



Australian Government

AUSTRAC

AUSTRALIA'S MUTUAL BANKING SECTOR

MONEY LAUNDERING AND TERRORISM
FINANCING RISK ASSESSMENT

COPYRIGHT

© Commonwealth of Australia 2019

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.itsanhonour.gov.au).

Contact us

For enquires regarding the license and any use of this report please contact AUSTRAC Media and Communications at communications@austrac.gov.au.

CONTENTS

BACKGROUND	03
EXECUTIVE SUMMARY	04
PURPOSE AND SCOPE	07
METHODOLOGY	07
CRIMINAL THREAT ENVIRONMENT	08
VULNERABILITIES	17
CONSEQUENCES	40
GLOSSARY	41
APPENDIX A: RISK ASSESMENT METHODOLOGY	43

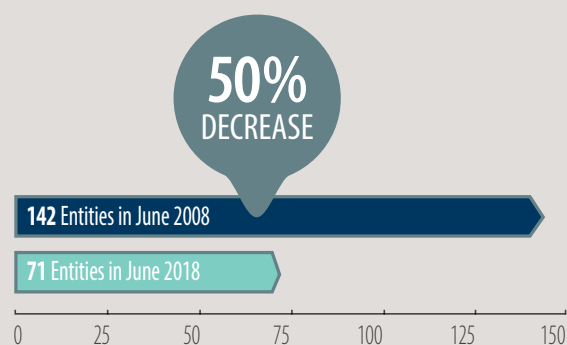
BACKGROUND

For the purpose of this report, mutuals are approved deposit-taking institutions (ADIs) that are owned by their customers, such as mutual banks, building societies and credit unions. Due to this ownership structure, mutuals return profits to their customers rather than distributing them to shareholders. Mutuals describe their heritage as one of service to a particular community or in support of customers in a particular industry, trade or profession.

Thirty years ago there were several hundred mutuals in Australia. Rapid consolidation and mergers between mutuals reduced that number to just over 70. Over the next ten years, continuing merger activity is likely to result in fewer, but larger, mutuals.

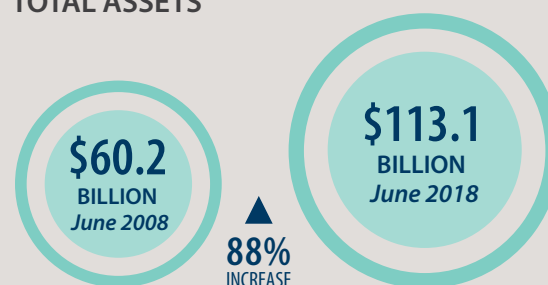
This risk assessment is intended to provide a summary and general overview; it does not assess every risk or product relevant to the mutual banking sector. It does not set out all of the obligations that mutuals have under the Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Act 2006, AML/CTF Regulations and AML/CTF Rules. It does not constitute nor should it be treated as legal advice or opinions. 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.

The mutual banking sector is consolidating¹

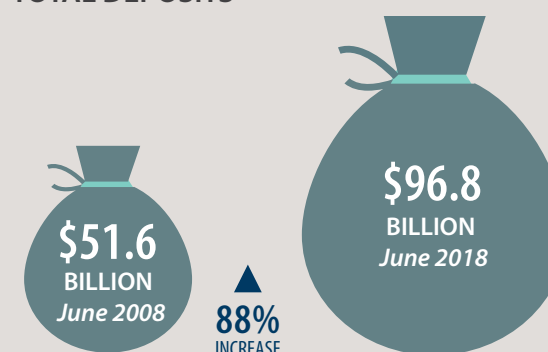


... while the sector itself is growing

TOTAL ASSETS



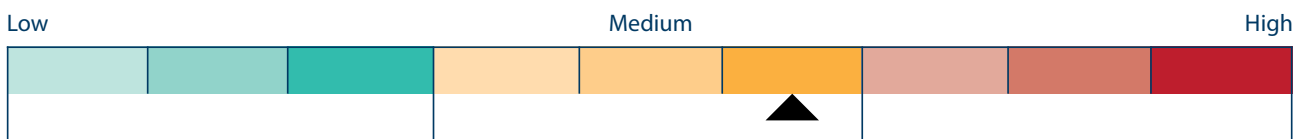
TOTAL DEPOSITS



¹ Data provided by the Australian Prudential Regulation Authority (APRA). APRA uses a slightly different definition of a mutual than that used in this report, however these figures are indicative of the changing size of the mutual sector over time.

EXECUTIVE SUMMARY

OVERALL RISK RATING



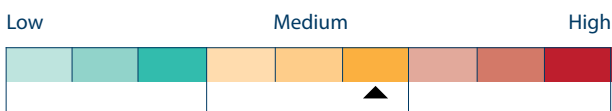
AUSTRAC assesses the overall money laundering and terrorism financing (ML/TF) risk associated with the mutual banking sector to be **medium**.

This rating is based on assessments of the criminal threat environment, the vulnerabilities in the sector, and the consequences associated with the criminal threat.

This assessment considers the risk associated with the mutual banking sector in the context of AUSTRAC's entire reporting population. Although some assessments draw comparisons to the broader banking sector for the purpose of illustration, this assessment should not be read as a direct comparison between mutuals and other ADIs.

AUSTRAC has also commenced a program of ML/TF risk assessments of the non-mutually owned banking sector, which will be of use to mutuals that wish to understand the comparative ML/TF risk profile.

CRIMINAL THREAT ENVIRONMENT



AUSTRAC assesses the overall ML/TF risk associated with mutuals' criminal threat environment to be **medium**.

Suspicious matter reports (SMRs) indicate the key threat faced by mutuals is money laundering, with substantial reporting activity detailing large and frequent cash transactions, transactions involving unknown third parties, and the rapid and complex movement of funds between financial products and institutions. However, having reviewed a sample of 2,000 SMRs submitted by mutuals, AUSTRAC considers many of these reports are highly likely to be trigger-based in nature, and describe legitimate, if unusual, transactional activity.

Due to the limited indication of actual criminality in many of the money laundering SMRs, AUSTRAC assesses the money laundering threat faced by the mutual banking sector is medium, despite the high number of SMRs.

Less than one half of one per cent of the SMRs in the dataset related to terrorism financing. Despite this, AUSTRAC assesses the nature and extent of the terrorism financing activity evident in the sector constitutes a medium risk. Key features of the terrorism financing risk facing mutuals is the use of charities and charitable donations to obscure illicit activity, as well as the risk of displacement of customers exited from non-mutually owned banks to the sector.

Forty-one per cent of sampled SMRs indicated activity related to predicate offending. While fewer SMRs indicated predicate offences than indicated money laundering, AUSTRAC assesses these SMRs are much more likely to relate to actual criminality than money laundering SMRs.

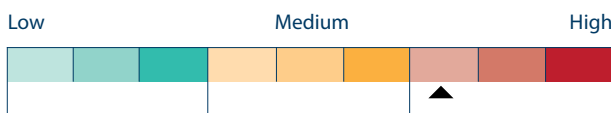
The predicate offences mutuals are most exposed to are frauds against individuals, including identity fraud and scams. Tax evasion and welfare fraud were also

evident in the sector, with some SMRs detailing large cash withdrawals suspected of being used to facilitate black economy payments.

Mutual banks noted that people holding powers of attorney or authorities to operate members' accounts appeared to be exploiting their account access for personal gain, including:

- Stealing from the primary account holder
- Using the primary account as a mule account to anonymise financial activity
- Attempting to access the primary account holder's government allowances after they had passed away.

VULNERABILITIES



AUSTRAC assesses the overall ML/TF risk associated with vulnerabilities in the mutual banking sector to be **high**.

Many of the factors leading to this assessment relate to the nature of banking products in general, and are not attributes specific to mutual banks.

The features that most expose the sector to financial crime include:

- The types of products offered by the sector, particularly transaction accounts with high levels of
 - o cash exposure
 - o access to international remittances, including with high-risk jurisdictions
 - o transactions by unknown third parties
- A high level of non-face-to-face service delivery
- High levels of outsourcing of customer-facing and AML/CTF processes, and limited oversight/influence over the operations of third-party service providers.

Mutuals with a bond to public service professions are also more likely to be exposed to the risks associated with integrity and corruption issues, including the misuse of public funds.

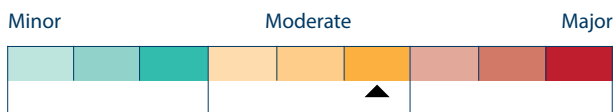
Other features that can expose the sector to vulnerability to financial crime include:

- The size of the customer base, including a moderate level of high-risk customers and an unclear source of funds for many transactions
- The risk mitigation systems implemented by the sector, such as
 - o the level of investment in AML/CTF systems and staff, limiting the effectiveness of risk assessment, transaction monitoring and suspicious matter reporting
 - o the quality of SMRs
 - o the clarity and oversight of outsourcing arrangements
 - o the use of off-the-shelf risk assessment and transaction monitoring tools that are not thoughtfully tailored to individual businesses.

Smaller mutuals may be less exposed to many vulnerabilities due to the lower value and number of transactions they facilitate. However, this benefit may be offset by less sophisticated systems and fewer resources to invest in proactive risk mitigation.

As the mutuals sector expands, the scale and complexity of its customer base, product offerings and delivery channels will also increase. Unless well-managed, increasing scale and complexity will also increase the sector's vulnerability to criminal exploitation. Mutuals need to continually review their systems and controls to ensure they remain adequate in relation to their changing profile.

CONSEQUENCES



AUSTRAC assesses the consequences of ML/TF activity in the mutual banking sector to be **moderate**.

These can include:

- personal loss and emotional distress for customers
- for mutuals, loss of revenue and capital from fraud, higher insurance premiums, reputational damage and heightened regulatory attention
- increased predicate offending affecting the community
- 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
- damage to Australia's international economic reputation as a safe and secure place to invest, and
- enabling and sustaining the activities of Australian foreign terrorist fighters, or enabling terrorist acts in Australia or overseas.

PURPOSE AND SCOPE

This risk assessment provides sector-specific information in relation to the ML/TF risks faced by the mutual banking sector. Its primary aim is to assist the sector to identify, understand and disrupt ML/TF and other criminal offences targeting Australia's financial system.

AUSTRAC expects mutuals will use this assessment to refine their own risk assessments, risk mitigation strategies and compliance controls. Information in this assessment should be applied in a way that is consistent with the nature, size and complexity of each mutual, and the ML/TF risk posed by each mutual's designated services, customers and delivery channels, as well as the foreign jurisdictions it facilitates transactions with.

The manner in which mutuals respond to the information in this report may be considered for future AUSTRAC compliance activities.

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. In this assessment:

Criminal threat environment refers to the nature and extent of ML/TF and relevant predicate offences in a sector.

Vulnerability refers to the characteristics of a sector that make it attractive for ML/TF purposes. This includes features of a particular sector that can be exploited, such as customer types, products and services, delivery channels and the foreign jurisdictions with which the sector deals. Vulnerability is also influenced by the risk mitigating strategies the sector has implemented.

Consequence refers to the impact or harm that ML/TF activity through the sector may cause.

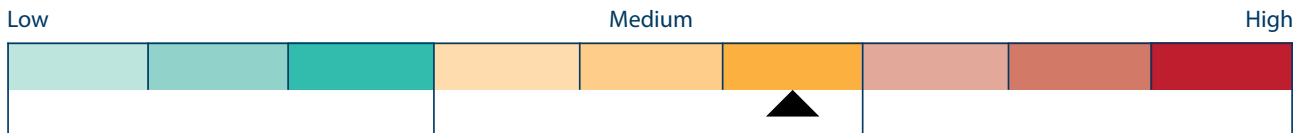
This assessment considered 19 risk factors across the above three categories. An average risk rating was determined for each category, and the average of each category determined an overall risk rating for the sector.

Further information on the methodology and how this was applied to the sector is in Appendix A.

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 mutuals, as well as industry experts, industry associations and key outsourced service providers.

CRIMINAL THREAT ENVIRONMENT



AUSTRAC assesses the mutuals sector faces a **medium** level of criminal threat, based on SMRs submitted by the sector and analysis of intelligence and information from AUSTRAC, partner agencies and industry.

The criminal threat environment refers to the nature and extent of ML/TF and predicate offences that are associated with the mutual banking sector.

To analyse the criminal threat environment faced by mutuals, AUSTRAC conducted an in-depth analysis of 2,000 SMRs randomly sampled from the total of 8,284 SMRs submitted by the sector in a two-year period.

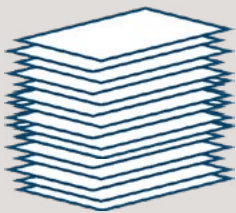
Suspected money laundering was the most common offence type indicated, with 67 per cent of SMRs observing potential money laundering attempts. Fraud against individuals was the next most commonly indicated offence type with 23 per cent, followed by tax evasion with 13 per cent, and welfare fraud with 5 per cent. Less than half of one per cent of SMRs submitted during the sample period were identified as being related to terrorism financing.

Four per cent of SMRs in the sample did not fit any of these categories. These SMRs captured a range of issues including customers behaving suspiciously at branches and customers appearing to use their account with the mutual to provide remittance services, including with high-risk jurisdictions. A small number of SMRs also indicated accounts with mutuals were being used to facilitate digital currency exchange (DCE) services, though these SMRs described activity prior to the commencement of AML/CTF regulation of DCEs.

Several SMRs in this cohort could not be categorised because the SMR itself contained insufficient information to apply a likely threat type.

REPORTING BY MUTUALS

SMRs submitted to AUSTRAC by mutuals from 1 July 2016 to 30 June 2018.



8,284

SMRs submitted with a total amount of



73 mutuals submitted at least one SMR

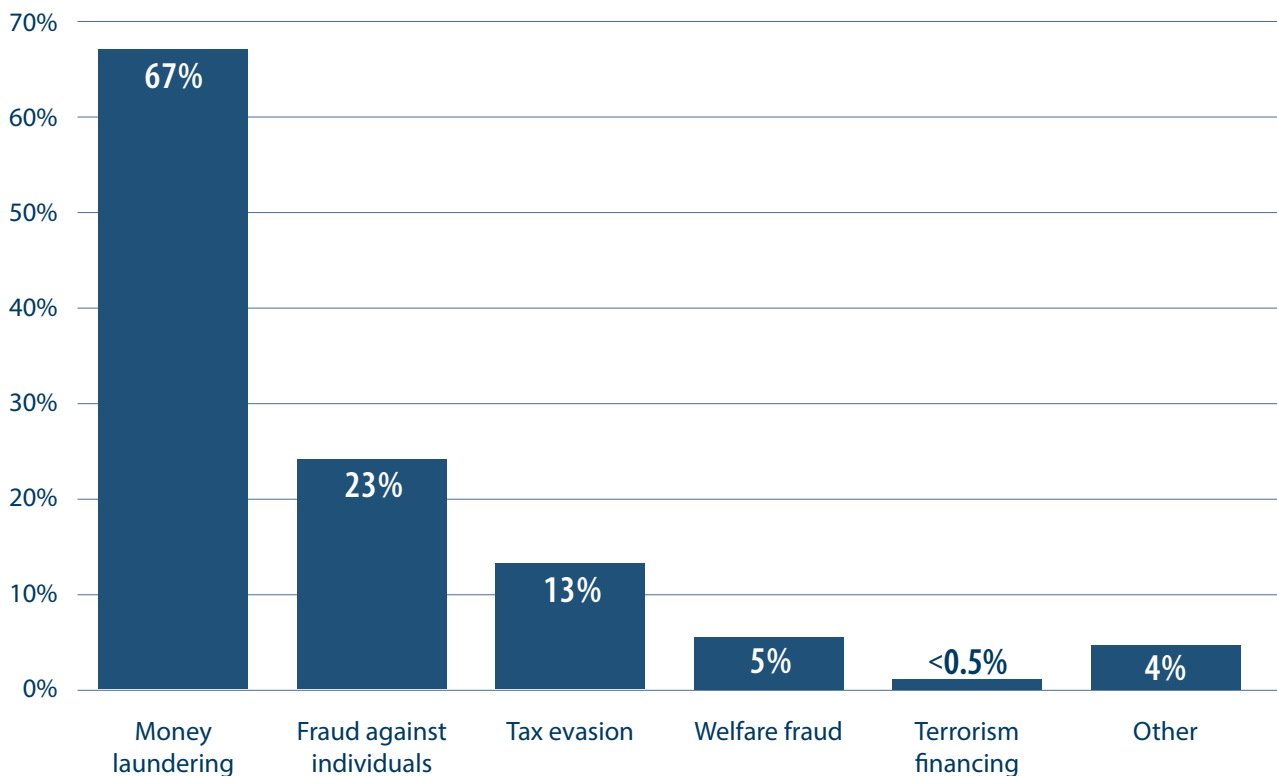
18 mutuals submitted 100 or more SMRs

5 mutuals accounted for 50 per cent of the SMRs submitted

7 mutuals did not submit any SMRs during the sample period.²

² These figures relate to entities that were in the sector when AUSTRAC commenced development of this risk assessment, at which point there were 80 mutuals in the sector.

SUSPECTED OFFENCE TYPES REPORTED BY THE MUTUAL BANKING SECTOR IN SMR SAMPLE



Note: many SMRs showed more than one suspected offence type.

SUSPICIOUS MATTER REPORTS PLAY A CRUCIAL ROLE IN LAW ENFORCEMENT

SMRs submitted by mutuals provide valuable intelligence to AUSTRAC. Working with its partner agencies, AUSTRAC pieces together intelligence from a range of sources to develop a picture of criminal activities and networks. Many of AUSTRAC's partner agencies – including the Australian Federal Police (AFP), Australian Criminal Intelligence Commission (ACIC) and the Australian Taxation Office (ATO) – have access to SMRs in order to generate leads and conduct further analysis and investigation.

MONEY LAUNDERING

AUSTRAC assesses the nature and extent of the money laundering threats facing the mutual banking sector to constitute a **medium** risk.

Money laundering accounted for the greatest number of SMRs of all criminal threat types, and related predominantly to cash and transaction account-based services. Despite the relatively high number of money laundering SMRs, the money laundering threat facing the mutual banking sector is assessed as medium because a large number of SMRs in this cohort appeared to be solely trigger-based.³

Of the 2,000 SMRs reviewed, 67 per cent included indicators of money laundering, with the most common indicators being:

- attempts to avoid reporting obligations by **structuring** large cash transactions into several smaller transactions of less than \$10,000 (28 per cent of the sample)
- customers making **multiple** cash deposits or withdrawals (23 per cent)
- customers making **large** cash deposits or withdrawals (21 per cent). A number of these SMRs detailed cash amounts in excess of \$100,000 in a single transaction
- the unusually **rapid movement** of funds in a manner that was not logical or expected (10 per cent).

Transactions described in money laundering SMRs were often conducted by somebody other than the customer and involved an unclear source of funds, increasing the suspicious nature of the transactions.

One mutual consulted for this risk assessment also advised they had observed account openings by local and overseas criminal syndicates. This is supported by AUSTRAC's analysis of SMRs submitted by mutuals, which showed that serious criminals known to government intelligence agencies are transacting through the sector, either as customers or parties to transactions.⁴

REPORTING BY MUTUALS - A PIECE OF THE INTELLIGENCE PUZZLE

Criminals often spread their financial activity across several entities to avoid raising suspicion. Many of the serious criminals about whom mutuals reported SMRs were also the subject of transaction reporting by other reporting entities such as banks and casinos.

SMRs submitted related to suspected proceeds of crime, money laundering, tax evasion and identity fraud, with many reports including structured and large cash activity, the use of third parties to conduct financial activity, and frequent and high-value domestic transfers.

It is important for mutuals to make reports to AUSTRAC even if they do not have comprehensive oversight over a customer's financial activity. SMRs form a 'piece of the puzzle' that, when combined with reporting from other entities, may assist law enforcement to develop a full picture of a customer's activity and consider escalation.

³ Trigger-based reporting is discussed further in the Risk Mitigation Systems section of Vulnerabilities.

⁴ AUSTRAC extracted the party names associated with SMRs lodged by the mutual banking sector over a two-year period, and compared these with names on externally-held criminal indices. Eighteen matches were found. AUSTRAC then searched across all SMRs lodged by any reporting entity for other SMRs relating to these 18 customers. 87 SMRs had been submitted by major banks, mutuals and gambling providers in relation to these 18 customers.

TERRORISM FINANCING

AUSTRAC assesses the nature and extent of the terrorism financing threats facing the mutual banking sector to be **medium** risk.

In particular, there is some evidence that entities who pose a high risk of terrorism financing may be turning to mutuals after a period of transacting with other banks.

SMRs demonstrate mutuals have customers with reported links to terrorist activity. Mutuals became aware of these links when the customer appeared in media reports or sanctions lists, or when they were approached for information about the customer by law enforcement.

While these SMRs confirm persons suspected of terrorism-related activities bank with mutuals, it was not always clear the mutual was actually used by the member to fund terrorism. Comparative analysis of SMRs submitted by mutuals and other banks does indicate that customers who pose a terrorism financing risk may be attempting to open accounts with mutuals at or around the same time non-mutual banks have submitted SMRs, highlighting TF-related suspicions about those customers.

While the non-mutual banks have not always explicitly reported an intention to close the customer's account, the absence of subsequent suspicious matter or transaction reporting about the customer indicates mutuals may be targeted by displaced terrorism financiers.

SMRs also demonstrate that mutuals' customers that are charities, or customers who use their bank accounts to donate to purported charities, expose mutuals to terrorism financing risk. Illegitimate charities and charitable donations can be very difficult for mutuals to detect; the reason being, that legitimate philanthropic activities may have a similar transactional footprint as terrorism financing. For example, an account receiving various small deposits/donations from different third parties and transferring accumulated funds to high-risk jurisdictions can be indicative of legitimate charitable activity, but it is also how someone may raise and move funds to support offshore terrorist activity.

Further information about the charity sector, including ML/TF risks, can be found in AUSTRAC's [Non-profit Organisation Sector Risk Assessment](#), and the Australian Charities and Not-for-profits Commission [website](#).

As well as analysing SMRs, AUSTRAC interrogated the intelligence reports it generated in relation to the customers of mutuals who were the subjects of SMRs. Over a two-year period, eleven tactical intelligence reports linked customers of mutuals with terrorism financing, seven of which related to the same individual and a questionable charitable organisation with which he was connected. Only one of these reports indicated the customer was actually using the mutual to facilitate terrorist funding. This matter was referred to relevant law enforcement agencies.

AUSTRAC undertook data matching between partner agency data and transaction reports lodged by mutuals. While data matching activities did not find any significant concerns relating to terrorism financing within the mutual banking sector, mutuals need to remain vigilant with respect to their customer identification and ongoing due diligence procedures, including checking against watch lists and media monitoring.

PREDICATE OFFENCES

AUSTRAC assesses the nature and extent of the predicate threats facing the mutual banking sector constitute a **high** ML/TF risk.

While fewer SMRs were submitted by the sector in relation to predicate offences than money laundering, sample analysis indicated that SMRs describing predicate offences was more likely to relate to genuine illicit activity. Consultations with industry also indicate that cyber-enabled fraud is not uniformly reported across the sector, so is likely to be under-represented in the sample. Further, intelligence reports generated about the customers of mutuals reported in SMRs was more likely to relate to fraud and scams than to money laundering.

AUSTRAC identified a variety of predicate criminal threats including scams, identity fraud, welfare fraud and tax evasion.

FRAUD AGAINST INDIVIDUALS

Twenty-three per cent of the SMRs in the sample group indicated possible fraud against individuals, with the most common fraud types being scams and identity fraud. Other forms of fraud included cheque fraud, providing false information in loan applications, and third party theft from customers' accounts.

Identity fraud

Nine per cent of SMRs in the sample related to the use of a false identity. The majority of these SMRs related to online account openings.

Several mutuals reported SMRs in which fraudsters used stolen identity information to open accounts that may then have been used to launder or move the proceeds of illicit activities. Mutuals also reported cases in which customers discovered that accounts had been opened using their details without their knowledge after having been contacted about the account by the mutual. This shows how processes to contact new members can assist mutuals to protect themselves from exploitation. In some instances, several account openings – using identical personal details – would occur concurrently. One mutual noticed that when several accounts were opened with false identity information, the criminal would often use the same answers to security questions across all of the accounts.



CASE STUDY: LARGE-SCALE IDENTITY FRAUD

One mutual discovered a large-scale identity fraud, in which many of its customers had been defrauded. The mutual observed online account openings for 13 different customers, several of which had common residential addresses. The accounts received funds from payday lenders specialising in fast online loan applications, and the funds were transferred to a single account at another financial institution.

Upon further investigation, the mutual discovered these 13 customers were being impersonated by a team of three fraudsters who had gained access to their personal information. The fraudsters used stolen identities to establish the accounts, and then applied for loans under the victims' names from payday lenders, with no intention of repaying the funds.

The mutual immediately froze the accounts, increased the customers' risk ratings, and commenced closing the fraudulent accounts.

During consultations with AUSTRAC, some mutuals noted transactions of very low amounts may indicate identity fraud activity. For example, a criminal would open an account using stolen identity details, then test whether the account was functional by transferring a very small amount of value into the account. The criminal may then use the account themselves or sell the account details on the black market. AUSTRAC also received feedback that micro-transactions may be used to confirm an account is active prior to receiving a fraudulent tax refund.

One mutual consulted observed a significant increase in the use of mobile phone diversions to enable fraudulent activities. This occurs when a perpetrator is able to gather sufficient details about a customer to port their mobile phone to a new provider. The perpetrator is then able to receive the confirmation text messages and calls from the mutual, confirm the account and then carry out transactions without the victim becoming aware.

CYBER-ENABLED FRAUD

Cyber-enabled fraud was a common feature in SMRs relating to identity fraud, scams, money mules and unauthorised card transactions.

Cyber-enabled fraud refers to crimes where computers or information communications technology are an integral part of an offence, such as online identity theft.

Cyber-enabled fraud was indicated in 8.5 per cent of SMRs in the sample; however, AUSTRAC assesses the actual volume of cyber-enabled fraud is likely to be much higher. Given the mutual sector's significant online presence, it is highly likely that scammers use account hacking and email phishing to facilitate scams and identity fraud in the sector.

Several mutuals engaged during the development of this risk assessment noted they were not aware that cyber-enabled fraud was reportable under the AML/CTF regime, which is likely to further account for the limited reporting on this threat by the sector.

It is important that mutuals' fraud and financial crime teams work together to ensure each has a robust understanding of the way cyber-enabled fraud is affecting the business. For tips on SMR reporting, see the Risk Mitigation Systems section of this document.

Scams

Six per cent of SMRs in the sample indicated scam activity, including romance scams, employment scams, malware and false billing scams. In these reports, mutuals often indicated they had gone to significant efforts to warn customers they were being scammed. In many cases SMRs note these warnings went unheeded – the customer preferring to believe they were not being scammed.

In most of the scam-related SMRs, the customer was the victim of the suspected scam. In a smaller number of SMRs, the customer appeared to be implicated in committing scams against others. In some cases, the customer knowingly allowed their account to be utilised by third parties, but were not aware that transacted funds were the proceeds of scams.

USING SCAMS TO RECRUIT MONEY MULES

One mutual AUSTRAC consulted for this risk assessment described an increase in money mule activity, and SMRs from mutuals indicated that customers are being scammed into being mules for money laundering.

Several SMRs in the dataset related to customers accepting jobs on employment websites, where the “job” was essentially to launder illicit funds through their own account to distance the scammers from illegal activity. Victims were often unaware of the illicit nature of the funds they were handling.

Some examples include:

- A mutual was notified by the fraud team of another bank that it had intercepted two payments totalling over \$150,000 which were destined for the customer’s account. The mutual’s investigation revealed the customer had accepted an online job offer as an “operations assistant”, for which their duties included “processing” these remittances.
- A customer requested a mutual to transfer several thousand dollars to a recipient in Nigeria. The mutual found the request suspicious due to the destination of the funds; the fact the customer was unemployed; and because the funds did not originate from the customer’s account (indicating possible mule activity).
- A mutual was notified by another bank that one of its customers had fallen victim to a scam and was sending money to the mutual. The mutual’s customer, who had fallen victim to a romance scam, had been tricked into receiving the scammed funds and storing them in his account with the mutual.

Welfare fraud

Five per cent of SMRs in the sample indicated possible welfare fraud. Mutuals described a number of scenarios that indicated possible welfare fraud, including:

- transactions inconsistent with the expected profile of a customer receiving Centrelink benefits, such as pensioners making large cash transactions, or requesting large international transactions
- customers receiving government benefits, but also receiving employment income which the mutual suspected they may not be declaring to Centrelink
- customers receiving government benefits without withdrawing the funds, indicating they were living off another source of (likely undeclared) income
- customers providing information on applications for credit that caused the mutual to develop the suspicion they were not declaring income to Centrelink
- customers making cash withdrawals from their savings account to ensure they would meet asset test requirements for government allowance eligibility. In many cases, customers actually articulated this intent to the teller facilitating the transaction.

Tax evasion

Thirteen per cent of SMRs in the sample were identified as relating to potential tax evasion. Tax evasion SMRs were more likely to involve cash transactions than other threat types (86 per cent of tax evasion SMRs involved cash, compared to 66.5 per cent for the whole sample).

Some indicators in tax evasion-related SMRs included:

- large cash payments into and out of customers' accounts, especially business-related payments and accounts
- large cash withdrawals to pay building and home renovation expenses, enabling the tradesperson to collect cash-in-hand payments and avoid tax
- customers providing inconsistent income details in home loan applications that indicate potential undeclared income.

In addition to SMRs, a matter that AUSTRAC considered in 2018 found that a mutual was one of a number of banks from which significant cash, suspected of being associated with cash wage payments and possible phoenixing, was being withdrawn.

THE BLACK ECONOMY TASKFORCE

In December 2016, the Australian Government established the Black Economy Taskforce to provide recommendations on how to address activities which take place outside the tax and regulatory system,⁵ including:

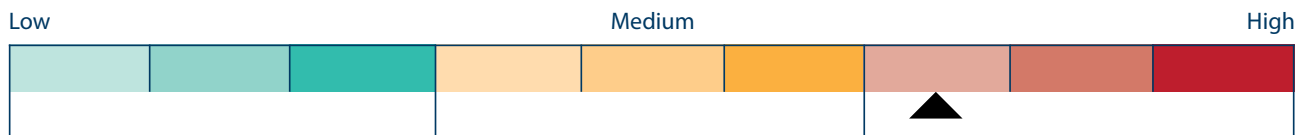
- non-reporting or under-reporting of income for tax purposes
- cash-in-hand wages
- identity fraud, and
- money laundering.⁶

As businesses with significant cash exposure, mutuals need to be aware of the role their cash transactions can play in facilitating the black economy, and ensure they implement measures to mitigate the harms the black economy can cause.

5 https://static.treasury.gov.au/uploads/sites/1/2018/05/Black-Economy-Taskforce_Final-Report.pdf p 12

6 Ibid p 13-14

VULNERABILITIES



AUSTRAC assesses the mutual banking sector is subject to a **high** 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 sections: customers, products and services, delivery channels, exposure to foreign jurisdictions and level of implementation of risk mitigation strategies.

CUSTOMERS

AUSTRAC assesses the mutuals' customer base overall presents a **medium** level of ML/TF vulnerability.

The sector has a sizeable and diverse customer base, and many SMRs reported concerns about customers' source of funds and wealth. However, mutuals tend to provide services predominantly to individual customer types, which generally pose a lower risk.

CUSTOMER BASE

Four million Australians and businesses bank with mutuals, holding some \$101 billion in deposits and \$119 billion in assets.⁷ The size of the customer base increases the sector's exposure to ML/TF exploitation.

The mutual banking sector's customer base is predominantly composed of individuals, including sole traders. Individuals can pose a lower ML/TF risk than corporate or trust customers, because there is less scope to obscure beneficial ownership or the purpose of transactions when customers are acting on their own behalf.

Mutual banks have a relatively uniform customer profile due to their historical "bond". Most mutuals originated as smaller credit unions and building societies that provided financial services to people of specific employment groups or residing in a particular geographic area.

Although many mutuals no longer restrict their customer base to those within their historical bond, their customer profiles still partly reflect this. Such customers often have relatively consistent transaction patterns, making deviations easy to identify and report on. Mutuals that focus on customers in a particular geographical area, on the other hand, tend to provide banking services to a more diverse range of customers in terms of their occupations, income levels, sources of funds and general behaviours. As a result, unusual activity may be harder to identify in location-based mutuals than it is in occupations-based mutuals.

Some mutuals engaged for this assessment continue to pursue a membership strategy which focuses on their historical bond, while other mutuals are looking to expand into the general marketplace, thus diversifying their membership base, and in some cases competing with larger ADIs. Such mutuals are likely to be exposed to a greater and more diverse range of ML/TF risks posed by their customers.

⁷ Customer Owned Banking Association, <http://www.customerownedbanking.asn.au/media-a-resources/key-stats-a-fact-sheets>

BUSINESS CUSTOMERS

Certain business customers may appear to pose an unacceptably high risk to mutuals based purely on the type of business activity they are engaged in. However, in many cases and with appropriate AML/CTF systems and controls in place, mutuals should be able to manage customers they deem to be high risk. It is important AUSTRAC encourages mutuals to continue to assess the particular risks relating to their customers in line with the risk-based approach.

One of the mutuals consulted by AUSTRAC conveyed they chose to retain – rather than de-bank – the remitter customers it inherited due to a merger. The mutual described the due diligence it applied to these customers including site visits, meetings, and review and assurance around the remitters' programs, transaction monitoring and independent reviews.

HIGH-RISK CUSTOMER TYPES

Over half of the entities in the mutuals sector reported in their 2018 Compliance Report having high-risk customers such as companies, trustees, partnerships and associations, registered cooperatives and government bodies.

Trusts held with mutuals include trust accounts for real estate agents and solicitors. Mutuals have limited or no visibility of the beneficial ownership or source of the funds moving through these trust accounts because the funds are often beneficially owned by the customer of the trust, rather than the mutual's customer.

AUSTRAC recommends mutuals apply heightened due diligence to trust accounts to satisfy themselves they have processes in place to identify transactions that are likely to be illegitimate, particularly large cash transactions. Other trusts held with mutuals include family trusts, accounts held in trust by parents on behalf of minors, and other trusts such as self-managed superannuation fund trusts.

Moreover, individuals' accounts that are associated with powers of attorney or third-party authorities increase the potential for anonymity and therefore carry higher ML/TF risk.

POLITICALLY EXPOSED PERSONS (PEPS) AND OTHER PUBLIC OFFICIALS

Several mutuals consulted for this risk assessment advised they had politically exposed persons (PEPs) among their customers, and just over half reported having PEPs in their 2018 Compliance Report.

PEPs are attractive targets for bribery and corruption due to their ability to award valuable contracts and make other significant decisions in relation to the exercise of government power. As such, reporting entities have heightened obligations in relation to PEPs.

SMRs from the sample dataset included instances of PEPs receiving multiple cash deposits.

Several mutuals have a bond to publicly-funded professions, and professions that wield the power of government. While these customers' positions may not be sufficiently senior to constitute the status of a PEP, they may still have access to substantial government money or decision-making delegations that criminal individuals or groups would pay to have influence over.

SMRs received by AUSTRAC indicate that some mutuals are aware of this risk and have adjusted their systems accordingly.

AUSTRAC recommends that all mutuals with a bond to government employees and/or other customers that have a high level of political exposure implement sensitive systems to monitor customer behaviour, identify questionable sources of funds, as well as processes to follow when legitimacy cannot be established.

There were a number of scenarios in which mutuals may allocate a customer a higher risk rating and retain such customers. These include customers who:

- hold a non-traditional occupation
- live a long distance from their nearest branch
- demonstrate unusual transaction behaviour
- had fallen victim to internet scams.

Mutuals told AUSTRAC that scam victims were often identified as high-risk to ensure heightened monitoring of their activity – both to protect them from future exploitation and also to monitor for instances in which the customer may be unknowingly involved in money mule activity.

CUSTOMERS' SOURCE OF FUNDS AND WEALTH

SMRs demonstrate a key challenge faced by the mutual banking sector is establishing the legitimacy of the source of the funds used by members. Mutuals generally do not have oversight over the source of funds deposited by unknown third parties, including via third-party billers, or by their real estate agent or solicitor customers into trust accounts. In 24 per cent of the sampled SMRs, mutuals indicated transactions were inconsistent with the customer's profile. Many of these SMRs related to suspected money laundering activity, with identity fraud and tax evasion also featuring prominently.

AGENTS AND OTHER THIRD PARTIES

Although the full extent of customers' use of agents and third parties in the mutual sector is unclear, AUSTRAC's analysis of SMRs and feedback from mutuals indicates it is a vulnerability that could be exploited by criminals to obscure their identity and distance themselves from their illicit activity. Agent risk can arise where agents – such as solicitors, accountants, and financial planners – act on behalf of a customer through a formal agency arrangement, creating opportunities to use others' accounts to conduct illegitimate transactions. Third-party risk can arise when unknown third parties, or persons holding powers of attorney or authorities or operate, are able to transact on others' accounts.

The SMR dataset contained many examples of unknown third parties making deposits into customers' accounts raising difficulties in terms of establishing source of funds. Many of these were linked to suspected money laundering activities, particularly mule accounts (as described in the section above on money laundering). One mutual noted it had observed a financial planner co-mingling their client's money into the planner's own personal account.

SMRs also indicated exploitation of power of attorney, signatory and trustee relationships to either:

- defraud primary customers
- engage in welfare fraud, or
- conduct financial activity through other people's accounts to hide activity from the ATO.

In these SMRs, mutuals noted the primary customer was often vulnerable in some way – such as being ill or elderly – and in some circumstances the mutual believed the primary customer to be deceased.

In one SMR, the mutual reported its customer was seriously ill and was approached by a person seeking power of attorney. The person seeking power of attorney wanted to know if he would be able to make blank cheques signed by the customer payable to himself after her death. As the Australian population ages, mutuals are likely to face increasing instances of elder abuse and will benefit from systems and controls to help them identify these cases and protect their more vulnerable members.

USING THIRD-PARTY AUTHORITY FOR TAX EVASION AND WELFARE FRAUD

SMRs submitted by mutuals indicate some people may be exploiting their third-party authority to operate customers' accounts to avoid taxation obligations or engage in welfare fraud. Mutuals described a number of instances indicating this was occurring:

- A five year-old customer whose account was used to pay business invoices in a likely attempt to hide business activity from the ATO.
- An 11 year-old customer whose account received large cash deposits, where a person with authority to operate the account was receiving Centrelink benefits.
- Two days after a mutual received information that a customer had passed away, the customers' Centrelink allowance was withdrawn in cash using her bank card, possibly by the person who was a signatory to the account.
- The daughter of a customer, who had authority to operate her father's account, made structured withdrawals to avoid the government's means-testing for welfare payments. She advised the mutual she had been struggling to find an affordable aged care solution for her father due to the value of his home.

PRODUCTS AND SERVICES

AUSTRAC assesses the nature of the products and services offered by mutuals pose a **high** ML/TF risk.

Mutuals offer a variety of banking products and services for individuals and sole traders, and a more limited range of products and services for companies and other non-individual customers. Products offered by mutuals which constitute a high exposure to ML/TF risk include transaction accounts, international funds transfers, and large cash transactions. However, some of this risk is partially mitigated in cases where mutuals have lower product caps and transaction limits on their products than other financial service providers.

TRANSACTION ACCOUNTS

Transaction accounts pose a very high ML/TF risk; they are among the most commonly misused financial products for financial crime and appear in a wide range of established money laundering methodologies.

More than two-thirds of the SMRs in the sample involved the use of transaction accounts. They were frequently associated with suspicions of money laundering through structuring and making large and/or frequent deposits and withdrawals. They were also associated with possible tax evasion, as cash deposits and withdrawals alerted the mutual to potential black economy cash trading. Transaction accounts were also key vehicles for fraud activities including identity fraud and scams.

Transaction accounts can be used:

- to place the proceeds of crime in-branch and, in some cases, through ATM deposits
- in the layering and/or integration stages of money laundering, particularly when electronic transfers and third-party billing are available
- to allow the proceeds of crime to be safely stored for long periods of time
- to facilitate the rapid movement of criminally-derived funds, particularly when online banking and international remittances are available
- to facilitate fraudulent activities such as identity theft and voluntary and involuntary muling
- to generate complex chains of transactions, making beneficial ownership and the ultimate beneficiary of transactions difficult to establish.

MUTUALS' TRANSACTION ACCOUNTS USED BY MULES

One SMR described a member opening an account with a mutual, advising they had chosen this particular mutual on the advice of a "friend". The member advised the mutual that they were unemployed.

In the following months, the member's accounts received several small deposits from other bank accounts, then quickly transferred into an external account held by a corporate and trust registry service provider. After each transaction, \$1 was left in the mutual account. The mutual began to suspect these were test transactions, which could cumulatively constitute the member's reward for muling.

Subsequently, the mutual was alerted that another bank had intercepted a large, illegitimate transfer intended for the member's transaction account. The mutual contacted the member, who claimed to be investing in bitcoin, but was unaware of the amount he was about to receive. The mobile number the member provided also appeared to be false, and the mutual formed the view that the member did not have a genuine reason for banking with them, so froze the account.

Such arrangements show how members' transaction accounts can be used in money laundering activities – in this instance it was unclear if the customer was aware they were involved in illicit activities.

The money laundering risk of transaction accounts may be less pronounced for smaller mutuals that have a more limited number and value of transactions, because the transactional activity required to sustain large-scale money laundering would be more easily identifiable against a background of smaller transactions.

However, the changing profile and scale of some mutuals will increase their exposure to larger, legitimate transactions that could be used to obscure the transactions of illegitimate actors. This will be particularly true for mutuals seeking to expand beyond their traditional customer base. Mutuals will need to ensure their AML/CTF systems and controls are able to keep pace with their changing nature, size and complexity.

USE OF CASH

As the proceeds of crime are often derived in cash, which is very difficult to trace, a reporting entity's exposure to money laundering placement risk significantly increases when facilitating a large volume and high value of cash transactions. This risk is further increased if the reporting entity also provides services in which cash, once deposited, can be moved between domestic accounts or to offshore accounts.

Cash is also a key facilitator of the black economy and tax evasion.

Mutuals have an obligation to report physical cash transactions of \$10,000 or more through threshold transaction reports (TTRs). Despite the increasing use of electronic banking, many mutual banks facilitate a significant value and volume of cash transactions.

TTRs submitted by mutuals to AUSTRAC from 1 July 2016 to 30 June 2018:

- **106,652** TTRs involving a total cash value of over \$1.7 billion
- **77** mutuals submitted at least one TTR
- **7** mutuals accounted for half of the TTRs submitted⁸

Given these figures only include transactions of \$10,000 and above, combined with the high incidence of SMRs indicating structuring to avoid threshold reporting obligations, the figure of \$1.7 billion understates the sector's exposure to cash.

Sixty-seven per cent of SMRs in the sample included references to the use of cash, with many indicating structuring to avoid threshold reporting obligations. Large or multiple transactions, rapid movement of funds and tax evasion were the other key threats indicated in cash-related SMRs.

Of particular note was the large number of cash-related SMRs in which customers advised they were withdrawing cash to pay tradespeople to renovate their homes. Some customers even noted the tradesperson had advised them that if payment was made in cash, they would charge a lower price for their work. Some large cash withdrawals were also justified by customers on the basis of being the payment price for a vehicle.

While in both of these cases any proactive tax evasion was on the part of the vendor rather than the member, mutuals need to remain aware the large cash transactions they facilitate may be contributing to the black economy and ensure they have the systems and controls to manage this risk, including appropriate suspicious matter reporting procedures.

Some mutuals described the policies they had implemented that helped to restrict the exposure they faced to the risks of cash. These included:

- having relatively low daily cash withdrawal limits on ATMs, and often not accepting cardless transactions or cash deposits into ATMs
- requiring that deposits and withdrawals in cash over a certain threshold be arranged in advance
- operating cashless branches.

⁸ These figures relate to entities that were in the sector when AUSTRAC commenced developing this risk assessment, at which point there were 80 mutuals in the sector.

LOANS AND CREDIT CARDS

Thirteen per cent of the SMRs in the sample related to loans, including loan applications and credit cards.

The misuse of loans is a well-established money laundering methodology. For example, loans can be fraudulently established and the funds stolen. One SMR in the dataset described a reporting entity's suspicion that its member had established a property loan for a property that did not, in fact, exist. Loans (legitimately or fraudulently established) can also be repaid or offset in part or whole with the proceeds of crime, as indicated in an SMR in which a mutual suspected the member was repaying a loan with structured cash deposits.

Further, repayment of commercial loans offers opportunities to co-mingle illegitimately obtained funds with legitimate business income, thereby transforming proceeds of crime into valuable, income-producing assets the business borrows money to buy, such as physical capital.

Almost half of the SMRs in the sample were about loans related to credit cards. Like other loans, credit card accounts can be set up with stolen identity information or paid off with criminal proceeds. SMRs relating to credit card accounts were often associated with large or multiple deposits, loan fraud, identity fraud and cyber-enabled fraud. In particular, customers' credit card accounts were often used to receive third-party biller deposits which put the account into credit. Funds have then been rapidly moved between accounts and often are ultimately transferred to another financial institution.

INCREASED DUE DILIGENCE FOR LOAN APPLICATIONS

Loan applications provide reporting entities with customers' employment details and information relating to other sources of income. Mutuals can use this information to inform their understanding of their customer's risk profile, as well as their source of funds and wealth for future monitoring.

Loan applications can also indicate customers who may be engaged in welfare and tax fraud, by uncovering undeclared income sources and inconsistencies between loan applications and supporting documents, such as:

- relationship status
- existence/number of dependents
- home ownership status.

Almost three per cent of SMRs in the sample related to loan application fraud, and several of these also indicated cyber-enabled fraud, identity fraud and welfare fraud.

AUSTRAC encourages mutuals to use the documentation customers provide in support of loan applications to support ECDD, and include relevant details from the application in any SMRs they may make about the customer/prospective loan applicant.

INVESTMENT PRODUCTS

Mutuals offer relatively simple investment products such as high-yield savings accounts and term deposits. These products are configured in different ways across the mutuals sector.

In general, high-yield savings accounts operate in much the same way as transaction accounts, except they are associated with incentives such as higher interest rates and early withdrawal penalties to encourage members to deposit heavily and withdraw sparingly. They are also less likely to be associated with debit cards than normal transaction accounts, making them less vulnerable to ML/TF as they discourage the rapid movement of funds. However, overall there is still significant scope to deposit, move and access money at short notice using these products meaning they pose a tangible ML/TF risk.

Term deposits, on the other hand, do pose a lower level of risk than many of the other products mutuals offer because of the inflexibility in accessing and moving value.

Twenty-nine SMRs in the sample included reference to a term deposit. Suspicions were generally based on the use of large cash deposits to establish term deposits, large cash withdrawals from (often immature) term deposits, transactions on term deposits held by Centrelink recipients, and insistence on taking large withdrawals from term deposits in cash. Moreover, the source of funds was often cited as unclear, and offers to provide funds via non-cash means such as electronic transfer or bank cheque were often refused.

OTHER WEALTH PRODUCTS PROVIDED BY MUTUALS

Some mutuals are designated service providers in relation to the provision of financial advice under an Australian financial services licence and/or superannuation. AUSTRAC encourages mutuals that offer these products to review AUSTRAC's suite of ML/TF risk assessments.

Financial planning

AUSTRAC's [risk assessment into the financial planning sector](#), found that the sector faces a variety of threats involving sophisticated tactics and methods. Cyber-enabled fraud is a particular threat to the sector, growing in scale and sophistication. AUSTRAC also developed a [Financial Crime Red Flags](#) poster, to assist staff who provide financial advice and financial planning services can use to detect criminal activity.

Superannuation

Superannuation offers a means for criminals to "park" the proceeds of crime to secure long-term gains. AUSTRAC's [risk assessment into Australia's superannuation sector](#) found the size of the superannuation sector makes it an attractive target for money laundering and predicate offences. Customers' limited engagement with their accounts, and the limited ability to identify source of funds are some of the factors that make superannuation more vulnerable to financial crime. AUSTRAC has also published [guidance for the superannuation sector](#) in response to requests from providers for information on how to apply their AML/CTF obligations.

INTERNATIONAL FUNDS TRANSFERS

Mutuals facilitate the movement of funds offshore. The movement of funds internationally constitutes a significant vulnerability for financial service providers, as it is linked to money laundering, terrorism financing, tax evasion, corruption, scams and fraud. SMRs submitted by mutuals in relation to international funds transfers included concerns that beneficiaries were high-risk for terrorism financing, and for possible scam activity.

Mutuals generally arrange for their customers' remittances to be sent or received by a third party as they do not have the infrastructure or relationships to facilitate the remittances themselves.

The process by which remittances are carried out for customers of mutuals varies between mutuals - generally the third party uses the customer identification details collected by the mutual as part of the mutual's customer on-boarding process. The third party then conducts its own screening of the customer, sends or receives the remittance, and reports the international funds transfer instruction (IFTI).

During consultations for this risk assessment, it became clear there were different views among mutuals, and between mutuals and relevant third parties, about which entity is considered to be the designated service provider in relation to remittances requested or received by members of mutuals. The alternate positions put forward were that:

- the designated service provider was the third party, which used the customer identification details collected by the mutual, or
- the designated service provider was the mutual, which outsourced the actual transmission of the remittance to the third party.

Under the AML/CTF Act, the designated service provider will be the entity that accepts the instruction to remit the funds or to make it available to the recipient. Depending on the exact nature of the agreement between the customer, the mutual and the third party, this could mean the third party or the mutual (or both) are designated service providers in respect of the remittance.

Given the inconsistent views expressed during consultations, AUSTRAC strongly encourages mutuals and their third party partners to review their agreements and the nature of their service delivery arrangements to ensure they have a common understanding of which entity is providing designated services and is a reporting entity under the AML/CTF Act.

AUSTRAC notes that, irrespective of any contractual arrangements between the parties, the reporting entity is ultimately responsible for meeting obligations under the AML/CTF Act in relation to the designated services it provides.

FOREIGN JURISDICTION EXPOSURE OF STORED VALUE CARDS

Stored value cards (SVCs) such as travel cards are a common way for individuals to move funds internationally. AUSTRAC's [risk assessment of SVCs](#) found they are used in money laundering typologies and are highly vulnerable to exploitation by terrorism financiers.

SVCs were also frequently implicated in cyber-enabled fraud, scams and tax evasion. Mutuals that act as issuers of SVCs should refer to this risk assessment to support their understanding of the ML/TF risk associated with SVCs.

DELIVERY CHANNEL

AUSTRAC assesses the delivery channels mutuals use to provide their services to their customers present a **high** ML/TF risk.

As well as having a significant network of ATMs across the country, the mutual banking sector has embraced online banking, banking apps and the New Payments Platform (NPP). Outsourcing of customer-facing services is also common in the mutuals sector, which creates ML/TF vulnerabilities.

BRANCHES

The mutual banking sector has a significant branch network, with an estimated 941 branches across Australia. Broadly speaking, face-to-face delivery channels present a lower risk than telephone or online banking as they limit the ability to obscure identity, and provide opportunities for reporting entities to observe behaviour and question the purpose of unusual transactions. It also provides greater opportunity for a mutual to develop closer customer relationships.

The value of the face-to-face delivery channel is demonstrated in SMRs. For example, SMRs describing large cash transactions contained more information when the transaction was conducted face-to-face than when it was conducted at a third-party shopfront or via an ATM. Mutuals were able to ask the customer about the purpose of the transaction and report on any suspicious, evasive or contradictory answers. When services are conducted face-to-face, it also gives mutuals enhanced opportunity to assess whether customers are making transactions voluntarily, or if they are acting on instructions from a third party.

On the other hand, many mutuals have expanded their branch network by allowing customers to utilise in-person banking services through other entities' shopfronts, expanding the size of this delivery channel several-fold. Several of the risk-mitigating characteristics of the face-to-face delivery channel, such as behavioural observation and closer customer relationships, can be undermined when provided by a third party.

CASH WITHDRAWALS FROM THIRD PARTIES

Several SMRs in the dataset described customers taking advantage of arrangements with third-party businesses that allow customers to conduct cash transactions on their bank accounts without having to visit a branch. SMRs indicated the maximum cash withdrawal limits allowed by the third party were being frequently reached.

While this was often associated with suspected attempts to avoid reporting obligations, concern was also raised in SMRs that customers were withdrawing from third parties in order to avoid the face-to-face scrutiny of branch staff. When customers withdrew large amounts of cash from third parties rather than at a branch, staff were unable to question them regarding the purpose of the withdrawals, limiting the amount of ECDD they could conduct.

AUSTRAC encourages mutuals to include what additional information they can in SMRs, for example the potential source of the funds the customer is withdrawing, even where the transaction is processed by a third party.

ONLINE BANKING

Mutuals are increasingly moving to online delivery channels, with the majority of mutuals already fully online.

The shift to electronic services is exposing mutuals to attempts at cyber-enabled fraud, such as online account opening and attempts to obtain financial benefits using stolen or fraudulent identities. Internet banking services also increase the speed with which funds can be moved between accounts and financial institutions, and ordering remittances online increases the speed and anonymity with which value can be moved offshore.

While a number of entities interviewed for this assessment indicated investments are being made to improve IT systems and improve cyber-security, an industry survey reported that one in ten mutuals felt that they were not prepared for a cyber-event.⁹

9 KPMG, Mutuals Industry Review 2017, KPMG, 2017, pg 40 <https://home.kpmg/au/en/home/insights/2017/11/mutuals-industry-review-2017.html>

FRAUDULENT ONLINE ACCOUNT OPENING

Fraudulent online account opening was a threat identified by a number of stakeholders engaged for this risk assessment.

Not all mutuals currently provide online account opening, but the continuing move to online operations was a broad theme of consultations and it is likely online account opening will become available across the entire sector in time.

Indicators of fraudulent online account opening discussed during consultations, and described in SMRs, included:

- addresses, phone numbers, customer details and answers to security questions that were common across a number of newly created accounts.
- illogical or nonsensical answers to customers' security questions, sometimes common across several accounts.
- the provision of contact details where email addresses and/or phone numbers were invalid/disconnected.
- addresses changed soon after account opening.

While some mutuals reported their customer verification procedures had, so far, prevented any significant criminal exploitation of the online account opening channel, the uncertainty associated with e-verification was mentioned by several mutuals.

Risk mitigation measures applied by some mutuals to limit the ability of criminals to fraudulently open online accounts included:

- setting standards that required a 100 per cent match against safe-harbour customer information (that is, rejecting 'fuzzy' matches of basic customer identification information);
- ensuring ongoing monitoring of the IP addresses of computers used by customers to interact with online facilities,
- the detection and rejection of any contact from an IP address that was masked, and
- ongoing testing of computer systems, networks and web applications to detect vulnerabilities.

One mutual still requires a share to be purchased for a small fee before any type of account opening, and found the fee dissuaded most fraudsters from attempting to open an account.

THIRD-PARTY ELECTRONIC BILLER DEPOSITS

There were 62 SMRs in the SMR sample that referenced payments processed by a third-party electronic billing service provider. Many of these SMRs related to third-party biller deposits of an unknown origin being made into mutuals' customers' transaction and credit card accounts. The grounds for suspicion in these SMRs frequently indicated funds were rapidly transferred to another financial institution once received.

Third-party biller deposits into credit card accounts were also frequently noted as having placed the account into credit. A small number of SMRs indicated the use of third-party electronic billing services to move funds obtained as a result of unauthorised account takeovers, and some described transfer of funds of an unknown source to external credit card accounts via third-party billers.

AUSTRAC's analysis of these SMRs found more than half were insufficiently detailed or contained little evidence that the mutual had properly investigated the matter.

While assessing the likely legitimacy of the source of funds deposited via third-party electronic billing services may be challenging for mutuals, AUSTRAC believes there is scope to improve reporting, particularly when deposits are made into transaction accounts.

The purpose of these biller services is to help businesses collect and pay bills, and customers can only receive bill payments through third-party billers if they have an Australian Registered Body Number (ARBN) or ACN. If a mutual's customer receives third-party billing deposits, it should indicate to the mutual the customer derives business income via these payments.

This is a good starting point for commencing ECDD investigations if the customer's recorded profession is not consistent with this mode of payment. Depending on the nature of the customer's employment, it may also raise questions with a mutual if payments processed by a third-party biller are going into a customer's personal account rather than a business account.

ATMS

ATMs are a key vehicle used by criminals to launder the proceeds of crime. ATMs facilitate movement of funds between disparate locations, including offshore. ATMs that accept deposits can also be used to place the proceeds of crime into the financial system.

Mutuals have numerous arrangements in place which provide access to ATMs across the country and overseas. Many mutuals have also enlisted third-party operated ATM networks, which gives their members fee-free access to a larger network of ATMs. Furthermore the major banks in Australia operate over 10,000 ATMs from which mutuals members can access their funds without additional fees. Offshore ATMs that accept relevant schemes' debit or credit cards can also be used to access funds held in mutuals' accounts.

Mutuals reported numerous SMRs in which a customer would receive a series of suspicious deposits into their account and then rapidly withdraw the funds from an ATM. Several SMRs in the sample also revealed systematic use of maximum ATM withdrawal limits by customers; mutuals often indicated they felt this behaviour was indicative of attempts to avoid threshold reporting obligations, even though ATM withdrawal limits were often only \$1,000.

Mutuals tend to have relatively strict limits on the ATM services they provide to their members. For example, mutuals' ATMs are less likely to accept cardless transactions or cash deposits. One mutual that does operate deposit-taking ATMs advised they had detected some displacement of suspected structuring activity from branches to these ATMs. As evidenced by the Federal Court proceedings in relation to the Commonwealth Bank of Australia,¹⁰ ATMs that accept cash deposits are highly vulnerable to misuse, particularly when associated with transactions accounts and access to international funds transfers.

CYBERCRIME INVOLVING ATM WITHDRAWALS

Cyber-enabled fraud methodologies can utilise ATM networks to steal from unsuspecting members.

One SMR described a situation in which a customer received a call from a scammer who claimed to be a representative from Australian Cybercrime Online Reporting Network, (ACORN).

The scammer claimed the customer's computer was under attack by a hacker, and convinced the customer to allow them access to their computer. The scammer then claimed that ACORN had deposited funds into the member's account which would be used to catch the hacker. In reality, the scammer had hacked into the member's computer, and was transferring the member's own funds from a separate online savings account into the transaction account. The scammer then asked the member to withdraw these funds by ATM, and then use a remitter to transfer the funds overseas.

Later that day, the scammer contacted the victim and advised the transaction had taken place, but was not enough to attract the attention of the hacker. The member remitted a second larger amount, and then agreed to remit a third amount before finally realising that they were being scammed.

¹⁰ Chief Executive Officer of the Australian Transaction Reports and Analysis Centre v Commonwealth Bank of Australia Limited ACN 123 123 124 [2018] FCA 930

NEW PAYMENTS PLATFORM

The NPP is open access infrastructure for fast payments in Australia that was developed in collaboration with industry to enable households, businesses and government agencies to make simply-addressed payments, with near real-time funds availability to the recipient, on a 24/7 basis.¹¹ The NPP commenced operation on 13 February 2018 and is currently available through 53 mutuals.

The increased speed with which money can be transferred via the NPP limits the ability for financial institutions to screen transactions and increases the risk that criminally-obtained funds can be layered and/or integrated into the financial system before they are detected. There was broad agreement from entities engaged for this risk assessment that the immediate transfer of funds would make it more difficult to freeze suspect transactions and may therefore expose adopters to a higher number of fraud attempts.

As with all new delivery channels, mutuals were required to have performed an ML/TF risk assessment of the NPP before they made it available to their customers. Many mutuals are setting low daily transfer limits of around \$1,000 per day until they gain experience with the system. Some stakeholders also noted the increased risk associated with the NPP would be at least partially mitigated because the NPP system can also facilitate sophisticated transaction monitoring.

OPEN BANKING

Open Banking is a framework designed to enhance a consumer's ability to access to the data financial institutions hold about them. In 2017, the Consumer Data Right was established by the federal government to support Open Banking with the intention to provide greater competition, improved efficiency and the creation of more tailored products and services. The initiative will be phased in by the major banks in July 2019, and by all remaining banks in July 2020.

Open Banking will enable customers to broaden the range of service providers they use to meet their banking needs, which may result in the disaggregation of transactions across multiple financial service providers. This will increase the complexity of the financial services market and limit individual reporting entities' oversight of their customers' activities, which may make it difficult to monitor and identify suspicious or unusual activity.¹²

As with the NPP, mutuals will need to ensure they have considered and prepared for the different risk environment that may be created by Open Banking before the implementation date of 1 July 2020.

¹¹ <https://www.rba.gov.au/payments-and-infrastructure/new-payments-platform/>

¹² <https://www2.deloitte.com/content/dam/Deloitte/au/Documents/financial-services/deloitte-au-fs-open-banking-6-financial-crime-080618.pdf>

OUTSOURCING OF SERVICE DELIVERY

The mutuals sector has a high level of outsourcing in relation to its service-delivery channels, including using third parties' ATMs, physical branch services, and international transaction infrastructure.

While outsourcing to third parties can provide advantages such as greater accessibility for members and improved sophistication of services, using third parties can create vulnerabilities in a mutual's ability to detect and act upon suspicious activity. In particular, mutuals noted:

- the lengthening of value chains increased difficulties in end-to-end oversight of customer activity and access to product-usage information
- the general inability to influence the risk-mitigation practices and processes of their outsourced service providers
- the lack of clarity, in some cases, as to whether the mutual, or the third party, were the designated service provider in relation to some transactions.

Overall, the vulnerabilities presented by outsourcing arrangements present significant risks to mutuals in terms of their ability to understand customer behaviour, and understand their own liability in terms of AML/CTF compliance.

FOREIGN JURISDICTION

AUSTRAC assesses the mutual banking sector has a **high** vulnerability to foreign jurisdiction risk.

Exposure to foreign jurisdictions creates ML/TF risk because serious and organised crime groups are likely to attempt to move proceeds of crime both to and from Australia, and many terrorist financiers are likely to attempt to fund terrorist activity offshore. Further,

transnational transactions add complexity, helping to obscure beneficial ownership and beneficiary customers, and increase potential for offshore tax evasion.

Transnational serious and organised crime threatens the safety, security and trust of the community, the prosperity of its businesses and Australian economy, the integrity of its institutions, and national security. While many mutuals have a somewhat limited exposure to foreign-based customers due to restrictions on membership, mutuals' facilitation of international transactions for their members creates ML/TF vulnerabilities for the sector.

TRANSNATIONAL SERIOUS AND ORGANISED CRIME

In 2018, the Department of Home Affairs released the Transnational Serious and Organised Crime Strategy,¹³ which states:

- Transnational, serious and organised crime is sophisticated, well financed and integrated into a global network – and 70 per cent of Australia's serious and organised crime threats are based offshore or have strong offshore links.¹⁴
- The threat causes untold human suffering and costs up to \$47 billion a year¹⁵ – money not spent on improving Australia and our quality of life.
- Australia is attractive to criminals because it is a wealthy, prosperous society.
- The threat environment is constantly changing, and organised criminals are adapting through new methodologies and advanced technologies.

13 <https://www.homeaffairs.gov.au/nat-security/files/strategy-transnational-serious-organised-crime.pdf>

14 Australian Crime Commission (ACC) 2015. The costs of serious and organised crime in Australia 2013–14. Canberra: Australian Crime Commission. <https://aic.govcms.gov.au/publications/intelligenceproducts/costs-serious-and-organised-crime-australia>

15 Smith R 2018. Estimating the costs of serious and organised crime in Australia 2016–17. Statistical Reports no. 9. Canberra: Australian Institute of Criminology. <https://aic.gov.au/publications/sr/sr09>

Eleven per cent of SMRs in the sample related to foreign jurisdictions. The five most common countries mentioned were Thailand, USA, UK, China and Malaysia. Cyber-enabled scams featured prominently in SMRs involving foreign jurisdictions, as overseas scammers attempted to coerce victims to transfer money withdrawn from their Australian accounts.

Consultations demonstrated that foreign jurisdiction risk is mitigated in the mutual banking sector in several ways. Usually, a person must be a resident or a citizen to open an account with a mutual, so mutuals have fewer customers based in foreign jurisdictions. Where mutuals do have overseas-based customers, this is generally because a customer who had been an Australian resident relocated offshore, but chose to maintain their banking relationship with the mutual.

One of the larger mutuals consulted for this risk assessment advised AUSTRAC it had about 400 customers who currently resided overseas, but that they had all been physically present in Australia when they opened the initial account. Other risk mitigation measures described by mutuals included:

- flagging accounts with higher levels of transactions involving foreign jurisdictions as high-risk
- refusing to facilitate international transfers for non-customers
- requiring customers to come into a branch to conduct international transfers.

However, as with other vulnerabilities, risk mitigation systems and controls in relation to foreign jurisdictions are not uniform across the sector and need to be considered at the reporting entity level. Further, a mutual's exposure to foreign jurisdiction risk will depend, to an extent, on the systems and controls used by their remittance partner.

REMITTANCES TO AND FROM MUTUALS USING THIRD PARTIES

Retail banks and remittance service providers (remittance partners) facilitate remittances on behalf of mutuals for mutuals' members. In the review period 1 July 2016 to 30 June 2018, mutuals' remittance partners submitted 20,993 IFTIs in which they nominated a mutual as the ordering or beneficiary customer, while mutuals submitted only 150 IFTIs as a reporting entity.

IFTIs reported with a mutual as an ordering or beneficiary customer:

- 7,317 outgoing IFTIs with a total value of over \$83 million, to 127 receiving countries. Most common receiving countries were the UK, the USA and New Zealand.
- 13,676 incoming IFTIs with a total value of over \$27 million, from 26 sending countries. Most common sending countries were Canada, the UK and the USA.

IFTIs with high-risk jurisdictions

A considerable proportion of international funds transfers go to jurisdictions that present a high risk of serious criminal activity, such as terrorism financing, child exploitation, and tax evasion. While the majority of these IFTIs are likely to be associated with legitimate activities, it is critical that mutuals develop an understanding of their members' transactions with high-risk jurisdictions in order to assess their exposure to foreign jurisdiction risk, and to detect instances of criminal behaviour.

Because mutuals typically utilise the services of third parties to affect international transfers, both the mutual and the third party have oversight over international transactions. This may insulate the mutual from their foreign jurisdiction risk to some extent, if the remittance partner's processes are robust.

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

IMPLEMENTATION OF RISK MITIGATION STRATEGIES

AUSTRAC assesses the level of implementation of risk mitigation strategies to pose a **medium** risk in the mutual banking sector.

Risk mitigation strategies include measures that mutuals have implemented that go towards mitigating ML/TF risks.

AUSTRAC observed during the development of this risk assessment that the mutuals sector has strengths in terms of:

- the use of fraud and compliance professional networks
- communication between branches of individual mutuals
- questioning customers who attempt unusual transactions at branches, and
- supporting customers who appear to be victims of scams.

There are also some areas in which mutuals' risk mitigation systems and controls could be strengthened.

RISK ASSESSMENT

A robust risk assessment is the centrepiece of an effective AML/CTF regime. It is important that risk assessment processes have the capacity to generate a genuine understanding of ML/TF exposure at an individual reporting entity level. This means the use of off-the-shelf risk assessment tools needs to be tailored to ensure it reflects the actual risks posed to mutuals operating within different contexts. Not only do risk assessments need to be entity-specific, they also need to be regularly updated to ensure changes in risk profiles and systems, and any changes to the nature of products or delivery channels are addressed in a timely and effective way.

One industry expert engaged for this risk assessment expressed concern that some mutuals may not be properly assessing the inherent risk of their products and services, meaning the development and application of risk mitigating systems and controls may not be fit for purpose.

SUSPICIOUS MATTER REPORTING PROCESSES

The mutual banking sector reports a relatively high number of SMRs, and while reporting volumes vary between individual entities, AUSTRAC noted that over 90 per cent of mutuals submitted at least one SMR over the two-year period studied for this assessment.

There were many examples of good SMR reporting practices from the sector, with reporting officers including detailed transaction histories, records of contact with the customer/suspicious party, and relevant information uncovered from carrying out ECDD.

However, AUSTRAC also observed several instances in which suspicious matter reporting processes were inadequate, for example:

- mutuals repeatedly reporting on the same customers exhibiting the same behaviours without any indication they were attempting to address their suspicion by engaging with the customer, conducting further investigation, or even exiting the customer in cases of unacceptably high risk.

- trigger-based reporting – a practice in which a reporting entity submits a suspicious matter report to AUSTRAC solely on the basis of a trigger generated by their transaction monitoring system without conducting further investigation to form suspicion on reasonable grounds.
- submission of SMRs with insufficient details in the Grounds for Suspicion section – some reports failed to provide details about why the activity was considered suspicious. In fact, some SMRs reviewed for this risk assessment contained only 2-3 words. SMRs of this length cannot contain sufficient detail to explain:
 - o what the questionable behaviour of the customer was,
 - o why the behaviour of the customer was considered questionable, and
 - o what type of criminal behaviour the mutuals considers the activity may be indicative of.

A number of mutuals AUSTRAC engaged advised they were in the process of reviewing their suspicious matter reporting systems. AUSTRAC encourages mutuals to engage in these types of reviews. AUSTRAC particularly encourages the mutuals that submit only a small number of SMRs to ensure their systems and controls can identify suspicious activity when it occurs.

BALANCING ENHANCED CUSTOMER DUE DILIGENCE WITH TIPPING OFF PROVISIONS

Mutuals should ensure they have robust ECDD processes in place to monitor high-risk customers, and customers subject of an SMR. At the same time, mutuals should also use discretion when making further enquiries about the customer, to minimise the risk of “tipping off” the customer that an SMR has been submitted about them.

AUSTRAC considers simply asking a customer for additional information (for example, about their identity or the source or destination of their funds) would not constitute an unlawful disclosure of information or an offence under the tipping off provisions of the AML/CTF Act.

FURTHER RESOURCES FOR GUIDANCE ON SUSPICIOUS MATTER REPORTING

As well as this risk assessment, AUSTRAC has developed resources which provide guidance on effective suspicious matter reporting and AML/CTF programs including:

- a [video animation](#) on the value of SMRs - what makes a good SMR and how they help protect Australia from financial crime and terrorism financing.
- a [webinar](#) about suspicious matter reporting and digital currency exchange providers. The first part of the webinar focusses on SMRs and provides practical advice on preparing SMRs and explains the benefits of reporting quality SMRs.

AUSTRAC encourages all mutuals to review these resources and consider if the systems they use to ensure compliance with their AML/CTF obligations could be improved.

Reporting entities can also contact AUSTRAC by emailing contact@austrac.gov.au or telephoning 1300 021 037 within Australia for further assistance.

TRANSACTION MONITORING PROGRAMS

Transaction monitoring programs need to be regularly reviewed and updated to remain effective. AUSTRAC received feedback that accessing adequate resources to invest in AML/CTF systems was a significant challenge for some mutuals. One industry participant commented that the most significant vulnerability for the mutual banking sector is the quality of automated systems to detect unusual transaction activity, which is limited by the amount of resources many smaller mutuals have to invest in their technology.

Any future merger activity will likely generate economies of scale and improve the ability to invest in risk mitigation systems. However risk may be retained when entities merge and pre-existing systems are not integrated or do not integrate effectively. In fact, one industry expert engaged for this risk assessment observed mutuals often have a “set and forget” approach to AML/CTF measures, particularly in the context of growing size and scale.

Many mutuals rely on the services of third parties to conduct their transaction monitoring activities. While for many mutuals this may increase the sophistication of the transaction monitoring they undertake, it also makes it difficult for them to tailor processes to their business' unique risk profile. On the other hand, where transaction monitoring is outsourced by many mutuals to the same third-party provider, the third party will have oversight over activities occurring across the whole sector and may be able to identify patterns of anomalous activity that would not otherwise be understood.

OUTSOURCING

The mutual banking sector outsources a significant amount of its AML/CTF compliance functions to third parties. This is because many mutuals do not operate on a scale large enough to efficiently deliver these functions in-house.

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

Mutuals and industry experts engaged for this assessment indicated they saw outsourcing as a major challenge for the sector. They made a number of observations in relation to outsourcing, including:

- there is inadequate documentation and oversight of service-level agreements
- oversight of outsourcing arrangements has not been adequately prioritised by senior management
- heavier reliance on off-the-shelf products which are not tailored to individual businesses is limiting effectiveness of controls.

One mutual consulted for this assessment noted that the limited resources to invest in AML systems, analytics and staff, together with potential lack of organisational agility to respond to the above risks, are exacerbated by the lack of agility in the sector overall and its high dependency on third party service providers.

Mutuals remain responsible for the functioning of their AML/CTF program even when AML/CTF activities have been outsourced. Effective outsourcing includes:

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

While outsourcing can increase ML/TF vulnerability, in certain circumstances there are benefits to outsourcing. Where smaller mutuals cannot generate the economies of scale necessary to develop and operate sophisticated systems in-house, the risks posed by outsourcing may be mitigated by mutuals having access to the robust, tested and well-resourced transaction processing and monitoring systems developed by service providers. The successful implementation of outsourcing arrangements is dependent on a clear, strong, collaborative and actively-managed relationship between all parties involved.

MERGERS INTRODUCING HIGHER-RISK CUSTOMERS

Several mutuals engaged for this risk assessment noted they had 'inherited' customers outside of their risk appetite as a result of merging with another mutual. This highlights the risks mutuals face as they pursue a strategy of mergers. Mutuals need to ensure customers inherited through mergers are reviewed for ML/TF risk, to ensure they meet the new organisation's ML/TF risk appetite and appropriate controls are in place.¹⁶ One industry expert advised AUSTRAC that no merger he had observed in the mutuals sector had applied rigour in discharging the applicable customer due diligence procedures required of it in circumstances of business sale/transfer.¹⁷

SMALLER MUTUALS

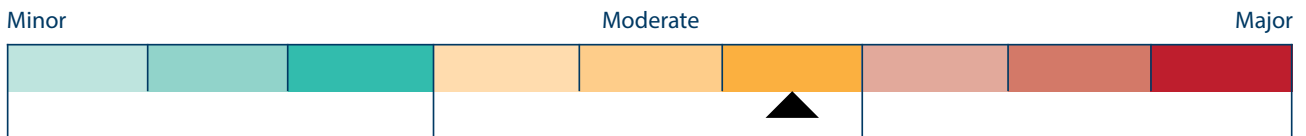
In relation to the smaller entities in the sector, it was noted that:

- resource constraints may mean the AML/CTF compliance officer will have several other responsibilities
- systems and controls may lack capacity and sophistication
- procedures may not be sufficiently documented or reviewed
- regional mutuals may struggle to attract and retain appropriately skilled staff, as the proportional cost for highly-skilled staff is higher for smaller mutuals than it is for larger financial institutions.

¹⁶ For more information on obligations relating to applicable customer due diligence in the context of compulsory partial or total transfer of business made under the Financial Sector (Business Transfer and Group Restructure) Act 1999, please see chapter 66 of the [AML/CTF Rules](#).

¹⁷ Required under Chapter 28 of the [AML/CTF Rules](#).

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 crimes may cause. Financial crime in the mutual banking sector has consequences for customers, individual mutuals, the sector as a whole, and the broader Australian economy. Where mutuals are used to facilitate the financing of terrorism, criminal exploitation has consequences for domestic and international security.

The impact of criminal activity on customers can include:

- financial losses from fraud, identify theft, or scams
- emotional distress and potential criminal implications for people unknowingly used as money mules and victims of financial abuse
- lower returns to members, either as higher borrowing costs or lower interest rates on investments, as mutuals' profits are reduced through actual losses and increased compliance costs.

The impact of criminal activity on mutuals can include:

- loss of revenue from fraud, and increased fraud insurance premiums
- heightened regulatory oversight
- increased costs associated with combating criminal attacks/cyber-enabled fraud, in particular IT security costs to build cyber resilience
- reputational damage to a sector following an incident, leading to loss of customers and increased public relations costs
- increased regulatory action, legal action, associated with civil or criminal penalties in the event of serious non-compliance by a mutual
- increased risk of legal action and compensation for customer losses arising from failed AML/CTF controls.

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 perception among criminals that the industry can continue to facilitate their illegal activity.
- increased criminal activity in the community, as ease of laundering illicit funds would encourage further criminal activities to occur
- mutuals with insufficient AML/CTF programs becoming known to criminal entities, encouraging further criminal activity and proceeds of crime to flow into the sector
- 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
- widespread loss in confidence in the mutual banking sector as well as the overall Australian banking system.

Significant breaches of AML/CTF controls could damage Australia's international economic reputation in relation to the security and safety 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.

FEEDBACK

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 via riskassessments@austrac.gov.au

GLOSSARY

Term	Description
ADI	An authorised deposit-taking institution (ADI) is a body corporate authorised under the Banking Act 1959, to carry on banking business in Australia (e.g. a bank, building society or credit union), the Reserve Bank of Australia or a person who carries on State banking.
AML/CTF	Anti-money laundering and counter-terrorism financing.
AML/CTF program	A document that sets out how a reporting entity meets its AML/CTF compliance obligations.
Customer Bond	Historically, membership in a mutual was limited to a specific customer grouping (or 'bond'), such as customers who worked in the same industry or lived in the same geographic region.
Trigger-based reporting	A practice in which a reporting entity submits a suspicious matter report to AUSTRAC solely on the basis of a trigger generated by their transaction monitoring system without conducting further investigation.
ECDD	Enhanced customer due diligence (ECDD) is the process of undertaking additional customer identification and verification measures in certain circumstances deemed to be high risk.
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.
IFTI	An instruction to transfer funds or property to either: <ul style="list-style-type: none"> - Australia from another country - another country from Australia.
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.
Layering	The second stage of the money laundering cycle, which involves moving, dispersing or disguising illegal funds or assets to conceal their true origin.

Term	Description
ML/TF	Money laundering and terrorism financing.
Mules	Third parties employed to transfer illicit funds between locations or accounts.
PEP	A politically exposed person (PEP) is an individual who holds a prominent public position or function in a government body or an international organisation; or is an immediate family member or close associate of such an individual.
Phoenixing	Phoenixing occurs when a new company is created to continue the business of a company that has been deliberately liquidated to avoid paying its debts, including taxes, creditors and employee entitlements.
Placement	The first stage of the money laundering cycle, in which illicit funds first enter the formal financial system.
Predicate offence	For the purpose of this risk assessment, predicate offence is any offence which generates proceeds of crime.
Remittance partner	For the purpose of this report, a remittance partner refers to the remittance provider or bank that facilitates mutuals' outgoing international funds transfers.
SMR	A report a reporting entity must submit under 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.
SOCG	Serious and organised crime group
TMP	Part A of a reporting entity's AML/CTF program must include a risk-based transaction monitoring program (TMP) that comprises of appropriate systems and controls to monitor the transactions of customers and identify suspicious transactions.
TTR	A report submitted to AUSTRAC about a designated service provided to a customer by a reporting entity that involves a transfer of physical or digital currency of A\$10,000 or more or the foreign currency equivalent.

APPENDIX A: RISK ASSESSMENT METHODOLOGY

The methodology below covers 19 risk factors across three categories – criminal threat environment, vulnerabilities and consequences. 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 scores of the criteria provides the total risk score for each category, and the average of the three risk scores for each category provides the overall risk rating for the sector.


CRIMINAL THREAT ENVIRONMENT		
Low	Medium	High
Minimal variety of money laundering methodologies. There is a low level of involvement by 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, or are easy detect. None or a very small number of terrorist groups and their financiers, associates and facilitators utilising the sector.	Terrorist financing methodologies are somewhat varied, or can sometimes be difficult to detect. There is a small number of terrorist groups, financiers, associates and facilitators utilising the sector.	Terrorist financing methodologies are highly varied, or are often difficult to detect. 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 and are easily detected. There is a low level of involvement by SOCGs and other high-risk actors.	Predicate offences are moderately varied and may sometimes be difficult to detect. There is a medium level of involvement by SOCG and other high-risk actors.	Predicate offences are highly varied and are often difficult to detect. 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 high-risk jurisdictions	Transactions sometimes involve high-risk jurisdictions	Transactions often involve high-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

 1300 021 037

 www.austrac.gov.au