



Australian Government
AUSTRAC

FIGHTING
FINANCIAL
CRIME
TOGETHER



AUSTRALIA'S NON-BANK LENDING AND FINANCING SECTOR

MONEY LAUNDERING AND TERRORISM FINANCING RISK ASSESSMENT

COPYRIGHT

© Commonwealth of Australia 2021

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

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

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



USE OF THE COMMONWEALTH COAT OF ARMS

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

This risk assessment is intended to provide a summary and general overview; it does not assess every risk or product relevant to the non-bank lending and financing sector. 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 license and any use of this report please email contact@austrac.gov.au or phone 1300 021 037 (within Australia).

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

CONTENTS

EXECUTIVE SUMMARY	03
PURPOSE	08
BACKGROUND	09
METHODOLOGY	11
CRIMINAL THREAT ENVIRONMENT	12
Money Laundering	15
Terrorism Financing	17
Predicate Offences	18
VULNERABILITIES	24
Customers	25
Products and services	30
Delivery channels	35
Foreign jurisdictions	37
Implementation of risk mitigation strategies	39
CONSEQUENCES	41
APPENDICES	43



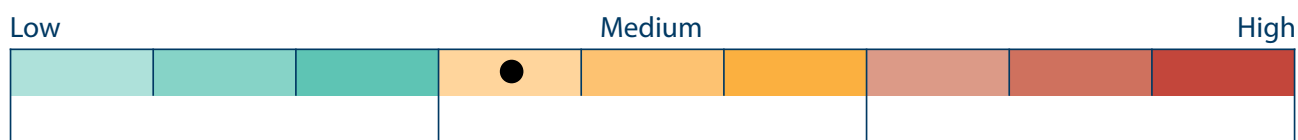
EXECUTIVE SUMMARY

For the purposes of this report, a non-bank lender and financier is a business that offers individuals and businesses loans, mortgages, personal finance, credit cards and other types of finance, but does not hold a banking license. They do not feature on the Australian Prudential Regulation Authority (APRA) list of authorised deposit-taking institutions as they do not accept deposits.

There are over 600 non-bank lenders and financiers in the Australian market, providing a range of services. The sector accounts for approximately seven per cent of debt financing in Australia.¹

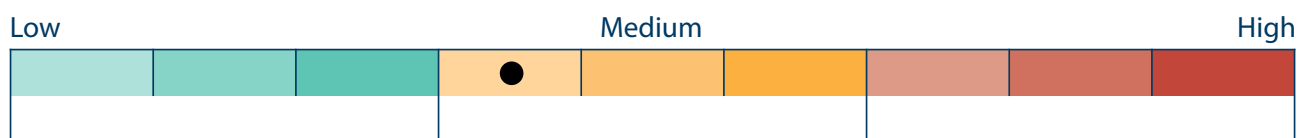
¹ Reserve Bank of Australia, Financial Stability Review, April 2019, [rba.gov.au/publications/fsr/2019/apr/pdf/financial-stability-review-2019-04.pdf](https://www.rba.gov.au/publications/fsr/2019/apr/pdf/financial-stability-review-2019-04.pdf), page 51.

OVERALL RISK RATING



AUSTRAC assesses the overall money laundering and terrorism financing (ML/TF) risk associated with the non-bank lending and financing sector to be **medium**. This rating is based on assessments of the criminal threat environment, the vulnerabilities present in the sector and the consequences associated with the criminal threat environment.

CRIMINAL THREAT ENVIRONMENT



AUSTRAC assesses the overall ML/TF threat associated with the non-bank lending and financing sector's criminal threat environment to be **medium**.

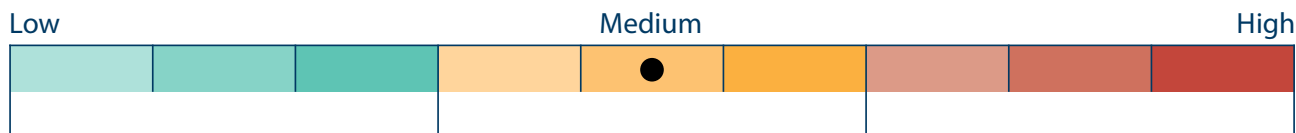
The key threat faced by the non-bank lending and financing sector is fraud, particularly loan application fraud, identity fraud and welfare fraud.² Loan application fraud was often associated with identity fraud, because the person seeking to secure funding used someone else's identity to avoid having to make repayments, or presented false or misleading information about themselves to increase their chances of obtaining finance. Welfare fraud was identified when information provided on a loan application was found to be inconsistent with a Centrelink income statement, when transactions were found to be inconsistent with the expected profile of a customer receiving Centrelink benefits or when Centrelink recipients were in receipt of employment income that was likely not being declared. Lower levels of other predicate offences, such as personal and corporate tax evasion, were also identified.

Suspicious matter reports (SMRs) indicate the second greatest threat faced by the non-bank lending and financing sector is money laundering and relates predominantly to unexpected early loan payouts using criminal proceeds. This methodology allows criminals to convert the proceeds of crime into high-value assets such as real estate and luxury vehicles. The non-bank lending and financing sector also suspected that, in some instances, companies were using criminal proceeds to repay their loans, essentially buying the asset with illicit funds. AUSTRAC also reviewed a number of SMRs lodged by other entities which contained reference to the non-bank lending and financing sector. These SMRs included transactions to and from higher-risk jurisdictions, large cash transactions and the use of cardless ATM cash deposits.

AUSTRAC assesses the terrorism financing threat associated with the non-bank lending and financing sector to be **low**. Two SMRs in the dataset and one intelligence report linked possible terrorist themes to the non-bank lending and financing sector where suspicions were based on the attributes of the customer and not their transactions with the sector. Overall, while some individuals with a higher terrorism risk may use the non-bank lending and financing sector, there is insufficient information to indicate they use the services of the sector to actually facilitate terrorism.

² Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, volume 3 - appendices, final report volume 3, royalcommission.gov.au/royal-commission-misconduct-banking-superannuation-and-financial-services-industry.

VULNERABILITIES



AUSTRAC assesses the level of ML/TF vulnerability in the non-bank lending and financing sector to be **medium**. There are a number of factors that render the sector vulnerable to criminal misuse.

Loans are well-established vehicles for money laundering, particularly when the loan is used to purchase high-value assets in which the proceeds of crime can be invested through loan repayments. The regulation of the sector from a consumer-protection perspective has resulted in entities implementing due diligence procedures that many non-bank lenders and financiers have effectively leveraged to mitigate the risks associated with money laundering through loan repayments.

The non-bank lending and financing sector reported a very low tolerance for the ML/TF risks of cash transactions and reports few threshold transaction reports (TTR) overall. However, a number of non-bank lenders and financiers provide a direct capability for their customers to transact in cash through third-party branches or agents such as nominated banks or post offices.

Cash deposits facilitated through third-party branches or agents are associated with diminished oversight by non-bank lenders and financiers over transactions and customers, inhibiting their ability to detect suspicious patterns of activity, particularly when the transaction falls below the threshold transaction reporting amount. In fact, given the high number of SMRs reporting structured cash loan repayments to avoid threshold reporting obligations, analysis of TTR reporting is likely to significantly understate the cash-based vulnerability the sector's products present to the financial system as a whole.

The primary customer-type for the non-bank lending and financing sector is individuals. They generally have a lower ML/TF risk profile than non-individuals because identities and transactions cannot be obscured behind complex business/company structures. However, the non-bank lending and financing sector also has a relatively low rate of direct customer interaction, placing significant reliance on brokers and other external loan originators, which can seriously undermine the benefits of a transparent customer-type. Brokers and aggregators lengthen the value chain, diminishing the oversight the non-bank lending and financing sector has over the customer identification and document-verification procedures carried out on their behalf. The conduct of brokers themselves can also present a vulnerability, with several identified cases of brokers submitting fraudulent loan applications with falsified documentation. This was also an issue raised through submissions to the Royal Commission into Misconduct in the Banking, Superannuation and Financial Service Industry.³

The non-bank lending and financing sector is increasingly moving to online delivery channels. This shift exposes the non-bank lending and financing sector to cyber-enabled fraud, including fraudulent online loan applications and attempts to obtain loans using stolen or fraudulent identities.

³ Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, volume 3 - appendices, final report volume 3, royalcommission.gov.au/royal-commission-misconduct-banking-superannuation-and-financial-services-industry, page 24.

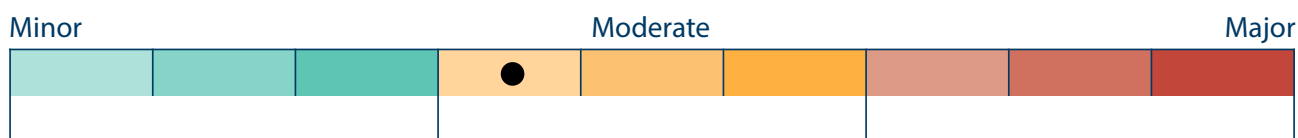
The non-bank lending and financing sector has a low number of overseas-based customers and is unlikely to disburse funds directly to overseas bank accounts. However, a small number of non-bank lenders and financiers facilitated approximately \$500,000 in international funds transfer instructions (IFTIs) on behalf of their customers, indicative of charitable donations or travel/tour expenses for interest group holidays abroad. While the vast majority of these IFTIs were low in value and likely related to legitimate activities, a large proportion were remitted to jurisdictions assessed as being higher risk for money laundering, tax evasion and/or child sexual exploitation.

A small number of non-bank lenders and financiers are also registered remittance service providers, which significantly increases their service offering but also their ML/TF risk profile. IFTI reporting data indicates that over 50 per cent of non-bank lenders and financiers have been associated with at least one IFTI during the assessment period.⁴ Further, a small number of non-bank lenders and financiers (approximately seven per cent) engage in more intensive IFTI activity, albeit with foreign jurisdictions considered as being lower ML/TF risk and predominantly appearing to relate to where they source their funding, including via their offshore parent companies.

It is highly likely there is significant under-reporting and non-reporting of suspicious matters across the non-bank lending and financing sector. Four of the 83 reporting entities that submitted SMRs during the assessment period reported over half of all the SMRs. AUSTRAC assesses there is considerable scope for the sector as a whole to improve their systems to identify and report suspicious matters.

4 Between 1 February 2018 and 31 January 2019.

CONSEQUENCES



The consequences of ML/TF activity in the non-bank lending and financing sector are assessed as **moderate**. They can include:

- personal loss and emotional distress for customers who are victims of fraud or scams
- loss of the non-bank lending and financing sector revenue and capital from fraud, higher insurance premiums, reputational damage and heightened regulatory attention
- where the non-bank lending and financing sector is used for money laundering, criminals are able to profit from their illicit activities, allowing them to maintain harm and expand their criminal activity
- increased placement risks for banks when accepting large cash transactions on behalf of non-bank lenders and financiers
- in relation to residential lending, increasing demand and therefore prices when money launderers seek to invest their criminal proceeds in real estate
- damage to Australia's international reputation as a safe and secure place to invest, impacting the economy and the non-bank lending and financing sector's ability to source overseas funding
- reduced government revenue as a result of tax evasion and higher government expenditure due to welfare fraud, impacting on the delivery of critical government services
- increased likelihood of a national security event where the sector is used to enable and sustain the activities of Australian foreign terrorist fighters, or terrorist acts in Australia or overseas.



PURPOSE

This assessment provides specific information to the non-bank lending and financing sector on ML/TF risks at the national level. Its primary aim is to assist the sector in identifying and disrupting ML/TF risks to Australia's financial system, and reporting 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 the sector 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 sector.

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



BACKGROUND

A non-bank lender and financier is a business that offers individuals and businesses loans, mortgages, personal finance, credit cards and other types of finance, but does not hold a banking license. They do not feature on the Australian Prudential Regulation Authority (APRA) list of authorised deposit-taking institutions as they do not accept deposits.

There are over 600 non-bank lenders and financiers in the Australian market, providing a range of services. The sector accounts for approximately seven per cent of debt financing in Australia.⁵

Non-bank lenders and financiers are recognised as reporting entities providing designated services under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act).

In accordance with the AML/CTF Act, reporting entities in the sector are required to maintain a compliant AML/CTF program and are obliged to report to AUSTRAC:

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

Reporting entities in the sector are also required to provide AUSTRAC with AML/CTF compliance reports.⁶

⁵ Reserve Bank of Australia, Financial Stability Review, April 2019, rba.gov.au/publications/fsr/2019/apr/pdf/financial-stability-review-2019-04.pdf, page 51.

⁶ A reporting entity must provide the AUSTRAC CEO a report relating to the reporting entity's compliance with the AML/CTF Act, the regulations and the AML/CTF Rules during the assessment period, legislation.gov.au/Series/C2006A00169.

AUSTRALIA'S NON-BANK LENDING AND FINANCING SECTOR⁷

Over 600 non-bank lenders and financiers operate in the Australian market, providing a range of services, including:



PERSONAL FINANCE

PAYDAY LENDING

BUY NOW PAY LATER SERVICES

RESIDENTIAL PROPERTY FINANCE

LOAN OFFSET ACCOUNTS

MOTOR VEHICLE FINANCE

EQUIPMENT AND LEASING FINANCE

COMMERCIAL FINANCE

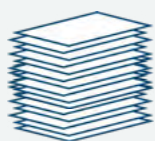
CREDIT CARDS

The sector's annual growth **2014-19 = 3.6%**⁸

The sector's projected annual growth **2019-24 = 9.6%**⁹

The sector's total assets¹⁰ **\$356 billion**¹¹

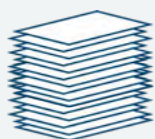
The sector accounts for less than **5% of total housing credit**¹²



SMRs SUBMITTED BY THE SECTOR¹³

83 reporting entities submitted **2,279 SMRs**, with a total value of **\$366.8 million**

4 reporting entities submitted over half (**53.5%**) of all SMRs



TTRs SUBMITTED BY THE SECTOR¹⁴

31 reporting entities submitted **545 TTRs**, with a total cash value of **\$9 million**

IMPACTS OF COVID-19

The COVID-19 pandemic has presented challenges for many Australian businesses, including the non-bank lending and financing sector. During periods of significant lockdown, face-to-face meetings moved online and in-person verification of identification and other documentation in many situations was not possible. A number of reporting entities implemented business continuity plans including protocols for digital document verification in response to the pandemic. The ML/TF impacts of any such changed protocols have not been assessed for this report.

7 For the purpose of this report, an entity must lend money under its control, rather than broker loans issued by third parties, to be considered a non-bank lender or financier.

8 IBISWorld Industry Report K6230 Non-Depository Financing in Australia, October 2018, page 4.

9 ibid.

10 Reporting institutions with total assets below \$50 million are not included.

11 March 2019, [rba.gov.au/fin-stability/fin-inst/main-types-of-financial-institutions.html](https://www.rba.gov.au/fin-stability/fin-inst/main-types-of-financial-institutions.html).

12 Reserve Bank of Australia, Financial Stability Review, April 2019, [rba.gov.au/publications/fsr/2019/apr/pdf/financial-stability-review-2019-04.pdf](https://www.rba.gov.au/publications/fsr/2019/apr/pdf/financial-stability-review-2019-04.pdf), page 51.

13 Between 1 February 2018 and 31 January 2019.

14 Between 1 February 2018 and 31 January 2019.



METHODOLOGY

The methodology used for this risk assessment draws on Financial Action Task Force (FATF) guidance that ML/TF risk can be seen as a function of criminal threat, vulnerability and consequence. According to this methodology:

- **Criminal threat environment** refers to the nature and extent of ML/TF and relevant predicate offences in a sector.¹⁵
- **Vulnerability** refers to the characteristics of a sector that make it attractive for ML/TF purposes. This includes features of the sector that can be exploited, such as its customer types, products and services, delivery channels and the foreign jurisdictions with which the sector deals. Vulnerability is also influenced by the risk mitigation strategies the sector has implemented.
- **Consequence** refers to the impact or harm that ML/TF activity through the sector can cause.

This assessment considered 19 risk factors across the above three categories. An average risk rating was determined for each category, and the average rating for each category determined the overall risk rating of the sector.

Further information on the methodology and its application in this risk assessment is in **Appendix B**.

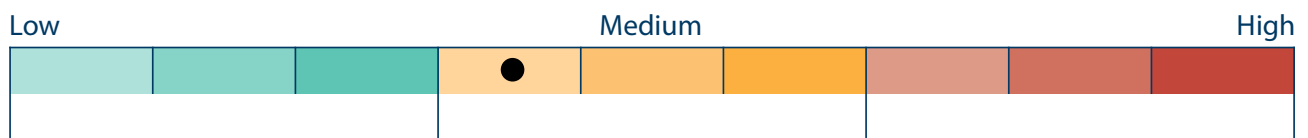
Three main intelligence inputs informed the risk ratings within this assessment:

- analysis of transaction reports, as well as other AUSTRAC information and intelligence
- reports and intelligence from a variety of partner agencies, including intelligence, law enforcement and regulatory agencies across government
- feedback and professional insights offered during interviews and consultations with a range of non-bank lenders and financiers, as well as industry experts and associations.

¹⁵ For ML/TF risk assessments, predicate offence refers to an offence which generates proceeds of crime, or other related crimes such as identity fraud.



CRIMINAL THREAT ENVIRONMENT



The criminal threat environment refers to the nature and extent of ML/TF and predicate offences associated with a sector. AUSTRAC assesses that the sector faces a **medium** level of criminal threat. This is based on SMRs submitted by and about the sector, and analysis of intelligence and other information from AUSTRAC, partner agencies and industry.

AUSTRAC conducted an in-depth analysis of the 2,279 SMRs submitted by the sector in a one-year period.

REPORTING BY THE SECTOR BETWEEN 1 FEBRUARY 2018 AND 31 JANUARY 2019

- Number of SMRs submitted during the sample period: **2,279**
- Total value of transactions reported in SMRs: **\$366.8 million**
- Number of reporting entities submitting at least one SMR: **83**
- Number of reporting entities accounting for over half of all SMRs submitted: **4**
- The vast majority of the 600+ entities in the sector did not submit any SMRs over the period.

WHAT HAPPENS AFTER AUSTRAC RECEIVES AN SMR?

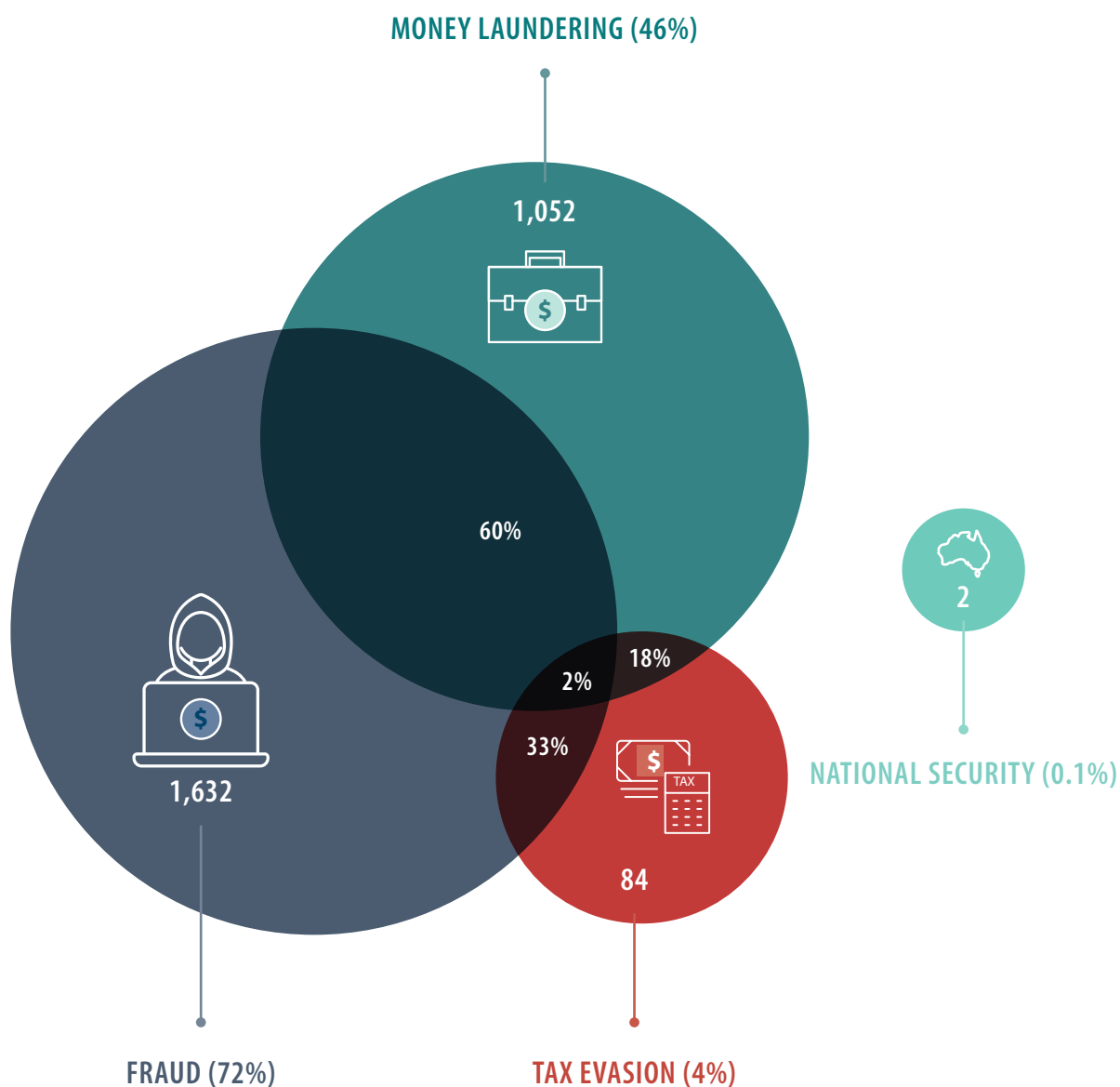
When an SMR is submitted to AUSTRAC, it is processed to detect crime types and surface high priority matters for immediate analysis. Reports and alerts are then assigned to AUSTRAC intelligence analysts to assess and respond in accordance with our national security and law enforcement intelligence priorities. Additionally, through direct online access to AUSTRAC's intelligence system, SMR information is available to over 4,000 authorised users from more than 35 of AUSTRAC's partner agencies to inform their intelligence gathering efforts and investigations.

SMRs PLAY A CRUCIAL ROLE IN LAW ENFORCEMENT

Under the AML/CTF Act, reporting entities have an obligation to report suspicious matters to AUSTRAC in various circumstances. For example, a reporting entity must submit an SMR if it reasonably suspects that the information it has concerning the provision, or prospective provision, of a designated service may be relevant to the investigation or prosecution of a crime. The full range of circumstances in which an SMR must be reported can be found in [section 41 of the AML/CTF Act](#).

SMRs submitted by the sector 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 their networks. Many of AUSTRAC's partner agencies – including the Australian Federal Police (AFP), Australian Criminal Intelligence Commission (ACIC), the Australian Taxation Office (ATO) and Services Australia – have access to SMRs in order to generate leads and conduct further analysis and investigation.

The following diagram illustrates the key threats identified in the SMRs in the dataset. While national security-related SMRs were standalone, a large number of SMRs indicated more than one threat type. For example, 60 per cent of SMRs that indicated tax evasion also include indicators of money laundering or fraud, or both.¹⁶



16 Percentages add to more than 100 because many SMRs showed more than one suspected threat type.

MONEY LAUNDERING

The nature and extent of the money laundering threats facing the sector are assessed as **medium**. Of the 2,279 SMRs reviewed, 1,052 SMRs (46 per cent) included indicators of money laundering, indicating criminals use loans to launder money by making loan repayments to the lender using the proceeds of crime.

EARLY LOAN PAYOUTS

The most common indicator of money laundering in SMRs was early loan payouts, which can indicate money laundering because:

- it is highly unusual for a customer to take out a loan and then repay the entire loan amount quickly
- it may indicate the customer is receiving income they had not declared to the lender.

Early loan payouts can indicate that illicitly-generated funds are being used to pay back the loan, thereby converting the proceeds of crime into high-value assets such as real estate and luxury vehicles. Even where the loan is not secured by a specific asset, funds that are sourced from legitimate lenders have a prima facie justifiable source, which, when repaid with the proceeds of crime, are effective tools for money laundering.

It can be difficult for the sector to determine whether an early loan payout is suspicious or not. It may simply reflect a customer's rational attempt to minimise interest payments, improve their credit score, obtain access to collateral benefits of a specific loan package, or adjust their financial strategy for some other legitimate reason. SMRs indicated that some reporting entities distinguished between legitimate and suspicious early loan payouts by assessing whether transactions were consistent with the customer's recorded profile, involved unexplained wealth or were conducted by a third party. While these are useful considerations, when an early loan payout is simply the result of a customer refinancing, unexplained funding may have been legitimately provided by a second lender.

OTHER INDICATORS OF MONEY LAUNDERING THROUGH THE SECTOR

While money launderers are likely to want to dispose of their criminal proceeds as quickly as possible, SMRs indicated that loan repayments that follow an expected repayment schedule can also be made with illicit funds. Excessive or unexpected use of cash repayment options were another indicator of money laundering identified during consultations and in SMRs. These repayments were often conducted through third-party branch networks and involved apparent structuring activity.¹⁷ In some cases it was the customer's suspicious behaviour, such as inconsistent or evasive responses when dealing with the reporting entity, that raised concern.

Two hundred and ninety-four of the SMRs (13 per cent) in the dataset related to companies, often involving finance for prestige vehicles. In some cases, the sector suspected the companies were using the proceeds of crime to repay their loans, essentially buying the asset with illicit funds. Large loan repayments, cash payments (including under the reporting threshold), early loan payouts and the use of third-party electronic billers to make repayments prompted the sector to submit SMRs about companies.

One reporting entity consulted also identified the complex movement of funds as a way to obscure financial activity. They described observing incoming payments, inconsistent with a customer's profile, being transferred between various offset accounts held by the customer for no clear reason. Twenty-five SMRs in the dataset describe similar transactional activity, some involving the rapid transfer of funds to and from third parties in a likely attempt to further obscure the origins of the funds.

¹⁷ Structuring occurs when a person deliberately splits a cash transaction into multiple transactions to avoid being reported in a threshold transaction report under section 43 of the AML/CTF Act.

GIFT CARDS

Several SMRs indicated that credit cards issued by the sector were being used to purchase unexpectedly large numbers of gift cards. Gift cards have been linked to money laundering and exploitation, including by foreign terrorist fighters. As described in [AUSTRAC's ML/TF risk assessment of stored value cards](#), gift cards can form a part of the money laundering cycle when reloaded (using cash), used overseas, and if purchased with the proceeds of crime and then on-sold. Depending on the nature of the gift card purchased, they can also be used to purchase goods and services anonymously.

One reporting entity conducted enhanced customer due diligence on a customer observed as making over \$800,000 in cash payments to their credit card over a three-month period. All the payments were made at third-party outlets and were under the TTR threshold, which is indicative of structuring.¹⁸ The reporting entity discovered the customer had used their credit card to purchase more than two million dollars' worth of gift cards in a twelve-month period.

They contacted the customer, who said they purchased baby formula for the Chinese market. This activity is known as *daigou*¹⁹ and can be high risk for money laundering and tax evasion.

SMRs LODGED BY OTHER REPORTING ENTITIES RELATING TO THE SECTOR

In addition to SMRs lodged by the sector, AUSTRAC reviewed a number of SMRs lodged by other reporting entities which contained reference to the non-bank lending and financing sector.

In general, these SMRs related to the non-bank lender and financier as a customer of another reporting entity (e.g. a bank). Suspicions raised included transactions to and from higher-risk jurisdictions and large cash deposits or withdrawals, in some cases where the source of funds is unknown. Some SMRs described the use of intelligent deposit machines (IDMs)²⁰ to make multiple cardless cash deposits. Some SMRs described the opening of accounts using a false identity. These SMRs also described excessive cash withdrawals by agents acting on behalf of the non-bank lender and financier, indicating possible misuse of the non-bank lender and financier's bank account for money laundering.

They also included instances of a third party who was a customer of both the non-bank lender and financier and another reporting entity that submitted the SMR. These SMRs described potential indicators of money laundering, in the form of large or otherwise unexpected transactions, including the purchase of high-value assets, remittance activity, and dealings with cryptocurrencies.

18 *ibid.*

19 *Daigou* literally translated means 'buying on behalf of' and refers to persons who buy items in one jurisdiction for residents of a second jurisdiction in which the items are difficult or costly to obtain.

20 Intelligent deposit machines (also known as Smart ATMs) are a type of ATM that have additional features, such as reconciling cash deposits in real time, conducting cardless deposits, transferring money between accounts, and depositing cheques.

TERRORISM FINANCING

The nature and extent of the terrorism financing threats facing the sector are assessed as **low**.

Overall, the primary terrorism threat to Australia stems from religiously-motivated violent extremism in the form of lone actors or small groups, although ideologically motivated violent extremism poses an increasing threat. These actors and groups primarily conduct small-scale, low-cost terrorist attacks using weapons that are inexpensive and easy to acquire, and tactics that do not require specialist skills. The national terrorism threat level at the time of publication is assessed by the National Threat Assessment Centre as **probable**.²¹

Two of the SMRs reported during the sample period were identified by the sector as being related to terrorism financing. While these SMRs indicate persons with possible links to terrorist activities were customers of non-bank lenders and financiers, they do not indicate the designated services provided by the reporting entity to the customer facilitated terrorism financing or extremist activities. AUSTRAC intelligence reports have not identified customers exploiting the services provided by the sector for terrorism financing.

While exploitation of the sector for terrorism appears to be very limited, the risk of terrorist actors utilising loan drawdowns has been identified previously and remains a risk. Often, their funding requirements do not involve significant amounts. Given these factors, the misuse of the sector by terrorist actors to raise funds remains possible, and the sector needs to remain vigilant to the risk of customers seeking to use their services for terrorism-related offences.

HOW MEDIA MONITORING HELPED THE SECTOR TO IDENTIFY POSSIBLE TERRORISM FINANCING

One of the terrorism financing SMRs was submitted by a non-bank lender and financier when an existing customer applied for additional finance. Media monitoring uncovered news articles reporting that the customer had been sentenced to imprisonment for criminal activity, and alleged that a portion of the funds obtained from this criminal activity was used to support foreign fighters. The news articles also alleged that the individual had links to an Islamic State-inspired terror cell. The application for finance was refused.

²¹ asio.gov.au/publications/speeches-and-statements/director-generals-annual-threat-assessment-2021.html, April 2021.

PREDICATE OFFENCES

The nature and extent of threats from predicate offences facing the sector are assessed as **medium**. AUSTRAC assessed SMRs describing predicate offences as being more likely to relate to actual illicit activity than the SMRs indicating money laundering.

FRAUD

AUSTRAC assesses that the key criminal threat faced by the sector is fraud, with 1,632 SMRs (72 per cent) most commonly describing loan application fraud, identity fraud and welfare fraud.

LOAN APPLICATION FRAUD AND IDENTITY FRAUD

Thirty-nine per cent of SMRs (890) included indicators of loan application fraud, the majority of which was conducted online. Loan application fraud was often associated with identity fraud, where the person seeking to secure funding used someone else's identity to avoid having to make repayments, or presented false and misleading information about themselves to the non-bank lender and financier to increase their chances of obtaining finance.

A person commits an offence under the AML/CTF Act if the person gives information or produces a document under the AML/CTF Act or Rules to, amongst others, a reporting entity or a person acting on a reporting entity's behalf, knowing the information or document to be false or misleading. Additionally, it is an offence if a person makes or possesses a false or misleading document and intends to produce it in the course of an applicable customer identification procedure.

The above offences attract a penalty of imprisonment for 10 years or 10,000 penalty units, or both. See sections 136, 137, and 138 of the AML/CTF Act for all elements of these offences.

FRAUDULENT LOAN APPLICATIONS USING STOLEN IDENTITY INFORMATION

A number of other SMRs describe reporting entities calling loan applicants to confirm details submitted in online applications, to find the person who answered the phone did not appear to be the same gender as the purported loan applicant, had a different name or displayed other suspicious behaviour. In one case, the reporting entity suspected the use of voice-altering technology. In other cases, instances of identity fraud were only identified after the reporting entity contacted the victim about overdue payments to find the victim had no knowledge of a loan having been taken out in their name.

In some cases, the victim of fraud was aware that their identification details had been stolen and used in several loan applications and were able to provide a police report to that effect. For example, one SMR detailed a case in which the victim of fraud was involved in a minor car accident and had exchanged licence and insurance details with the other party to the accident, only to discover a number of weeks later that their details had been used to fraudulently obtain a loan.

In some cases, a fraudulent loan application was made by a previous or current partner, or family member, of the victim. In a number of these cases the victim was reluctant to take action, citing that the family member was suffering from mental illness or drug addiction and preferred to repay the loan themselves rather than involve the police.

IDENTITY THEFT DISCOVERY REVEALS OTHER FRAUDULENT APPLICATIONS

One reporting entity received a phone call from an individual advising they had received an account statement from the lender but did not hold any accounts. The individual provided a police report demonstrating that their driver's license had been stolen.

By searching for other credit applications using the same phone number and passwords as the suspect application, the sector identified a further 48 fraudulent applications made in retail outlets in the same geographic area, likely by the same offender, who was well known to police for previous fraud offences. The offender was arrested and sentenced to a twelve-month custodial sentence.

SMRs in the sample indicated that, in cases of identity theft, the offender often makes several fraudulent loan applications, and information provided in one fraudulent application can be used to uncover other fraud attempts.

PERPETRATORS USING THEIR OWN IDENTITY BUT PROVIDING FRAUDULENT DOCUMENTATION

The other key form of identity fraud occurred when customers submitted falsified payslips, bank statements, Centrelink statements and other documentation in an attempt to fraudulently obtain finance. The sector noted inconsistencies in fonts and errors in the gross, net, taxation and superannuation amounts that raised their suspicions. False or old employer details were also common features of fraudulent loan applications. The level of sophistication in fraud attempts varied but was typically in proportion to the loan amount applied for.

Once a fraudulent application was identified, the sector was often able to identify other related fraudulent applications in their systems, by cross-checking other applications to identify common internet protocol (IP) addresses, phone numbers, passwords, physical addresses and employers. One reporting entity emphasised the usefulness of monitoring for the repeated use of the same

disbursement account. The sector indicated that, while IP addresses can be masked and phone numbers are relatively easy to obtain, disbursement accounts are subject to banks' AML/CTF processes, are likely to be re-used by fraudsters and can be used to identify them.

Engagement with industry indicated there is an over-representation of first payment defaults on fraudulently-obtained loans. This means that attributes (such as IP addresses, telephone numbers, disbursement accounts) used in loans where there was a default on the first payment can be considered by the sector as higher-risk for fraud, and subjected to heightened screening.

Several reporting entities reported using software to directly access the applicant's bank account as part of the loan approval process and which had eliminated many unsophisticated attempts at loan application fraud. The loan applicant is required to provide their banking login details to the non-bank lender and financier to facilitate this process. This information is encrypted and a minimum of 90 days' worth of transaction history from the bank account provides the information needed to make a decision about the loan. This access is read-only and the banking login details are not kept. However, not all entities in the sector use such software.

In a number of instances, the sector assessed that their customer had, in fact, legitimately taken out a loan and then claimed they had had their identity stolen in an attempt to avoid loan repayment. These matters were often identified because of the customer's reluctance to obtain or provide a police report in relation to the alleged fraud.

REGULAR MONITORING IDENTIFIES LARGE SCALE LOAN APPLICATION FRAUD BY BROKER

One reporting entity discovered a large-scale loan application fraud operation in a retail outlet. A staff member operating as a broker was falsifying customer application information so they would qualify for credit. The staff member was an employee of the retail outlet and was not employed by the non-bank lender and financier.

The fraud was uncovered when the reporting entity reviewed its monthly broker monitoring report. The particular retail outlet was identified for having higher-than-portfolio trends on customer applications for residential status, employment and residential tenure, marital status and financial liabilities. An investigation revealed the suspicious applications were all entered under the same username.

When a number of the customers were contacted, the discrepancies between the information on the application and their real circumstances were confirmed. It is unclear whether the customers were aware of the fraud perpetrated on their behalf, or if the employee of the broker was motivated by financial incentives provided by the non-bank lender and financier to originate a large number of loans.

As this example demonstrates, brokers acting as intermediaries between the sector and customers have scope to commit large-scale fraud. AUSTRAC identified 12 SMRs in the dataset relating to fraudulent behaviour by brokers, highlighting the risks posed by brokerage arrangements and the importance of robust systems and controls to monitor this activity. It is likely that, in some cases, bonuses and commissions motivate brokers to engage in fraudulent activity.

SMRs lodged about the sector by other reporting entities support the finding that non-bank lenders and financiers are exposed to identity fraud and loan application fraud. While it is clear the sector is aware of these threats, AUSTRAC encourages reporting entities to ascertain from their customer how long the bank account into which loaned funds are to be disbursed has been operational. SMRs from banks indicate this may assist the sector to mitigate against the threat that the account has only been opened to receive loaned funds, after which they are immediately withdrawn and the account closed.

LOAN FRAUD IDENTIFIED BY AUTHORISED DEPOSIT-TAKING INSTITUTIONS (ADIs)

Having identified indicators of attempts to obtain fraudulent access to a transaction account, a bank conducted enhanced customer due diligence (ECDD). Investigations revealed the perpetrator had successfully applied for loans from a range of non-bank lenders and financiers in a family member's name, and requested that the loaned funds be disbursed into the family member's transaction account. While the perpetrator was attempting to obtain access to the family member's bank account, the bank declined to process transactions until the account holder came into a branch to be physically identified.

WAGE STAGING

Wage or salary staging occurs when a loan applicant arranges for regular deposits to be made into their bank account to create the impression they are receiving a salary from an employer that doesn't exist, or with whom they are not currently employed. The purported employer may be difficult to contact or locate, or may be a family member. In some cases, one employer and associated income may be genuine but a second job or income stream may be staged to boost loan eligibility.

In cases of wage or salary staging, the bank statements supplied by applicants in support of their loan application have not been falsified, making it more difficult for lenders to detect the fraud.

SMRs submitted by other sectors have identified cases of suspected wage staging however this was not reported in any SMRs submitted by the non-bank lending and financing sector. While identifying this type of activity may be difficult, AUSTRAC urges non-bank lenders and financiers to remain vigilant to wage-staging attempts.

WELFARE FRAUD

Two hundred and fifty-four SMRs in the dataset (11 per cent) indicated possible welfare fraud. The sector described a number of scenarios indicating possible welfare fraud, including:

- information provided on the loan application being inconsistent with the Centrelink income statement, such as marital status, home ownership, rental payments, employment status and number of dependants
- transactions being inconsistent with the expected profile of a customer receiving Centrelink benefits
- customers receiving Centrelink benefits but also receiving employment income which the reporting entity suspected was not being declared
- customers receiving Centrelink benefits without withdrawing the funds, indicating they had access to another source of (likely undeclared) income.

During the consultation process, a number of reporting entities indicated it was difficult for them to establish exactly what an applicant's Centrelink entitlement was, which in turn made it difficult to establish whether they were receiving more than their due.

The financial and personal information gathered as part of the credit approval process places many reporting entities in a position where they have substantial knowledge of the financial circumstances of an individual. Non-bank lenders and financiers that require a Centrelink income statement will be more likely to be able to identify potential welfare fraud than if they only collect bank account statements.

i AUSTRAC strongly encourages the sector to leverage the information they collect to assess creditworthiness to identify possible instances of welfare fraud and to report them to AUSTRAC.

VISA FRAUD

The sector reported cases of international students who, during the loan application process, indicated they were exceeding the hours of work specified on their visa and were being paid 'off the books'. It appears this was done by the applicant in the belief they were strengthening their application by revealing to the non-bank lender and financier that they were working significantly more than what was permitted and officially declared. In one case, a loan applicant on an international student visa revealed they were not entitled to work and were receiving no legitimate income, but were working illegally and being paid in cash. While the motivation behind this activity was likely to circumvent visa conditions rather than evade tax, it does increase vulnerability to both payroll and personal income tax evasion.

SCAMS

The sector is subject to a limited threat from scams. Only six SMRs in the dataset indicated scam activity, three of which were in response to adverse media identifying the reporting entities' customers as perpetrating scams. In these cases, it is possible the proceeds of scams were used to repay the perpetrators' loans, but the scam itself was not facilitated through the reporting entity.

SOPHISTICATED CRIMINAL SYNDICATE TARGETS THE SECTOR

While undertaking a review of documentation submitted in support of a home loan, one reporting entity noticed an error in a payslip indicating the gross monthly pay amount was being deposited into the customer's bank account instead of the net amount. A review of the company the customer worked for linked their place of employment with a payroll scam syndicate. The syndicate was alleged at the time to be involved in phoenixing activity and large-scale taxation fraud.

After several months of non-payment of the home loan, an agent of the non-bank lender and financier conducted a field call and reported the financed dwelling had been used for the purposes of the hydroponic cultivation of cannabis. Police raided the property and arrested the occupants.

Members of the payroll scam syndicate were charged with proceeds of crime, fraud and blackmail offences for alleged involvement in an extortion attempt. Two individuals were arrested in connection with the hydroponic cannabis house and charged with several offences.

This case study demonstrates how sophisticated criminal syndicates can target the sector and that the assets financed by the sector can be used to commit predicate offences. Further, it shows how the information collected as part of the loan approval process can be used to identify serious criminality and help the sector protect itself and the community from exploitation.

EMPLOYMENT SCAM

During consultations, one reporting entity indicated they had received information about an identity theft scam where scammers posted employment advertisements on a number of Australian job websites. As part of the job application process, victims were asked for personal information – purportedly to assess suitability for the advertised role. Eventually the victim was required to provide bank account details, personal information and copies of identity documents such as their passport and driver's license. The scammers then used this information and the copies of documents to fraudulently apply for loans.

TAX EVASION

Seventy-five SMRs (or three per cent) in the dataset included indicators of personal or corporate tax evasion, with a small number of reports indicating both. As is the case with welfare fraud, the due diligence the sector does on their customers can be very useful in identifying possible tax evasion. For example, SMRs demonstrate that the sector often forms a suspicion of tax evasion when customers were unable to provide documentation to satisfy the non-bank lender and financier of their income source, because they were involved in the cash economy.

THE SHADOW ECONOMY

A number of the sector's delivery channels allow their products to facilitate the placement of large amounts of cash into the financial system. The sector needs to be aware of the role these transactions can play in facilitating the shadow economy (also sometimes referred to as the black economy), and ensure they implement measures to mitigate the harms the shadow economy can cause. In its final report, the Black Economy Taskforce stated that the shadow economy could be as large as three per cent of GDP – in 2015-16 this equated to \$50 billion.²²

THE BLACK ECONOMY STANDING TASKFORCE (BEST)

In response to the recommendations of the Black Economy Taskforce's Final Report²³ the Federal Government announced in the 2018-19 Budget²⁴ funding to the Australian Taxation Office of \$3.4 million over four years to lead the BEST and facilitate a cross-agency approach to combating the shadow economy. The BEST was announced to bring together key government agencies to allow the effective exchange of information, knowledge and experience across taskforce agencies and deliver a coordinated approach to identify and address serious, complex and high-value shadow economy activity, and broadly unreported and untaxed economic activity. AUSTRAC is a member of the BEST.

SMRs indicated that, in some cases, customers receiving cash income willingly inform their non-bank lender and financier of their involvement in the cash economy, so they can improve their chances of qualifying for finance and/or increase the amount they are eligible to borrow. Examples included:

- a business applying for finance notifying a non-bank lender and financier that their business only *appears* to be running at a loss because it is actually being paid in cash.
- an individual applying for a credit card who indicated they were working full-time for cash and continuing to receive full Centrelink benefits.
- a reporting entity assessing a loan application that could see no expenditure for living expenses in the applicant's bank statement. When queried by the non-bank lender and financier, the individual indicated they did a lot of cash-in-hand work and paid for their living expenses with the cash they earn.

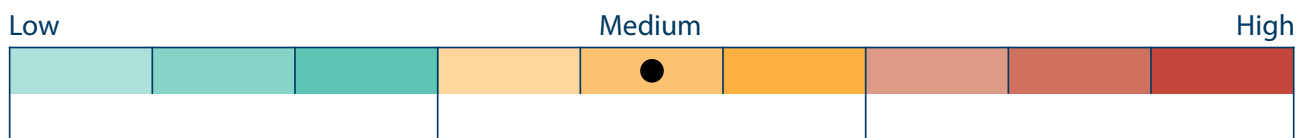
22 Black Economy Taskforce (Taskforce), Black Economy Taskforce: Final Report – October 2017, The Treasury, Canberra, October 2017, treasury.gov.au/review/black-economy-taskforce/final-report, page 35.

23 treasury.gov.au/sites/default/files/2019-03/Black-Economy-Taskforce_Final-Report.pdf.

24 Budget Measures Budget Paper No. 2 2018-19, archive.budget.gov.au/2018-19/.



VULNERABILITIES



AUSTRAC assesses that the sector faces a **medium** level of ML/TF vulnerability. Vulnerability refers to the characteristics of a sector that make it susceptible to criminal exploitation. AUSTRAC's assessment of vulnerabilities falls into five broad categories:

- customers
- products and services
- delivery channels
- foreign jurisdictions
- level of implementation of risk mitigation strategies.

CUSTOMERS

AUSTRAC assesses the sector's customer base presents a **medium** level of ML/TF vulnerability. This assessment is based on the size of the sector's customer base and the risk profile of its customers.

SIZE OF THE CUSTOMER BASE

The sector has a relatively large and growing customer base. Increased prudential regulation of ADIs by APRA over recent years has seen some lending activity migrate from ADIs to the sector, which are not subject to oversight by APRA. A 2019 report indicated the sector accounted for seven per cent of debt financing in Australia.²⁵ Analysis from 2020 indicates the sector's share of the commercial debt market is expected to rise over the next three years to more than \$50 billion by 2024.²⁶

In the rapidly expanding buy now pay later sector alone, it is estimated that 30 per cent of the adult population of Australia use this type of service.²⁷ Demand is also set to increase with regards to mortgage lending. Annual growth for the period 2019-24 is projected to increase at an annualised 9.6 per cent compared to 3.6 per cent for the 2014-19 period.²⁸

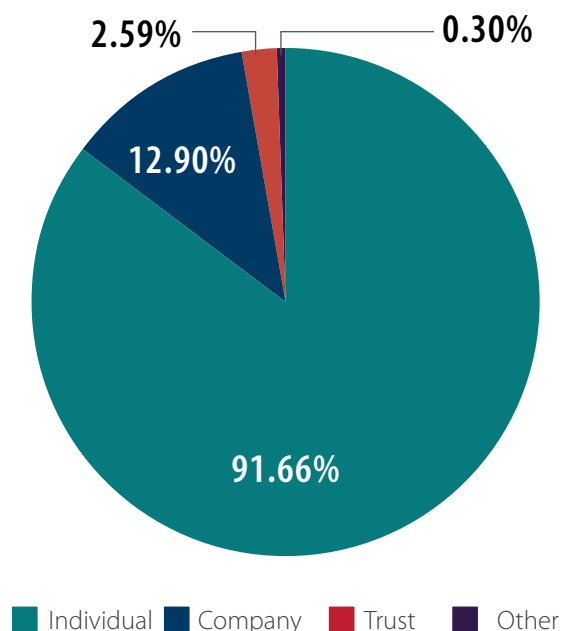
As the sector expands, the scale and complexity of its customer base, product offerings and delivery channels are also likely to increase. This will heighten the sector's exposure to ML/TF exploitation and put pressure on existing AML/CTF systems and controls. AUSTRAC expects the sector to carefully consider the impact of any expansion in their operations on their likely vulnerability to financial crime and the adequacy of their existing detection and mitigation systems.

HIGHER-RISK CUSTOMERS

NON-INDIVIDUAL CUSTOMERS

While the majority of the sector's customers are individuals, over 70 per cent of the sector reported in their 2018 compliance report having customers such as companies, trustees, partnerships and associations, registered cooperatives and government bodies. Non-individual customers present higher risks than individuals because they provide opportunities for perpetrators to obscure beneficial ownership and co-mingle criminal proceeds with legitimate funds, complicating detection efforts by authorities. The 2018 compliance report indicated the sector has a wide variety of customer types, while analysis of the SMR sample indicated that amongst these customer types, 92 per cent were individuals.

CUSTOMER TYPE REPORTED BY THE NON-BANK LENDING AND FINANCING SECTOR IN THE SMR SAMPLE²⁹



25 Reserve Bank of Australia, Financial Stability Review, April 2019, rba.gov.au/publications/fsr/2019/apr/pdf/financial-stability-review-2019-04.pdf, page 51.

26 Australian Financial Review, Property, 06/10/2020, Larry Schlesinger, page 27.

27 static1.squarespace.com/static/598589963e00bec843be0ea1/t/5e2fd417d30cb9303f3565cf/1580192793292/200129+-+Final+BNPL+release.pdf

28 IBISWorld Industry Report K6230 Non-Depository Financing in Australia, October 2018, page 4. Note: this forecast was generated prior to the COVID-19 pandemic.

29 Percentages add to more than 100 because many SMRs related to more than one customer type.

Two hundred and ninety-four of the SMRs (13 per cent) in the dataset related to companies, often involving finance for prestige vehicles. In some cases, non-bank lenders and financiers suspected the companies were using the proceeds of crime to repay their loans, essentially buying the asset with illicit funds. Large loan repayments, cash payments (including under the reporting threshold), early loan payouts and the use of third-party electronic billers to make repayments prompted the sector to submit SMRs about companies.

Fifty-nine SMRs in the dataset (three per cent) related to trusts. When assessing a trust's justification for an early loan payout, it can be difficult for reporting entities in the sector to determine affordability for trust customers because financial information contained in the trust deed can be unclear. Like other non-individual customers, trusts are also highly vulnerable to exploitation for the purposes of obscuring beneficial ownership and tax evasion.

POLITICALLY EXPOSED PERSON (PEP) SCREENING IDENTIFIES HIGH-RISK CUSTOMERS

Politically exposed persons often have the ability to award valuable contracts and make other decisions in relation to the exercise of government power, making them attractive targets for bribery and corruption.

One SMR from the dataset described a foreign PEP residing and working in Australia, and paying out a loan for a luxury vehicle early. As no reason was provided for the early loan payout, the transaction was deemed suspicious. Further investigation uncovered that the payment was made by cheque from an unrelated third party, making it higher risk for bribery/corruption or money laundering.

Consultations demonstrated many entities in the sector had PEPs as customers. As the above example demonstrates, PEP screening can assist the sector to identify high-risk customers and protect their businesses and government processes from exploitation. Systems to identify PEPs are also required under the AML/CTF Act and Rules.

CUSTOMERS' SOURCE OF FUNDS AND WEALTH

Over half of the SMRs in the dataset related to transactions being inconsistent with the customer's profile and/or unexplained wealth. In particular, the sector reported difficulty in understanding the source of funds for repayments when a third-party electronic biller was used to make transactions.

Third-party electronic billers enable payments to be made via an online, mobile or telephone payment system to businesses registered with the biller, including many non-bank lenders and financiers. Consultation with the sector, as well as information reported in SMRs, demonstrate that identifying the source of repayments made through third-party electronic billers is more difficult than when repayments are made through other channels, such as direct debit, due to the very limited information the sector receives about the sender.

LOW-DOC LOANS

Some lenders offer finance to self-employed people or small business owners who are unable to provide comprehensive evidence of their income. While for many borrowers, the absence of documentation reflects operational realities, some money launderers may seek to exploit this offering to avoid having their source of funds thoroughly investigated during the application process. Further, as described in the **Criminal threat environment** section, due diligence on source of funds was a key tool to determine loan serviceability. The sector used this to identify fraud, welfare fraud and tax evasion. AUSTRAC encourages additional due diligence activities in relation to low or no-doc loan applicants to mitigate the risks associated with these products.

AGENTS AND OTHER THIRD PARTIES

Agent and third-party relationship models carry different AML/CTF risks and need to be managed accordingly. The successful implementation of agent and other third-party arrangements is dependent on clear contracts, extensive collaboration and robust reviews. The systems put in place by the lender will determine how much additional risk is created by outsourcing.

Brokers play a critical role in the home loan and vehicle finance market, for both ADIs and the sector. Brokers have a significant and growing share of the home loan market and now account for the sale of more loans than lenders' own distribution channels.³⁰

Broker bonus commissions, bonus payments based on number of loans sold, and 'soft-dollar' incentives create a vulnerability because they can motivate brokers to create loans fraudulently.³¹ The Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, also known as the Banking Royal Commission, received over 130 submissions that focused specifically on conduct by intermediaries such as mortgage brokers.³²

Issues raised included the falsification of loan application information by mortgage brokers, including income and asset valuations and forgery of signatures.³³ SMRs in the sample included several cases of brokers submitting fraudulent loan applications with falsified documentation. The presence of this vulnerability is supported by action taken by ASIC in relation to loan fraud, where brokers and staff employed by lenders have been found to falsify documents when organising loans for customers.³⁴ Several credit providers have been temporarily or permanently banned from providing credit services as a result of this activity.

30 ASIC, REP[ORT] 516 Review of mortgage broker remuneration, released 16 Mar 2017, asic.gov.au/regulatory-resources/find-a-document/reports/rep-516-review-of-mortgage-broker-remuneration/, page 48.

31 'Soft dollar' benefits include any rewards that are not cash. This can include such things as hospitality and travel.

32 Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, volume 3 - appendices, final report volume 3, royalcommission.gov.au/royal-commission-misconduct-banking-superannuation-and-financial-services-industry.

33 *ibid.*

34 ASIC, REP[ORT] 516 Review of mortgage broker remuneration, released 16 Mar 2017, asic.gov.au/regulatory-resources/find-a-document/reports/rep-516-review-of-mortgage-broker-remuneration/, page 48.

Many reporting entities also use the services of aggregators who provide technological and administrative support to facilitate their relationships with brokers. Aggregators have contractual arrangements with lenders, allowing brokers on the aggregator's 'panel' to arrange loans from these lenders. Rather than holding their own credit licence, many brokers operate under the licence of an aggregator. In such cases, the aggregator is responsible for the conduct of the broker under the *National Consumer Credit Protection Act 2009*.³⁵

The sector's use of brokers and aggregators lengthens the value chain, in turn diminishing the oversight reporting entities have over the customer identification and document-verification procedures carried out on their behalf.

CONCERN FOR CUSTOMER'S SOURCE OF FUNDS AND COMPLICIT BROKERS

In one SMR, an individual made a series of large deposits onto their home loan in a short period of time via a third-party electronic biller. Then, in a one-week period, a series of rapid transactions in and out of the loan account occurred without any apparent economic purpose. The reporting entity formed the suspicion that the customer was attempting to obscure the funds' audit trail with multiple transactions of various amounts. Correspondence with the customer's mortgage broker claimed that the customer had recently won the lottery. The reporting entity suspected the customer, possibly with the assistance of the broker, was disguising illegitimately sourced funds as lottery winnings.

SERIOUS AND ORGANISED CRIMINAL NETWORKS

AUSTRAC's analysis demonstrated that persons of interest to law enforcement are transacting through the sector, either as customers or parties to transactions. Twenty-eight SMRs (1.2 per cent) related to a suspected or known member of a criminal network or gang, professional money laundering organisations, outlaw motorcycle gangs (OMCGs) or other groups.

In a number of cases, the non-bank lender and financier only became aware of links to criminal networks when a customer appeared in media reports or matched a heightened-risk entity on a third-party database. While these SMRs confirm persons suspected of links to criminal networks are customers of non-bank lenders and financiers, it was not confirmed that the non-bank lender and financier was actually *used* by the customer to fund crime.

One reporting entity engaged for this risk assessment indicated they had been targeted by an organised crime group well known to law enforcement. In this scheme, an individual who was part of the criminal group would legally obtain finance for a vehicle using their own identity documents. Once they took possession of the vehicle, they would pass it on to a criminal group (often to be broken down and used for parts) and then leave the country with no intention of returning. This kind of activity is one of the reasons the sector often refuses to provide credit to customers on short-term visas.

³⁵ ASIC, REP[ORT] 516 Review of mortgage broker remuneration, released 16 Mar 2017, asic.gov.au/regulatory-resources/find-a-document/reports/rep-516-review-of-mortgage-broker-remuneration/, page 48.

Several SMRs submitted about the sector by other entities were lodged in response to an enquiry by a government agency. Most often, the enquiry related to a third party who was a customer of both the reporting entity that submitted the SMR and the non-bank lender and financier, who may have been spreading their transactions across entities. In a handful of cases, the enquiry by the government agency related to the non-bank lender and financier itself.

SMRs ABOUT THE SECTOR'S CUSTOMERS BY OTHER REPORTING ENTITIES

One SMR was submitted by a non-bank lender and financier after they were notified that a motor vehicle loan was obtained as a result of identity fraud. This individual was also named in an SMR submitted by a second non-bank lender and financier for falsifying documents in an attempt to transfer existing assets prior to declaring bankruptcy and shield them from liquidation.

A further 10 SMRs submitted by banks indicated the customer was involved in identity takeover, suspicious cash withdrawals, fraudulent loan applications, unusually large transfers, account hacking and depositing valueless cheques.

In fact, many of the serious criminals about whom the sector reported SMRs were also the subject of transaction reports from other sectors. SMRs submitted about these subjects related to suspected proceeds of crime, money laundering, tax evasion and identity fraud, with many reports including structured and large cash activity and the use of third parties to conduct financial activity.

Non-bank lenders and financiers should submit reports to AUSTRAC even if they do not have comprehensive oversight over a customer's financial activity – AUSTRAC and its law enforcement partners can piece together reports submitted by the sector and other reporting entities to develop a full picture of a customer's activity.

PRODUCTS AND SERVICES

The nature of the products and services offered by the sector are assessed as posing a **medium** ML/TF vulnerability.

ABILITY TO STORE AND MOVE FUNDS OR VALUE

Loan structures are a well-established money laundering methodology, particularly when the loan is used to facilitate the purchase of high-value assets in which the proceeds of crime can be invested. Even when a loan is taken out without an associated asset, loan repayments can be an effective means of placing and integrating the proceeds of crime into the financial system while creating the perception of a plausible source of funds (the lender).

Loan products differ widely in terms of their capacity to allow customers to move funds. In general, the closer a loan product is to a transaction account (such as through an offset loan account facility), the more flexibly customers can move funds and further obscure their source.

ASSETS

With its relatively stable prices and tendency to appreciate over time, real estate can be attractive to money launderers for storage of the proceeds of crime. It is also a useful asset in terms of providing a place to live, deriving a rental income and generating wealth through appreciation.

As the examples in the **Criminal threat environment** and **Vulnerabilities** sections have demonstrated, mortgaged real estate can also be used as a physical location to commit predicate offences. Additionally, if a mortgaged real estate asset is seized by law enforcement, the criminal entity loses less than if the property is owned outright.

Some SMRs indicate the sector suspects the proceeds of crime are being used to repay mortgages. The inability to establish the source of funds for these repayments is a significant vulnerability, particularly when payments are made in cash at third-party branches, or via third-party electronic billers. SMRs also indicate criminals are attempting to use fraudulent documentation to obtain mortgages, in some cases with the suspected complicit assistance of brokers.

Vehicle financiers are also vulnerable to accepting repayments derived from the proceeds of crime. A number of SMRs observed early loan payouts without reason, in a manner deemed inconsistent with the customer profile, and/or by unknown third parties.

While the value of criminal proceeds that can be stored in a vehicle is relatively low compared to real estate, vehicle loans can attract money launderers because of the reduced due diligence required in relation to the acquisition and disposal of vehicles compared to that required for real estate. Further, vehicles purchased with borrowed funds can be stripped down and the parts on-sold in a manner that makes it difficult to link the purchased asset with the money launderer. Luxury goods of high value such as vehicles and yachts are also attractive to criminal entities because they offer lifestyle benefits and can act as status symbols.

OFFSET ACCOUNTS

Loan offset accounts essentially operate like transaction accounts that are linked to a mortgage. Money in the offset account is available to the customer to withdraw but, while in the offset account, it reduces the interest payable on the debt.

When money is deposited into an offset account with a non-bank lender and financier and then transferred into an account held at another financial institution, it creates a vulnerability in relation to layering that is not present in loan structures that don't allow withdrawals.

STORAGE AND MOVEMENT OF FUNDS THROUGH OFFSET ACCOUNTS

One SMR in the dataset described 60 electronic payments totalling over \$300,000 being made into a customer's offset account. An investigation revealed that payments appeared to come from 50 different third parties in different geographic locations and without any discernible relationship to the customer. The customer then debited the vast majority of the funds into their personal bank account. Given a logical and reasonable explanation for this activity could not be found, the reporting entity suspected the customer may have been facilitating money laundering.

A second SMR described business revenue being deposited into an offset account and then withdrawn into a personal account in a possible attempt to evade tax.

CREDIT CARDS

Two hundred and thirty eight SMRs in the dataset (10 per cent) related to credit cards. Like other loans, credit card accounts are open to exploitation when they are established with stolen identity information or paid off with criminal proceeds, including cash. The ability to deposit cash directly onto a credit card is an ML/TF vulnerability, exacerbated when the repayment is made via a third party.

Like offset accounts, credit card accounts can be used to move funds between locations, accounts, and payment types (e.g. cash to electronic value), increasing their similarity to transaction accounts and the flexibility they offer to those who would seek to exploit them. Moreover, most credit cards have the capacity to facilitate international transactions, including purchases of goods offshore, which increases the ML/TF vulnerability caused by exposure to foreign jurisdictions.

A number of entities in the sector offer white label credit cards through retail outlets.³⁶ White labelling arrangements are generally associated with diminished oversight of customer activity by the issuing entity (in this case, the non-bank lender and financier). This makes transaction monitoring and ongoing customer due diligence more challenging and, at times, less effective.

PERSONAL FINANCE INCLUDING PAYDAY LOANS

The ML/TF vulnerability associated with unsecured personal finance varies significantly with the amount financed, as this directly impacts how much money can be laundered via repayments. In some cases, SMRs indicated the sophistication of exploitation attempts increased with the amount borrowed, meaning threats associated with higher loan amounts may be harder to detect.

Given that personal loans are not tied to the purchase of an asset, they provide flexibility to the customer in terms of how the loaned funds are used. On the other hand, the lower transactional value associated with these loans compared to secured loans lessens the potential for the laundering of large amounts.

Small-value loans or credit contracts (also known as payday loans) are unsecured loans with a credit limit of \$2,000 and a term ranging between 16 days and one year.³⁷ Small loan providers have a strong online presence and are moving to more automated processes which can make them more vulnerable to fraud. Because payday lenders allow customers to apply for and receive personal finance online with no face-to-face contact, they are vulnerable to loan and identity fraud.

³⁶ A white label credit card is a store-branded credit card that is issued and managed by a third-party financial institution. The third-party financial institution issues the card, funds the credit, and collects the payments from customers.

³⁷ moneysmart.gov.au/loans/payday-loans.

BUY NOW PAY LATER

Buy now pay later (BNPL) arrangements allow consumers to buy and receive goods and services immediately but pay for those purchases over time. The ability for customers to apply for these loans online with no face-to-face contact heightens the risk of fraud, a fact that is reflected in SMRs from the BNPL sector. Fraudulently obtained loans can lead to losses for the service provider, or loans can be repaid with the proceeds of crime and the goods on-sold.

BNPL loans cannot be repaid with cash, and in fact need to be repaid via credit or debit card. This may reduce the risk of money laundering because it means transactions will be monitored by two reporting entities. On the other hand, it can also reduce the oversight the sector has over source of funds which may still be cash deposits into linked bank accounts.

Substantial growth in the BNPL sector is likely to put pressure on a reporting entity's existing AML/CTF systems and controls. Reporting entities offering these services should ensure their due diligence and transaction monitoring practices are consistent and robust, and SMRs are submitted when a reporting entity has a suspicion that a customer or transaction is related to criminal activity.

PAWNBROKING

A pawnbroker loan is an individual loan in exchange for goods, which become security for the loan repayment. If the loan, interest and other fees and charges are not repaid in the specified time, the pawnbroker can sell the goods to a third party.

The pawnbroking industry has grown at a slow pace over the past five years, due to the negative effects of COVID-19, mixed consumer sentiment, higher unemployment, and low household income growth.³⁸ One threat associated with pawnbroking is that the goods pawned are stolen and the customer has no intention of buying them back.

POTENTIAL STOLEN GOODS PAWNED AT DIFFERENT STORES TO AVOID THRESHOLD REPORTING OBLIGATIONS

In one SMR a non-bank lender and financier described how, during a one-week period, a customer pawned nine luxury watches to five different retail outlets in two states. The reporting entity suspected the customer may have used the different stores to avoid threshold reporting obligations, and that the goods may have been stolen.

38 ibisworld.com/au/industry/pawn-shops/5124/, page 9.

COMMERCIAL FINANCE

Customers of commercial finance can present significant vulnerabilities. They often involve corporate structures that can obscure beneficial ownership and complicate due diligence and detection measures. The proceeds of crime can also be co-mingled with legitimate business takings, complicating the sector's efforts to understand source of funds.

Distinct from consumer finance, commercial finance includes loans undertaken between a lending institution and a business, predominantly used to fund operating costs and capital expenditure. Commercial finance can include business term loans, commercial property loans, commercial overdrafts, cash flow finance, invoice finance, business credit cards, equipment finance and motor vehicle finance.

During industry consultations, it was noted that due to their complexity, commercial loans were more likely to be processed manually. Further, because they are larger in value, these loans typically prompt increased and ongoing customer due diligence.

For example, an SMR was submitted by a non-bank lender and financier regarding a commercial finance application for a business in the hospitality sector. During the credit assessment stage, it was identified that the company that owned the business was established in a jurisdiction associated with money laundering risks and a well-known tax haven.³⁹

The reporting entity commenced ECDD checks to better understand the beneficial ownership structure of the corporate entity. The corporate entity declined to assist with these additional enquiries and immediately withdrew their application, adding to the non-bank lender and financier's suspicion.

USE OF CASH

AUSTRAC assesses the ML/TF vulnerability posed by the sector's cash exposure to be **medium**.

While much of the sector does not accept cash from customers directly, and therefore reduces their exposure to the risk of money laundering placement, a number of entities in the sector provide a direct capability for their customers to transact in cash through third-party branches or agents such as nominated banks or post offices.

A large number of SMRs in the dataset demonstrated that the use of cash to repay loans through third-party branches or agents is a reasonably significant vulnerability for the sector. Cash deposits facilitated through third-party branches or agents are associated with diminished oversight over transactions and customers, particularly when the transaction falls below the threshold transaction reporting amount. In one example, a non-bank lender and financier that issued a credit card to a customer identified multiple cash payments being made at a third-party branch just under the reporting threshold, with \$9,900 being deposited twice a day across multiple days.

In a small number of cases described by the sector in SMRs, AUSTRAC could not identify that a TTR had been submitted in relation to large cash transactions conducted through third-party branches or agents. This may indicate there is uncertainty between the third party/agent and the sector regarding who has the TTR obligation.

Some reporting entities may have formal agent bank arrangements with domestic banks to facilitate cash deposits for their customers and it is essential reporting entities understand their reporting obligations for TTRs under these arrangements. Further details of ML/TF vulnerability associated with these arrangements and TTR reporting obligations is provided at page 36 in the section **Delivery channels**. Reporting entities can also refer to AUSTRAC's [website](#) for specific guidance.

³⁹ icij.org/investigations/panama-papers/.

TTRs SUBMITTED BY THE SECTOR TO AUSTRAC BETWEEN 1 FEBRUARY 2018 AND 31 JANUARY 2019

Over the reporting period, 31 non-bank lenders and financiers submitted 545 TTRs involving a total cash value of \$9 million. While this is a relatively low cash exposure, it still demonstrates that there is capacity in the sector to facilitate very large cash transactions.

These TTRs included:

- 356 incoming transactions with a cash value of \$6 million
- 189 outgoing transactions with a cash value of \$3 million
- three TTRs were for cash amounts over \$50,000, including one TTR for a cash amount over \$1,000,000
- four reporting entities accounted for over half of the TTRs submitted.

Given the number of SMRs reviewed indicated structuring to avoid threshold reporting obligations, it is clear the figure of \$9 million significantly understates the sector's exposure to cash.

TTRs submitted about non-bank lenders and financiers by other reporting entities also show numerous instances of individuals conducting large (sometimes repeated) deposits in favour of the non-bank lender and financier. While it is not evident in these cases that the deposits constitute repayments for loans held with the non-bank lender and financier, these TTRs further demonstrate the sector's overall exposure to cash is understated by its own TTR reporting.

During consultations, the sector confirmed there was a low tolerance for the risks of dealing in cash. A number of non-bank lenders and financiers described the introduction of policies that eliminated or restricted the ability of customers to pay cash into loan accounts. One entity reported they only allow customers to make loan repayments using direct debit payments. Another reported having removed customers' ability to repay loans using cash, cheques or via third-party arrangements.

DELIVERY CHANNELS

Delivery channels refer to the methods by which reporting entities deliver their products and services to their customers. The sector provides its services in a number of ways including face-to-face through branches, online, by phone, and through third-party arrangements.

LEVEL OF CUSTOMER CONTACT

Compared to other sectors, non-bank lenders and financiers have a low rate of customer interaction. This is due in part to the nature of loans – once a loan is established it is common for a customer to have no further direct contact with the lender outside of making repayments, which often occurs online.

Engagement with industry for this risk assessment confirmed the low level of face-to-face customer interaction, with one reporting entity indicating they have contact with their customers, on average, once every two years. This, coupled with the trend towards online services, decreases the sector's opportunity to oversee and understand its customers, and increases the sector's vulnerability to criminal exploitation if sufficient controls are not in place to mitigate the risk.

BRANCHES

A small number of entities in the sector have a significant branch network. Broadly speaking, face-to-face delivery of services via a branch network present a lower risk than online delivery channels because they limit the customer's ability to obscure their identity.

Branch networks also provide opportunities for reporting entities to observe behaviour and question the purpose of unusual transactions like early loan payouts and large cash repayments. Engagement with industry also indicated that delivery of services through branches provide a greater opportunity to develop closer customer relationships. This can have business benefits as well as improve the sector's understanding of customers' circumstances and transactions.

ONLINE SERVICES

The sector is increasingly moving to online delivery channels. A significant number of reporting entities engaged for this risk assessment deliver, or intend to deliver, their products *exclusively* online. Some reporting entities have a purely online application process, to the point where automated systems make the decision to lend.

Online services expose the sector to cyber-enabled fraud such as fraudulent online loan applications and identity fraud. Several SMRs described reporting entities calling loan applicants who disclaimed any knowledge of the loan application, but could identify an incident in the past in which their identity details may have been compromised.

Indicators of fraudulent online loan applications described in SMRs and in consultations with industry included:

- passwords, physical and IP addresses, phone numbers, disbursement accounts, customer details, and answers to security questions that were common across a number of loan applications
- the provision of contact details where email addresses and/or phone numbers were invalid or disconnected
- contact information that was changed immediately after a successful loan application.

Online delivery channels also increase the speed with which funds can be moved between accounts and financial institutions, making illicit funds more difficult to restrain or confiscate.

The speed of technological change within Australia's non-bank lending and financing sector is expected to continue into the foreseeable future. However, new technologies also present new ML/TF risks and AUSTRAC encourages the sector to remain vigilant and adjust their systems and controls accordingly.

THIRD-PARTY ELECTRONIC BILLERS

Many loans offered by the sector allow repayments to be made via third-party electronic billers. Transactions facilitated by third-party billers are vulnerable to ML/TF because they can obscure the customer making the payment, meaning payer details are not visible to the reporting entity. Transaction descriptions are also not required, further limiting a reporting entity's ability to investigate the source of funds.

Individuals could exploit the lack of visibility created by third-party billers to layer illicit funds from a transaction account held with a bank to a loan account held with a non-bank lending and financing entity.

A number of sector SMRs and consultations with reporting entities revealed concerns about unknown third parties making loan repayments using a third-party electronic biller.

COMPLEXITY OF PRODUCT DELIVERY ARRANGEMENTS

AUSTRAC assesses that the complexity of the product delivery arrangements associated with the sector presents a **medium** level of ML/TF vulnerability.

The sector relies heavily on brokers and aggregators to deliver their products to customers. A number of entities in the sector offer white labelled credit cards, personal loans and mortgages, and a number have agreements with retail outlets to provide customer finance in store. In several SMRs relating to this delivery channel, retail outlet staff members were the key point of vulnerability facilitating the fraudulent loan applications, rather than customers.

As noted previously, a number of reporting entities provide a direct capability for their customers to transact in cash through third-party branches or agents such as nominated banks or post offices.

While outsourcing to third parties, including through agent banking arrangements, can provide advantages such as greater accessibility for customers and improved sophistication of services, using third parties can create vulnerabilities in the ability to detect and act upon suspicious activity due to the increased distance between the reporting entity that holds the AML/CTF obligations and the ultimate customer.

REPORTING OBLIGATIONS TO AUSTRAC

Some reporting entities may be uncertain as to who is responsible for reporting TTRs to AUSTRAC in agent bank arrangements. In these arrangements, the loan provider (in this case the non-bank lender and financier) is providing the designated service and is therefore required to submit a TTR if the designated service involves a threshold transaction. However, a loan provider and agent can enter into a contractual arrangement permitting the agent to report TTRs on the loan provider's behalf. Where such an arrangement is in place, AUSTRAC expects the loan provider to ensure appropriate risk management processes are in place for agent monitoring and assurance.

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

FOREIGN JURISDICTIONS

AUSTRAC assesses the sector to have a **medium** level of vulnerability with respect to foreign jurisdiction risk. Exposure to foreign jurisdictions creates ML/TF risks because it allows serious and organised crime groups to move the proceeds of crime to and from Australia. It may also facilitate the movement of funds for illegal purposes, such as terrorism financing or the purchase or sale of illicit goods transnationally. Further, international transactions add complexity and make it more difficult for unlawfully-obtained funds to be recovered.

MOVEMENT OF FUNDS OR VALUE INTERNATIONALLY

It is difficult to obtain a comprehensive understanding of the foreign jurisdiction exposure of the non-bank lending and financing sector. As described throughout this report, the sector is very diverse – different product lines are naturally associated with different levels of foreign exposure, and entities have widely differing marketing strategies and risk appetites in this area. Further, a number of reporting entities are also registered remittance service providers. This increases the foreign jurisdiction exposure of those *entities* in the sector without necessarily reflecting on the exposure of their loan products.

Broadly speaking, the sector requires prospective borrowers to be Australian residents or have long-term visas, and to hold an Australian bank account for loan fund disbursements. This latter control, however, can be of limited effectiveness given the ease with which foreign nationals can open, transact on, and quickly close an Australian bank account.

A number of entities reported they will only accept Australian or New Zealand identification documents. Like credit checks, controls in relation to the borrower's country of residence constitute examples of business practices also serving to mitigate ML/TF risk. The sector is likely to use these controls predominantly to increase the likelihood that the loan is repaid in a timely fashion, but they also mitigate foreign jurisdiction risk.

In some cases, the sector reported that they targeted particular resident migrant groups as part of their business strategy – either directly or by maintaining relationships with brokers who work with specific communities. One reporting entity indicated that, in these situations, they may see large loan repayments atypical of their usual customers. These are justified as being the result of pooled resources, gifts from their home countries or the proceeds of the sale of overseas assets.

Credit card-issuing entities in the sector indicated most cards can be used almost anywhere in the world. Generally speaking, the transaction processing schemes associated with credit cards control which jurisdictions activity can take place in, rather than the entity that issues the card itself. This limits the sector's capacity to control the nature of their foreign jurisdiction exposure.

INDIRECT FOREIGN JURISDICTION EXPOSURE

The customer of a non-bank lender and financier was the subject of an SMR submitted by a reporting entity outside of the sector. This reporting entity noted that the proceeds of a very large loan from a non-bank lender and financier were immediately transferred offshore, which was considered unusual in the context of the expected purpose of a residential loan.

While the non-bank lender and financier may not have been aware of the actual purpose of the loan, this example demonstrates that robust due diligence is required to ensure the actual purpose of a loan is the one stated by the customer, so their foreign jurisdiction exposure is not higher than they are aware. It also demonstrates that while a non-bank lender and financier itself may not directly transact with foreign jurisdictions, disbursing funds into Australian bank accounts which do allow international transactions constitutes a form of indirect foreign jurisdiction exposure.

IFTI REPORTING

A number of entities in the sector are registered remittance service providers and/or provide financial services in addition to loans. These other services may trigger an IFTI reporting obligation by the reporting entity or a third party.

AUSTRAC extracted the IFTIs submitted by a wide range of reporting entities to which the sector was party, identifying tens of thousands of IFTIs involving approximately half of the non-bank lending and financiers in the Australian market. However, over 90 per cent of the total value transferred was associated with fewer than 50 non-bank lenders and financiers (most of which are well-recognised brands with a global footprint).

While the overall number and associated value of these IFTIs are quite high, it is likely the vast majority of these reports do not relate to the sector's lending activity (though it may relate to where they source their funding, including via their offshore parent companies). Notwithstanding, these IFTIs indicate the foreign jurisdiction exposure of the *entities* in the sector is significantly higher than was expected based on industry engagement.

TRANSACTIONS WITH HIGHER-RISK JURISDICTIONS

AUSTRAC assesses the jurisdictions with which the sector transacts pose a **medium** level of ML/TF vulnerability. IFTI data indicates many international transactions appear to be related to the sector transacting with their offshore parent companies, largely in jurisdictions considered to be a lower ML/TF risk. However several high-value IFTIs (averaging several million dollars each) reported by the sector indicate likely commercial finance repayments by customers in jurisdictions deemed to be higher-risk for money laundering or other serious crimes.

Over the assessment period, a small number of reporting entities also reported a total of approximately \$500,000 in IFTIs facilitated on behalf of their customers, indicative of charitable donations to Christian groups or missions overseas, or indicative of travel/tour expenses for interest group holidays abroad.

While the vast majority of these IFTIs were low in value (significantly less than \$5,000 each) and likely relate to legitimate activities, a large proportion were remitted to jurisdictions assessed as being higher risk for ML, tax evasion and/or child sexual exploitation (CSE). It is critical reporting entities understand their customers' transactions with these jurisdictions in order to assess their risk exposure and detect criminal behaviour.

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 off-the-shelf solutions that risk rate jurisdictions. If doing so, reporting entities should consider their own risk profile and be able to override default risk ratings.

In line with this approach, 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 sources AUSTRAC has leveraged to inform these decisions include:

- European Union's high-risk third countries with strategic deficiencies in their AML/CTF regimes
- European Union list of non-cooperative jurisdiction in taxation matters
- FATF's high risk and other monitored jurisdictions
- Transparency International's Corruption Perception Index
- US State Department's International Narcotics Control Strategy Report.

IMPLEMENTATION OF RISK MITIGATION STRATEGIES

AUSTRAC assesses the level of implementation of risk mitigation strategies poses a **medium** level of vulnerability in the sector. Risk mitigation strategies include both measures that are mandatory under AML/CTF legislation and other practices that are unrelated to AML/CTF obligations but also mitigate ML/TF risk.

Non-bank lenders and financiers have strengths in terms of leveraging the due diligence they do for business and consumer credit protection reasons to protect themselves from financial crime.

As discussed in the **Criminal threat environment** section, investigation of customers' financial status to assess creditworthiness enabled the sector to identify welfare fraud and tax evasion. Further, reluctance to lend to customers who may permanently leave the country before repaying the loan has lowered the sector's foreign jurisdiction exposure.

Other risk mitigation strategies identified during the development of the risk assessment in relation to a number of reporting entities include:

- restrictions on the extent of cash deposits to repay loans
- communication and collaboration between reporting entities, such as at AML/CTF industry forums
- communication and collaboration between the sector and government/law enforcement agencies
- provision of support to customers who appear to be victims of fraud
- some reporting entities conduct all due diligence and know your customer (KYC) processes, irrespective of whether the loan originated with a third party
- disbursing funds directly to the vendor of the vehicle being purchased, rather than to the borrower – this ensures the loan is used for the stated purpose

- audit of completed loan applications to maintain fraud and quality control standards
- collaboration with banks for the purpose of fraud detection
- strictly limiting the redraw facilities attached to some mortgages
- the use of software that enables read-only access to an applicant's bank account and the previous 90 days of their banking history as part of the loan approval process.

Two areas in which the sector's risk mitigation systems and controls could be strengthened – outsourcing and SMR reporting – are outlined below.

OUTSOURCING

Many entities in the sector outsource customer identification processes, AML/CTF program development and/or transaction monitoring practices.

Outsourcing arrangements can be complex and difficult to oversee and manage. Insufficient oversight of outsourced functions places the sector at risk of unintentional non-compliance. This risk increases when the outsourced service provider uses automated systems to fulfil its obligations, when automated systems are not subject to regular testing and quality assurance, and when service providers themselves outsource to an additional party.

Non-bank lenders and financiers remain responsible for their AML/CTF obligation regardless of whether any functions or activities have been outsourced. Effective outsourcing includes:

- ensuring roles and responsibilities are clearly and sufficiently detailed in contracts
- proactively monitoring and testing, and conducting quality assurance in relation to AML/CTF systems and processes provided by others, including automated systems.

SUSPICIOUS MATTER REPORTING PROCESSES

The sector reports a relatively low number of SMRs, with numbers varying radically between individual entities of a similar size and scale. Only 13 per cent of the sector submitted an SMR over the one-year assessment period.

SMRs are a crucial source of intelligence for AUSTRAC and a key obligation for all reporting entities, including the sector. AUSTRAC uses SMRs and other information to generate intelligence products for use by law enforcement and national security agencies. The information provided in an SMR can lead to the detection and disruption of criminal activity or even prevent a terrorist attack.

AUSTRAC urges the sector to review their systems to detect and report suspicious matters, and ensure they are appropriate to the nature of the business.

FURTHER RESOURCES ON SUSPICIOUS MATTER REPORTING

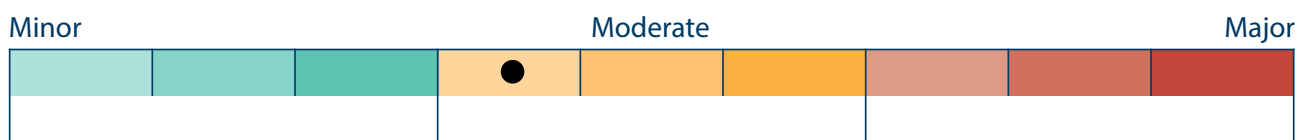
Further guidance on submitting SMRs can be found on [AUSTRAC's website](#). AUSTRAC has also developed the following resources to help reporting entities understand what makes a good SMR, and how SMRs help protect Australia from financial crime and terrorism financing.

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

AUSTRAC encourages all non-bank lenders and financiers to review these resources and consider if their reporting could be improved.



CONSEQUENCES



The consequences of ML/TF activity in the sector are assessed as **moderate**.

Consequence refers to the potential impact or harm that ML/TF and other financial crime may cause.

Financial crime in the sector has consequences for customers, individual reporting entities, the sector as a whole and the broader Australian economy. Where the sector is used to facilitate the financing of terrorism, there are consequences for domestic and international security.

The impact of criminal activity on customers can include:

- financial loss and emotional distress from fraud or scams facilitated through the sector
- higher borrowing costs, as the sector passes on the costs of responding to financial crime to their customers.

The impact of criminal activity on the sector can include:

- loss of revenue from fraud and increased fraud insurance premiums
- increased costs associated with combating criminal attacks/cyber-enabled fraud, in particular IT security costs to build cyber resilience
- non-bank lenders and financiers with insufficient AML/CTF programs becoming known to criminal entities, encouraging further criminal activity and proceeds of crime to flow into the sector
- reputational damage to the sector following an incident, leading to loss of customers and increased public relations costs
- increased regulatory attention, or legal action, associated with civil or criminal penalties in the event of serious non-compliance by a non-bank lender and financier.

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

- undetected criminal activity, thereby providing a safe haven for the proceeds of crime and the perpetuation of predicate offences
- reduced government revenue from tax evasion and heightened expenditure from welfare fraud, impacting on the delivery of critical government services
- higher costs of policing, as crucial financial intelligence is not reported to law enforcement agencies
- increasing cash placement risks for banks where the sector allows cash repayments to be accepted on behalf of non-bank lenders and financiers
- widespread loss in confidence in the sector as well as the overall Australian financial system

- increases in real estate prices due to purchases of real estate with the proceeds of crime, pricing legitimate buyers out of the market
- damage to Australia's international economic reputation in relation to the integrity of Australia's financial sector.

The impact of criminal activity on national and international security can include sustaining and enabling the activities of Australian foreign terrorist fighters and enabling terrorist acts both in Australia and overseas, causing severe distress and uncertainty and harming Australia's global image.




APPENDIX A: GLOSSARY

Name	Description
ADI	An authorised deposit-taking institution (ADI) is either (1) a body corporate authorised under the <i>Banking Act 1959</i> to carry on banking business in Australia (e.g. a bank, building society or credit union); (2) the Reserve Bank of Australia; or (3) a person who carries on state banking within paragraph 51(xiii) of the Constitution.
AML/CTF	Anti-money laundering and counter-terrorism financing.
AML/CTF Act	The <i>Anti-Money Laundering and Counter-Terrorism Financing Act 2006</i> (AML/CTF Act) is the main piece of Australian government legislation that governs AUSTRAC's functions. Its aim is to prevent money laundering and the financing of terrorism by imposing a number of obligations on the financial sector, gambling sector, remittance (money transfer) services, bullion dealers and other professionals or businesses (known as 'reporting entities') that provide particular services (known as 'designated services'). ⁴⁰
AML/CTF program	A document that sets out how a reporting entity will meet its AML/CTF compliance obligations.

⁴⁰ oaic.gov.au/privacy/other-legislation/anti-money-laundering/.

Name	Description
Compliance report	<p>The compliance report is an annual report that includes information submitted by a reporting entity about how it has met its anti-money laundering and counter-terrorism financing (AML/CTF) obligations.</p> <p>The compliance report is a requirement under <i>the Anti-Money Laundering and Counter-Terrorism Financing Act 2006</i> (AML/CTF Act).</p>
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.
Daigou	Daigou literally translated means 'buying on behalf of'. It refers to persons who buy items in one jurisdiction for residents of a second jurisdiction in which the items are difficult or costly to obtain.
Enhanced customer due diligence (ECDD)	Enhanced customer due diligence (ECDD) is the process of collecting and/or verifying additional customer identification undertaken by a reporting entity in certain circumstances deemed to be higher risk.
Financial Action Task Force (FATF)	The Financial Action Task Force (FATF) is an inter-governmental body focused on fighting money laundering, terrorism financing and other related threats to the integrity of the international financial system, by ensuring the effective implementation of legal, regulatory and operational measures.
Integration	The final stage of the money laundering cycle, in which illicit funds or assets are invested in further criminal activity, 'legitimate' business or used to purchase assets or goods. At this stage, the funds are in the mainstream financial system and appear to be legitimate.
International funds transfer instruction (IFTI)	<p>An international funds transfer instruction (IFTI) involves either:</p> <ul style="list-style-type: none"> • an instruction that is accepted in Australia for money or property to be made available in another country • an instruction that is accepted in another country for money or property to be made available in Australia.
Layering	The second stage of the money laundering cycle, which involves moving, dispersing or disguising illegal funds or assets to conceal their true origin.
ML/TF	Money laundering and terrorism financing.
Politically exposed person (PEP)	A politically exposed person (PEP) is an individual who holds a prominent public position or role in a government body or international organisation, either in Australia or overseas. Immediate family members and close associates of these individuals are also considered PEPs. PEPs often have power over government spending and budgets, procurement processes, development approvals and grants.
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, predicate offence is any offence which contributes to the generation of proceeds of crime.

Name	Description
Remittance service provider	<p>A remittance service provider is an entity that accepts instructions from customers to transfer money or property to a recipient. It is also commonly known as a 'money transfer business'. This does not include a business operating as a financial institution such as a bank or credit union.</p> <p>A 'registered remittance service provider' is registered with AUSTRAC. It is against the law to provide remittance services in Australia without being registered.</p>
Suspicious matter report (SMR)	<p>A report that must be submitted by a reporting entity under the AML/ CTF Act if they have reasonable grounds to suspect that a transaction may be related to money laundering, terrorism financing, tax evasion, proceeds of crime or any other serious crimes under Australian law. An SMR must also be submitted if the reporting entity has reasonable grounds to suspect the customer or an agent of the customer is not who they say they are.</p>
Structuring	<p>Structuring is where a person deliberately:</p> <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. <p>Structuring can be a money laundering technique and is against the law under the AML/CTF Act.</p>
SOCG	<p>Serious and organised crime group.</p>
Threshold transaction report (TTR)	<p>A report submitted to AUSTRAC about a designated service provided to a customer by a reporting entity that involves a transfer of physical or digital currency of \$10,000 or more or the foreign currency equivalent.</p>



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 19 risk factors across the above three categories and each risk factor was assessed as low, medium or high, as per the table below. These assessments were based on quantitative and qualitative intelligence inputs, including analysis of SMR and other reporting data, intelligence assessments from partner agencies, and feedback from industry. The average of the scores of each criterion provides the total risk score for each category. The average of the three risk scores for each category provides the overall risk rating for the sector.

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

VULNERABILITIES		
Low	Medium	High
Few higher risk customers.	A moderate number of higher risk customers.	A high number of higher risk customers.
Sector has a small customer base.	Sector has a medium customer base.	Sector 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.
Sector tends to have simple and direct delivery arrangements.	Sector tends to utilise some complex delivery arrangements.	Sector tends to utilise many complex delivery arrangements.
Funds and/or value are generally not transferred internationally.	Moderate amount of funds and/or value can be transferred internationally.	Significant amounts of funds and/or value are easily transferred internationally.
Transactions rarely or never involve higher-risk jurisdictions.	Transactions sometimes involve higher-risk jurisdictions.	Transactions often involve higher-risk jurisdictions.
At a sector level, significant systems and controls have been implemented to mitigate vulnerabilities.	At a sector level, moderate systems and controls have been implemented to mitigate vulnerabilities.	At a sector level, limited systems and controls have been implemented to mitigate vulnerabilities.

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



AUSTRAC.GOV.AU

