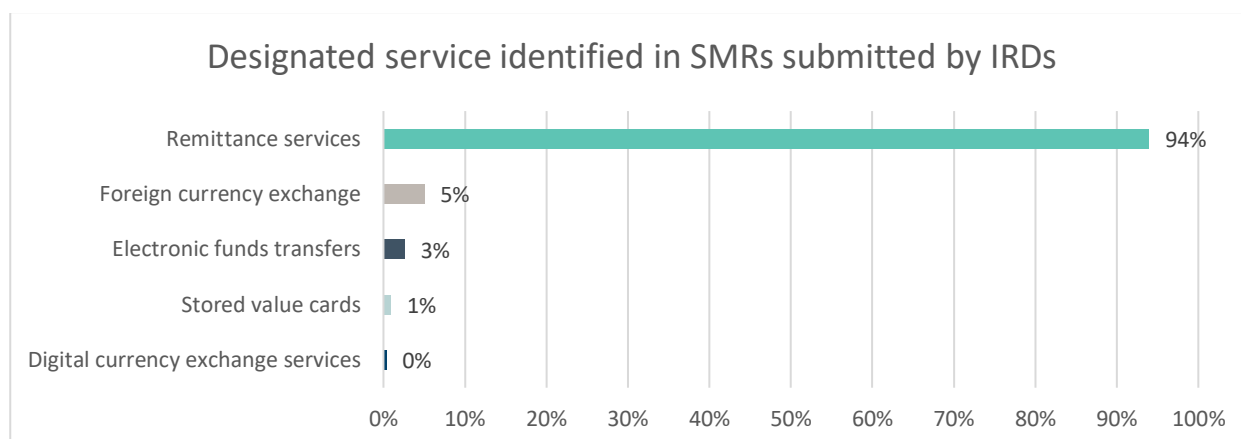


Figure 4: Proportion of IRDs registered with AUSTRAC to provide each designated service

³³ 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 IRDs during the reporting period generally reflect the concentration of products and services offered. During the reporting period, 94 per cent of SMRs identified suspicious activity involving remittance services, while five per cent identified foreign currency exchange.



Remittance services

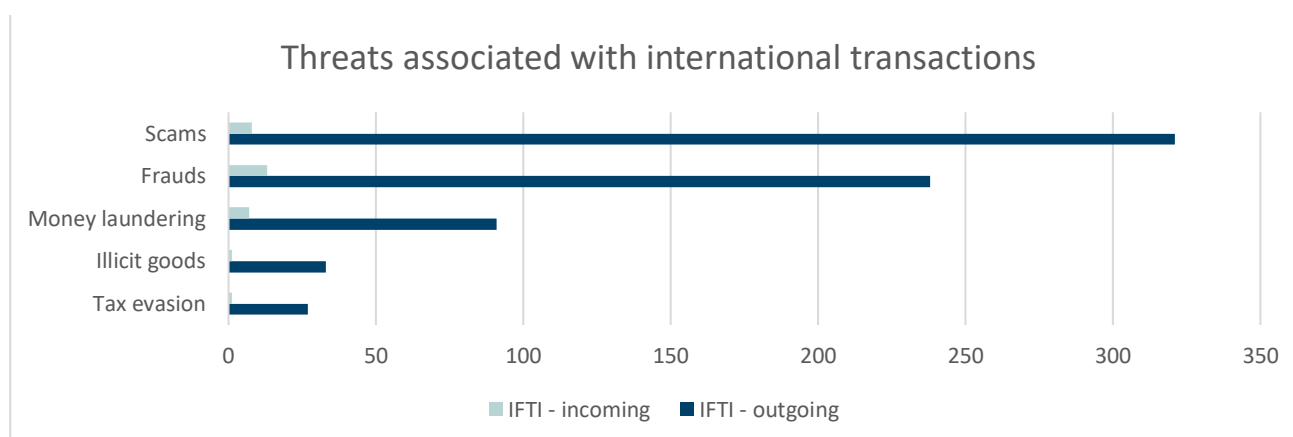
Remittance services enable fast and effective movement of funds domestically and internationally, exposing the subsector to significant foreign jurisdiction risk (**Foreign jurisdiction risk** is discussed on page 48). Approximately three-quarters of reporting entities that responded to the IRD survey said remittance is the only product or service they offer.

During the reporting period, IRDs submitted nearly 18.8 million IFTIs with a total value of approximately \$72.6 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 than 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 81 per cent of the SMR sample, with outgoing remittances making up 96 per cent remittance-related SMRs. The average value of outgoing remittance SMRs was moderate-to-high, at \$19,000. The most common threats associated with international transactions in the SMR sample were scams, frauds and money laundering.



Foreign currency exchange

Foreign currency exchange services are vulnerable to ML/TF misuse 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 10 per cent of the SMR sample. Most reports related to suspected money laundering or fraud activity with a moderate-to high average value of \$28,000.

The number of foreign currency exchange transactions over \$10,000 has declined by 87 per cent between 2019 and 2020, almost certainly as a result of COVID-19 restrictions.³⁴ 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.

³⁴ The number of TTRs submitted by IRDs where 'currency exchange services' was identified as the designated service fell by 87 per cent during the June and December 2020 period compared to the same time in 2019.

DELIVERY CHANNELS

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

Across the subsector, face-to-face customer contact is declining as business decisions and customer preferences shift to remote service delivery channels, particularly online.

IRDs are also exposed to ML/TF vulnerability related to outsourced product delivery arrangements, as well as the practice of offsetting.

Level of customer contact

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

While many reporting entities maintain a physical shopfront, an increasing number operate wholly online. The COVID-19 pandemic has also accelerated this shift. The trend towards more remote product delivery channels makes it easier to impersonate a customer or transact anonymously, increasing ML/TF vulnerability. Criminals exploit these features to distance themselves from illicit activity.

IMPACT OF COVID-19 ON CUSTOMER CONTACT

The onset of COVID-19 and resulting government restrictions have had a significant and ongoing impact on IRDs, and forced many to rely on remote delivery channels such as online and over the phone.

Unlike bank branches, many IRDs have not been able to open their physical shopfronts during lockdown restrictions. As such, reporting entities consulted for this risk assessment reported a substantial drop in face-to-face customers across Australia – even when lockdowns are lifted, some reporting entities report lower customer numbers visiting their physical shopfront.

On the other hand, IRDs that offered products or services mostly or wholly via remote delivery channels, such as websites and apps, reported fewer COVID-19-related disruptions. One online-only IRD reported revenues had increased by more than a third since the onset of the pandemic. Submissions to AUSTRAC's compliance report also indicate an increase in IRDs introducing remote delivery channels in 2020.

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 IRDs continue to offer face-to-face transactions. More than two-thirds indicating they offered in-person transactions in 2020, and 12 per cent indicated they only offered in-person transactions.

Face-to-face transactions generally provide reporting entities with more opportunities to identify suspicious behaviour and respond to it 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

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

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



During consultations, a number of IRDs stated they are uncomfortable asking for customer identification information. Industry representatives expressed concern that doing so makes them less competitive because customers prefer businesses that ask fewer questions.

Some IRDs also said that the CDD process may be perceived as intrusive or even offensive, particularly when dealing with returning customers. Some reporting entities emphasised the importance of trust and familiarity within culturally distinct communities, and fear that CDD-related questioning will be viewed as a betrayal of that trust.

All IRDs must remain vigilant in implementing robust CDD procedures. To alleviate customer concerns about being asked probing CDD questions, businesses can display information that CDD procedures are a legal requirement that all businesses must comply with.

Online channels

A significant volume of remittance transactions facilitated by IRDs originate online – either through websites or mobile applications. Just over half of IRDs that submitted a compliance report in 2020 said they offered their services online, while approximately one-third of respondents to the IRD survey said they operate wholly online. Consumer demand for speed, convenience and lower costs for reporting entities have driven the shift towards online services.

The increasingly online nature of remittance transactions introduces inherent ML/TF vulnerabilities. The speed with which transactions can be executed is attractive for criminals trying to layer illicit funds. With one device, a money launderer can direct funds through multiple accounts with different IRDs, masking the true source or destination of the funds.

With no face-to-face interaction or CCTV monitoring, online channels also introduce an additional element of anonymity that is attractive to criminals. For example, criminals can exploit online applications for remittance accounts to establish mule accounts using stolen identities, which are then used to launder the proceeds of frauds, scams and other predicate offences.



Partner agencies have told AUSTRAC that tech-savvy criminals often spend hours testing new versions of mobile apps to discover and exploit features to perpetrate crimes faster and with greater anonymity.

Reporting entities should carefully consider the financial crime implications when introducing new mobile app features because criminals can exploit even minor changes.

Complexity of product delivery arrangements

Some IRDs outsource their product delivery arrangements to third-parties. Outsourcing can expose IRDs to ML/TF risk because it lengthens the product delivery chain and reduces the level of oversight an IRD might have over customers and transactions.

Likewise, some IRDs 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.

ML/TF vulnerabilities increase when multiple third-party providers are used, where remittance transactions become overly complex, or where IRDs become too reliant on the due diligence and risk mitigation strategies of third-party providers.

Outsourcing

IRDs often rely on overseas correspondent institutions or third-party service providers to fulfil transactions involving foreign jurisdictions without the need to operate in these jurisdictions. Outsourced product delivery arrangements can expose IRDs to increased inherent ML/TF vulnerability. This is because outsourcing lengthens and complicates the product delivery chain, making it harder for IRDs to detect and act on suspicious activity. Poor governance practices can further exacerbate these vulnerabilities.

In particular, smaller IRDs may partner with third-party currency exchanges or digital wallet providers to facilitate remittance quickly and at a competitive rate. Major IRDs may have less need for third-party providers if they have a physical presence in overseas jurisdictions. Instead, these major IRDs tend to leverage their own international network, increasing their visibility of the product delivery chain and therefore reducing ML/TF vulnerabilities.

IRDs use a range of methods to accept payment or deliver funds to customers, including:

- bank-to-bank transfers
- cash delivery in the destination jurisdiction
- third-party payment processors to accept card or online payments
- use of third-party payment platforms for popular currency exchanges
- cash pick-up from a correspondent bank branch in the destination jurisdiction
- third-party payment platforms to effect international transactions, particularly among underbanked populations (e.g. mobile payment system)



IRDs 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 IRD's transaction volumes, operating jurisdictions and existing risk mitigation strategies.

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.

Since 2014, many IRDs have been subject to de-banking which can include outright account closures or an implication that such action will be taken in the future. This has generated operational uncertainty among some IRDs, while others have been forced out of business. Industry engagement revealed that de-banking is more likely to affect smaller IRDs than major IRDs.

De-banking is likely to increase the subsector's reliance on third-party service providers to process payments, which allows IRDs 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 IRDs 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 IRDs to continue operating when they have been de-banked. As discussed below, offsetting exposes the subsector to ML/TF vulnerabilities.

Offsetting

Offsetting is a method of exchanging value internationally that relies on business-to-business relationships instead of established banking arrangements.³⁵ In its simplest form, a customer will ask an Australia-based IRD to send money to a jurisdiction where the IRD has a correspondent operator. The Australia-based IRD will then inform the overseas correspondent of the transaction, which will then release funds to the nominated beneficiary abroad. The Australia-based IRD and its overseas counterpart will settle their balance of payments at a later date.³⁶

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.

According to the IRD survey, approximately 12 per cent of IRDs use offsetting arrangements. For some IRDs, 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 IRDs may use offsetting if they have been de-banked. Large multinational IRDs 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, therefore exposing the subsector to ML/TF risk. 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 IRD has poor or limited record-keeping practices.

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

³⁵ Other common names for offsetting include hawala, hundi, chit and fei chi'en.

³⁶ 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.



IRDs must still submit relevant reports to AUSTRAC when using offsetting arrangements. AUSTRAC emphasises the need for IRDs to know and understand their AML/CTF reporting obligations when using offsetting arrangements.

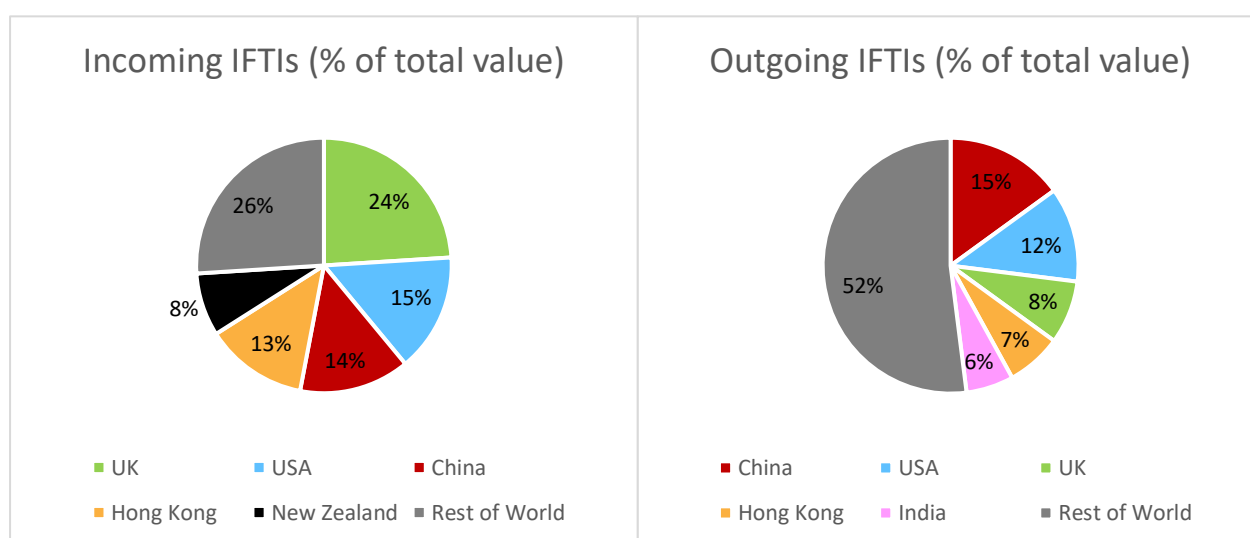
FOREIGN JURISDICTIONS

AUSTRAC assesses IRDs have a **high** inherent ML/TF vulnerability to foreign jurisdictions.

The IRD 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 the 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 internationally³⁷



In the reporting period, IRDs submitted almost 18.8 million IFTIs with a recorded value of \$72.6 billion. Major IRDs accounted for more than three-quarters of the total recorded value of IFTIs submitted, suggesting foreign jurisdiction risk is largely concentrated in these reporting entities.

Outgoing transactions accounted for almost two-thirds of the value of IFTIs.³⁸ The average value of incoming IFTIs was approximately three times greater than outgoing. This is likely a reflection of the purpose of the transfer. 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.

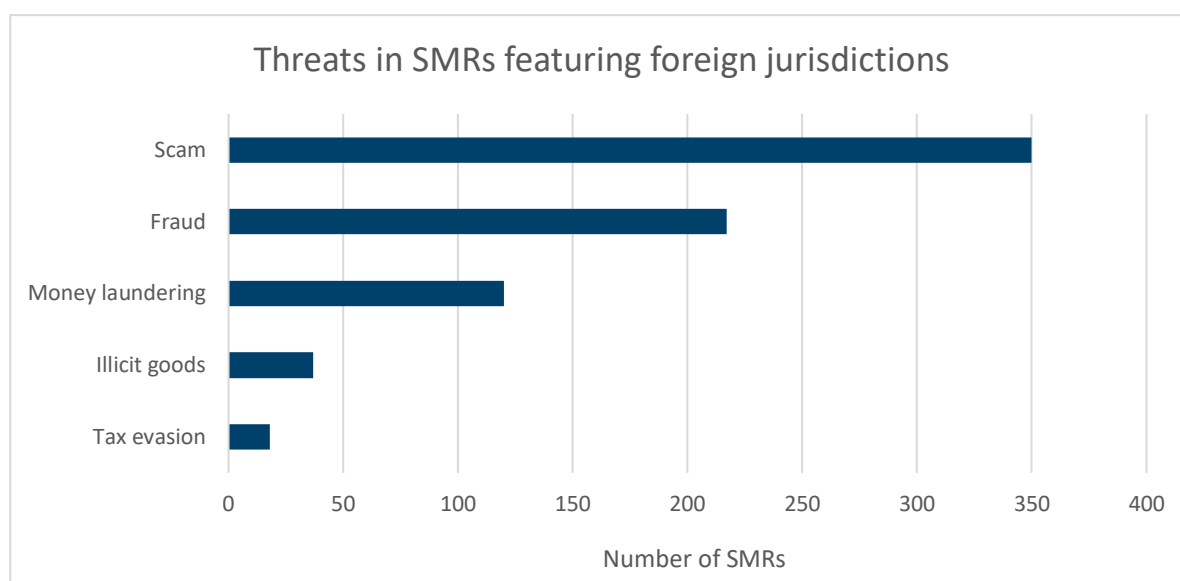
International transactions were identified in 81 per cent of the SMR sample. The top five jurisdictions identified in the SMR sample were the Philippines, Nigeria, USA, China and the UK. Three of these jurisdictions (USA, China and the UK) rank in the top five source or destination jurisdictions for IFTIs

³⁷ 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.

³⁸ Industry IFTI submissions include data quality issues surrounding incomplete or inaccurate inputs. Caution should be applied when interpreting IFTI source and destination countries.

submitted by IRDs. This suggests suspicious activity from the Philippines and Nigeria is over-represented relative to the value of transactions with these jurisdictions.

Scams, frauds and money laundering were the primary threats in SMRs involving foreign jurisdictions.



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

Transactions with higher-risk jurisdictions

The IRD subsector frequently transacts with higher-risk jurisdictions. 67 per cent of all IFTIs by value involved transactions with higher-risk jurisdictions.³⁹ This includes a moderate volume and value of funds flowing to or from global financial centres.⁴⁰ Approximately two-thirds of transactions with higher-risk jurisdictions were outgoing (67 per cent).⁴¹



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.

³⁹ 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.

⁴⁰ 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

⁴¹ 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.

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 JURISDICTIONS⁴²

Incoming value

Outgoing value



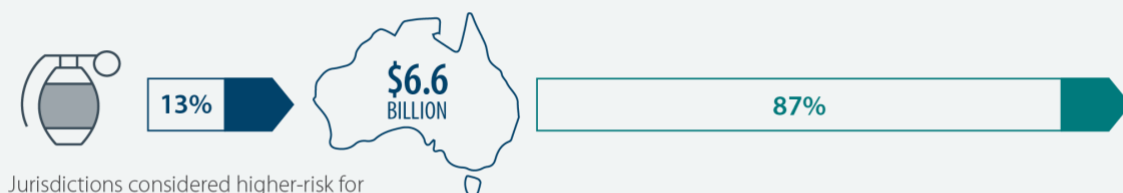
Jurisdictions considered higher-risk for money laundering (including global financial centres)



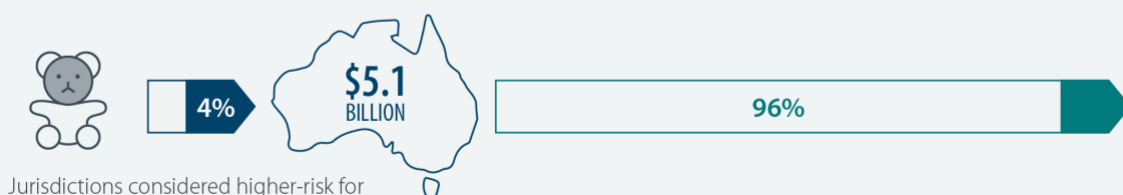
Jurisdictions considered higher-risk for money laundering (less global financial centres)



Jurisdictions considered higher-risk for tax evasion



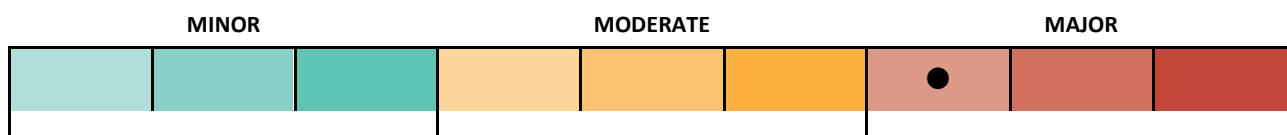
Jurisdictions considered higher-risk for terrorism financing



Jurisdictions considered higher-risk for child exploitation

⁴² 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 IRD subsector are **major**.

Consequences include the potential impact or harm that ML/TF and other financial crimes may cause.

Financial crime that impacts IRDs has consequences for customers, individual reporting entities, the subsector as a whole, and the broader Australian and international community. Where IRDs are 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 IRDs have **moderate** consequences for customers of the subsector.

IRDs report varying 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 an IRD. 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 IRDs are 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 IRDs 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 IRDs have **major** consequences for individual reporting entities and the subsector as a whole.

Criminal activity has had a significant impact on the operations of a number of IRDs and continues to pose financial, operational and reputational risks to the subsector. The perceived or actual threat of criminal activity is linked to the de-banking of IRDs, which in turn constrains the operations of some reporting entities and may force others out of business. This consequence is particularly pronounced for small IRDs, which are more vulnerable to de-banking because they may be perceived to have less sophisticated risk mitigation strategies.

Certain IRDs may also be targeted by criminals if they are identified as having poor AML/CTF controls.

The impact of criminal activity on IRDs can include:

- loss of revenue and increased insurance premiums
- more stringent regulatory oversight, creating additional costs for businesses
- enforcement or legal action and associated civil or criminal penalties in the event of serious non-compliance
- difficulty continuing or establishing relationships with domestic and overseas financial institutions
- 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

- an increase in unregistered remittance activities due to de-banking, which compounds reputational damage to the subsector and could provide an unfair advantage to unregistered businesses that do not invest in risk mitigation strategies.

AUSTRALIAN FINANCIAL SYSTEM AND THE COMMUNITY

AUSTRAC assesses that ML/TF and predicate offences involving IRDs 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 IRD subsector, as well as the concentration of activity in a small number of products and services.

The speed and capacity the subsector possesses to move funds offshore 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 offences such as 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
- 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 enterprise⁴³
- a loss of confidence in IRDs as a legitimate method of sending funds internationally. This could reduce competition in the remittance sector and result in increased remittance costs.

NATIONAL AND INTERNATIONAL SECURITY

AUSTRAC assesses that ML/TF and predicate offences involving IRDs have **major** consequences for national and international security.

Serious and organised crime groups are likely to have a presence in the subsector, including likely links to a small number of IRDs. The ability for these groups to launder their illicit funds can contribute to their growth. Serious and organised crime 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. drug 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.

⁴³ 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 between IRDs, presenting ongoing and potentially significant risks to the subsector. Some IRDs appear to have relatively comprehensive risk mitigation strategies in place, including systematic approaches to transaction monitoring programs, annual internal audits, introductory and ongoing training of staff, appointing AML/CTF specialists to inform their policies and practices, and the use of risk matrices to assess foreign jurisdiction risk.

However, other IRDs have unsophisticated approaches to customer due diligence, do not deliver sufficient staff training, or generally lack an understanding of their AML/CTF obligations. Criminals are known to target reporting entities who they suspect employ weak customer identification, CDD or other procedures.

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. Additionally, some IRDs operate other businesses, with remittance services comprising only a small component of their operations. For these businesses, ML/TF risk mitigation may not be considered a significant priority.

Across the subsector, improvements could be made to ensure:

- customer risk is appropriately assessed and regularly reviewed
- enhanced customer due diligence processes are understood and consistently applied
- enterprise ML/TF risk assessments are comprehensive

- regular independent reviews of risk management frameworks occur
- adequate employee due diligence and training is undertaken.

Improvements to the quality and quantity of SMR submissions can also be made across the subsector (see page 60).



GUIDANCE RESOURCES FOR IRDs

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

Corporate customers

IRDs who primarily service corporate customers acknowledge the risks associated with complex corporate structures and the challenges in identifying beneficial ownership. In the IRD survey, these reporting entities also indicated they feel better equipped to service individual customers because the associated due diligence requirements are generally simpler.

Conversely, industry feedback suggests many IRDs that primarily service individual customers doubt they have adequately assessed the risks of corporate customers – including beneficial ownership – and have indicated their practices and procedures would need to be significantly enhanced to be able to do so.



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

Approximately two-thirds of IRDs who responded to AUSTRAC's compliance report indicated that they conducted PEP checks in 2020. Some IRDs report using a combination of official watch lists, commercial third-party databases and open source searches for PEP and sanctions screening.

However, industry feedback reveals that many reporting entities rely on a single database to conduct PEP and sanctions screening. IRDs using 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](#).

Enhanced customer due diligence

A number of IRDs indicated circumstances that would trigger ECDD activities, such as questioning the source of funds. These include:

- suspicious customer behaviour
- high-value remittance transaction requests
- transfer requests to certain higher-risk jurisdictions
- transaction patterns (and/or the use of cash) which deviate from an established customer's usual remittance profile.

Some IRDs said they felt they knew their customers sufficiently well, often through family or community ties, and were reluctant to directly question their customers for additional information, even when warranted.

Additionally, while IRDs generally recognise that establishing a customer's source of funds may form a part of their ECDD processes, industry feedback suggests some entities may not understand the difference between 'source of funds' and 'source of wealth', which may compromise their ability to fully understand their customer profiles and associated ML/TF risks.

It is important reporting entities understand that a customer's source of wealth refers to how the customer would be expected to have accumulated and how the customer acquired their overall wealth and financial position. A customer's source of funds refers to the origin of the particular funds or other assets involved in one or more specific transactions.



AUSTRAC reminds IRDs of the importance of clear and consistent enhanced customer due diligence processes and that a compliant AML/CTF program includes an ECDD program which documents the actions IRDs take in high-risk situations. It is also critical IRDs have transaction monitoring programs in place to help their businesses:

- identify, mitigate and manage ML/TF risks
- identify and report suspicious matters to AUSTRAC
- meet their ongoing customer due diligence and ECDD obligations.

IRDs can locate further information about their [ECDD obligations](#), [source of wealth/source of funds considerations](#) and [transaction monitoring programs](#) on the AUSTRAC website.

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 IRDs use.

Most IRDs that AUSTRAC consulted indicated they impose limits on the total value and/or number of remittance transactions per customer during a given time period, which varied depending on the risk associated with the jurisdiction involved. Some IRDs also limit the number of currencies a customer may remit in or restrict transactions to multiple countries within a given time period. 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 jurisdiction.

Other IRDs described a more simplistic approach, by capping the daily total value of remittances at a nominated figure. Value-based transaction limits varied greatly: one IRD advised AUSTRAC it capped its daily remittance value at \$1 million per customer, whereas other businesses – often servicing a single jurisdiction – said they had a \$5,000 cap in place.

Twenty-three per cent of IRDs surveyed for this assessment said they did not impose transaction limits on customers. Several businesses said this was because they only serviced a single jurisdiction or knew their customers well enough to mitigate ML/TF risk.



Strategies to slow and simplify the movement of funds offshore, such as transaction limits, can help minimise the subsector's exposure to ML/TF risks. AUSTRAC encourages IRDs to consider how transaction limits may reduce their business's ML/TF exposure and to review these limits on a regular basis.

RISK ASSESSMENTS

Industry feedback suggests a varied understanding and approach to risk assessment processes. Some IRDs indicated they did not fully or adequately understand and assess the ML/TF risks associated with one or more of the four key elements of an enterprise risk assessment – customers, designated services, delivery channels, and the foreign jurisdictions they do business with.



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 IRDs 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

IRDs 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 the 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. There are detected instances where organised crime groups targeted IRD employees to facilitate money laundering (see **Money laundering** on page 22).

Approximately three-quarters of IRDs surveyed for this assessment indicated they conduct regular ongoing or new-starter training programs. Several IRDs also outlined initial and ongoing staff due diligence procedures such as police and reference checks, PEP and sanctions screening, and open source or social media searches. However, some IRDs indicated they had limited time or resources to undertake employee due diligence checks.

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 IRDs to facilitate money laundering and the movement of funds internationally.



Appropriate initial and ongoing employee training is critical for all reporting entities. 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 also an important ML/TF risk mitigation strategy.

AUSTRAC expects IRDs 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 the IRD subsector submit few, if any, SMRs to AUSTRAC. In many instances, this is likely due to an IRD being inactive. Low or no reporting may also be attributable to differences between reporting entities’ scale of operations, their customer base and/or remittance transactions with lower-risk foreign jurisdictions. However, low SMR reporting can also reflect varying levels of:

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

AUSTRAC also believes that 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.

Reporting entities should have policies and procedures in place 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
- SMR reference guide with real-life examples
- SMR checklist containing key elements and details required

APPENDIX A: GLOSSARY

Affiliate	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.
AML/CTF	Anti-money laundering and counter-terrorism financing.
AML/CTF program	A document that sets out how a reporting entity meets its AML/CTF compliance obligations.
Beneficial owner	An individual who owns 25 per cent or more of, or otherwise controls the business of an entity.
Customer due diligence (CDD)	Customer due diligence (CDD) is the process where pertinent information of a customer's profile is collected and evaluated for potential ML/TF risks.
Designated business group	A designated business group (DBG) is a group of two or more reporting entities who join together to share the administration of some or all of their anti-money laundering and counter-terrorism financing obligations.
Designated non-financial businesses and professions (DNFBP)	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.
Enhanced customer due diligence (ECDD)	Enhanced customer due diligence (ECDD) is the process of undertaking additional customer identification and verification measures in certain circumstances deemed to be high risk.
Financial Action Task Force (FATF)	The Financial Action Task Force 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.
Global financial centres	For the purposes of this report, global financial centres refer to the jurisdictions that are home to the top four cities in the Global Financial Centres Index 26
Independent remittance dealer (IRD)	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.
International financial transaction instruction – designated remittance agreement (IFTI-DRA)	<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"> the entity accepting the instruction from the customer or the entity making the money or property available <p>is not a financial institution.</p>
Inherent risk	Inherent risk represents the amount of risk that exists without the reporting entity implementing AML/CTF controls
Integration	The final stage of the money laundering cycle, in which illicit funds or assets are invested in further criminal activity, 'legitimate' business or used to purchase assets or goods. At this stage, the funds are in the mainstream financial system and appear to be legitimate.
Know your customer (KYC)	'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.

Layering	The second stage of the money laundering cycle, which involves moving, dispersing or disguising illegal funds or assets to conceal their true origin.
Major IRDs	For the purposes of this report 'major IRDs' are defined as reporting entities with an IRD registration that submitted more than \$500 million worth of IFTIs in 2019.
ML/TF	Money laundering and terrorism financing.
Mules	Third parties used to transfer illicit funds between locations or accounts.
Ongoing customer due diligence (OCDD)	Ongoing customer due diligence relates to the systems and controls in place to decide whether additional customer and beneficial owner information should be collected and verified on an ongoing basis. It includes ensuring customer information is up to date, and processes for transaction monitoring and enhanced customer due diligence (ECDD).
Permanent establishment	<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"> • have physical offices or business premises in that country • carry on your business in that country (even without a physical office).
Politically exposed person (PEP)	<p>A politically exposed person (PEP) is an individual who holds a prominent public position or role in a government body or international organisation, either in Australia or overseas. Immediate family members and/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"> • Domestic PEP – someone who holds a prominent public position or role in an Australian government body. • Foreign PEP – someone who holds a prominent public position or role with a government body in a country other than Australia. • International organisation PEP – someone who holds a prominent public position or role in an international organisation, such as the United Nations (UN), the World Trade Organisation (WTO) or the North Atlantic Treaty Organisation (NATO).
Placement	The first stage of the money laundering cycle, in which illicit funds first enter the formal financial system.
Predicate offence	For the purpose of this risk assessment, a predicate offence is any offence which generates proceeds of crime.
Refining	The process of exchanging lower denomination bills into higher denominations. Can occur using foreign exchange which provides further distance from funds' origin.
Remittance service	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.
Remittance network provider (RNP)	A remittance business structure that allows a network of affiliates to use its brand, products, platforms or systems to provide remittance services to customers.

Remittance service provider (RSP)	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.
Residual risk	Residual risk is the amount of risk that remains after a reporting entity's AML/CTF controls are accounted for.
Structuring	Where a person deliberately: <ul style="list-style-type: none"> • splits cash transactions to avoid a single large transaction being reported in threshold transaction reports • travels with cash amounts in a way that avoids declaring cross border movements of the cash
Source of funds	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.
Source of wealth	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.
Trigger-based reporting	Where a reporting entity submits a suspicious matter report to AUSTRAC solely on the basis of a trigger generated by their transaction monitoring system without conducting further investigation.
Suspicious matter report (SMR)	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.
Transaction monitoring program	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.
Third party service providers	Services that businesses often use to facilitate the final payment to a beneficiary.
Threshold transaction report (TTR)	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.
Unregistered remittance dealers	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

