Australian Government

AUSTRAC

AUSTRALIA'S SECURITIES & DERIVATIVES SECTOR >>>

MONEY LAUNDERING AND TERRORISM FINANCING RISK ASSESSMENT

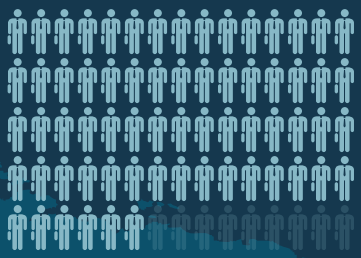
AUSTRALIA'S SECURITIES & DERIVATIVES SECTOR

929,000 trades per day on the Australian Securities Exchange*

worth **$4.7 billion***

76 market participants**

66 over the counter (OTC) derivatives providers***



45% of equity held by foreigners‡

6.7m Australians own shares†

SUSPICIOUS MATTER REPORTS (SMRs)

663 SMRs submitted to AUSTRAC from 1 April 2014 to 31 March 2016

7 reporting entities reported half of the SMRs

28 were market participants

19 were foreign or domestic banks, or other entities

18 were contracts for difference/ foreign exchange (CFD/FX) and other OTC derivatives providers

3 were both market participants and CFD/FX and other OTC derivatives providers

* There are a significant number of trades on other exchanges such as Chi-X as well as off market trades. As of 2015/2016, provided by ASX

** Market Participant trade data for a six-month period to 20 June 2016, provided by Australian Securities and Investments Commission (ASIC)

*** As at July 2016, provided by ASIC

† ASX, *Corporate Overview,* 2016, http://www.asx.com.au/about/corporate-overview.htm

‡ As of June 2016, provided by ASX

CONTENTS

KEY TERMS

Term	Description
Contracts for difference (CFD)	A contract for difference is a leveraged derivative financial product where the value is derived from the value of an underlying asset[1].
Derivatives	Instruments that derive value from an underlying asset such as shares, currencies, commodities.
Direct market access (DMA)	A form of electronic trading in which market participants allow customers direct access to submit orders through their internal systems onto an exchange or trading platform.
Foreign exchange trading	Foreign exchange trading is the practice of buying and selling foreign currency to make a profit[2].
Grounds for suspicion	The free text field in the suspicious matter report (SMR) form that allows the reporting entity to provide a description of the suspicious matter.
Market participant	Trading, clearing or settlement participants that meet the ASX or other financial market exchange requirements for admission.
Off-market transfer	Off-market transfers involve transferring legal ownership of parcels of shares from one person or entity to another, without trading on an exchange. This is carried out through a private agreement between two parties by lodging a form with a share registry. Alternatively, a customer may ask a market participant to carry out this activity on their behalf.
Offshore service provider (OSP)	OSPs are businesses which offer products and services to residents of other countries including the creation of corporate entities such as companies and trusts.
Over the counter (OTC) trading	Trading that is not conducted on a formal exchange such as the ASX.
Retail customer	A customer who does not come under the definition of 'wholesale customer' (see below).
Securities	Securities can also be referred to as shares, stocks and equities. Investing in securities gives the holder part-ownership in a company.
Structuring	Structuring refers to the practice of deliberately making cash deposits or withdrawals in amounts of less than $10,000 in order to avoid the threshold transaction reporting requirement to AUSTRAC. Structuring is a criminal offence under section 142 of the AML/CTF Act.
Suspicious matter reports (SMRs)	Reports to AUSTRAC in relation to suspicious transactions, submitted under section 41 of the AML/CTF Act.
Wash trading	Trading activity where the same person or entity buys and sells shares simultaneously (that is, with no change of beneficial ownership), to either manipulate the market or create a capital loss in order to evade tax.
White labelling	Businesses can facilitate access to trading platforms for their customers despite not being market participants. They do this by entering into an agreement to access a market participant's trading platform. This activity is known as "white labelling" and is common in the securities and derivatives sector. White-labelled entities are also referred to as 'indirect market participants', 'securities dealers' or 'shadow brokers'.
Wholesale customer	An entity that meets a number of criteria in terms of the amount of money it has to invest, net assets and gross income. This includes professional investors such as those with an Australian Financial Services License (AFSL), Australian Prudential Regulation Authority (APRA) regulated bodies, trustees of public superannuation funds, and listed entities controlling at least $10 million.

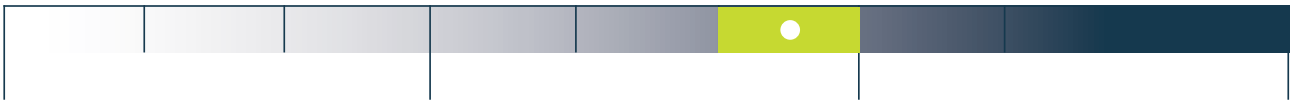
1 ASIC, *Thinking of trading contacts for difference*, 2012, https://www.moneysmart.gov.au/media/173820/thinking-of-trading-in-contracts-for-difference-cfds.pdf

2 ASIC, *Foreign exchange trading*, 2017, https://www.moneysmart.gov.au/investing/complex-investments/foreign-exchange-trading

EXECUTIVE SUMMARY

OVERALL RISK RATING

The overall money laundering and terrorism financing (ML/TF) risk for the securities and derivatives sector is assessed as **MEDIUM**. This rating is based on assessments of the criminal threat environment, vulnerabilities in the sector and the associated consequences.



CRIMINAL THREAT ENVIRONMENT

AUSTRAC assesses that Australia's securities and derivatives sector attracts a wide range of criminal threats that often involve sophisticated tactics and methods. Serious and organised crime groups have exploited the sector to launder money and engage in market manipulation. The criminal threat environment is assessed as **MEDIUM**.

Reporting entities operating in the securities and derivatives sector nominated a variety of suspected criminal offences in the 663 SMRs submitted to AUSTRAC over the two-year sample period.

Money laundering: Suspected money laundering accounted for 21 per cent of SMRs in the dataset. Many of these involved well-established methodologies, including structured cash deposits and unusually large cash deposits and withdrawals. A significant number of SMRs described the placement of cash into general transaction accounts, which was subsequently transferred into trading accounts.

Terrorism financing: The level of reporting on terrorism financing was very low. However, as the three SMRs detailed in the assessment highlight, the sector should not be complacent about the potential terrorism financing risk. Awareness of this risk may result in increased detection and SMR reporting.

Fraud: The most common offence reported in SMRs from this sector was fraud, representing 51 per cent of SMRs. Half of these fraud-related SMRs were enabled by cybercrime, with many reporting entities assessing the threat of cyber-enabled fraud to be increasing – in both the volume and level of sophistication.

Insider trading and market manipulation: Reporting on suspected cases of insider trading and market manipulation was also prevalent, accounting for 21 per cent of SMRs. These included individuals and entities conducting trades based on unpublished price-sensitive information or employing a range of tactics to manipulate share prices. Intelligence from an AUSTRAC partner agency also indicates that online trading platforms are increasingly being used by overseas-based entities to manipulate the market.

Tax evasion: Although tax evasion was suspected in only two per cent of SMRs, partner agency intelligence indicates the threat may be more significant. This is due to customers using offshore service providers (OSPs) to create corporate structures that conceal beneficial ownership of shares to evade tax.

VULNERABILITIES

There are a significant number of factors that render the securities and derivatives sector vulnerable to criminal misuse. AUSTRAC assesses the level of vulnerability as **MEDIUM**.

Entities operating in the securities and derivatives sector are exposed to a wide array of customer types. The majority (78 per cent) of SMRs were in relation to individuals; however, there are also a variety of other customer types present in this sector including companies, trusts and foreign entities.

The use of agents and third parties posed a significant vulnerability for some entities – especially when located offshore – due to difficulties in obtaining customer identification and authorisation forms, and difficulties in conducting assurance activities on the agents and third parties.

Four main products and services were identified in this assessment as vulnerable to criminal misuse:

- **Accounts**: The provision of general transaction and trading accounts provide the principal mechanism for moving funds in and out of the sector.
- **Trading**: Trading activity itself is vulnerable to criminal exploitation – in particular insider trading and market manipulation – primarily due to the large volume of trades conducted on a daily basis, and the speed with which trades often need to be executed.
- **Off market transfers**: The ability to transfer shares, and thereby value, from one person or entity to another without trading on an exchange.
- **Third-party payments**: Transferring funds to third parties is vulnerable to misuse if the third party is not known to the reporting entity – particularly if funds are sent overseas.

The trend towards customers increasingly using online services to open accounts and trade creates additional **delivery channel** challenges for reporting entities, particularly in relation to cybercrime.

The ability for **cash** to be placed into general transaction accounts and quickly moved to and between trading accounts, makes the sector vulnerable to money laundering. This risk is heightened when the transaction and trading accounts are held with different financial institutions because of the limited visibility both firms have over the customer's financial activity.

With some 45 per cent of the ASX market owned by foreign entities, the sector is subject to significant **foreign jurisdiction** risk. In the dataset, 206 SMRs (31 per cent) reported suspicious transactions relating to 49 foreign jurisdictions. China and Hong Kong combined accounted for a quarter of these SMRs. Corporate customers in low-tax jurisdictions create additional vulnerabilities, especially in relation to tax evasion, fraud and other offences.

The practice of 'white labelling' trading platforms creates significant **operational vulnerabilities** for the sector. Poorly developed agreements or contracts that do not clearly indicate which entities are responsible for AML/CTF obligations significantly undermine the AML/CTF framework.

Front office staff, such as traders and advisers, may also represent a vulnerability if there is complacency around AML/CTF obligations in favour of a greater focus on credit risk and retaining client business.

AUSTRAC assesses that there is considerable scope for entities operating in these markets to improve their **AML/CTF systems and controls**. Some 60 per cent of market participants and 74 per cent of CFD/FX providers did not submit a SMR to AUSTRAC over the two-year sample period.

CONSEQUENCES

The overall consequences of ML/TF activity in the sector is assessed as **MODERATE**.

There are consequences for individual customers as a result of criminal misuse of the sector. These generally relate to financial losses from accounts and investment portfolios, and emotional distress as a result of fraud-related crimes.

The most significant consequences of ML/TF activity are generally borne by the securities and derivatives sector as a whole. These include reputational damage, increased regulatory action and other costs, and decreased dividend distributions to shareholders.

The severity of the consequences vary from one reporting entity to another in the sector, depending on the extent to which they understand the ML/TF risks they face and have effective controls and strategies in place to mitigate these risks, such as the various controls highlighted throughout this risk assessment.

Financial crime in the sector also has the potential to impact the broader Australian economy. This includes reduced taxation revenue, impacting on the delivery of critical government services, as well as reduced investment in the sector which may affect economic growth.

PURPOSE

This risk assessment provides sector-specific information on ML/TF risks at the national level for entities operating in securities and derivatives. Its primary aim is to assist the sector to identify, understand and disrupt ML/TF and other criminal offences targeting Australia's financial system.

The assessment covers exchange traded and OTC securities and derivatives. It is relevant to market participants ('stockbrokers') operating on licensed exchanges such as the ASX, licensed entities providing services in the CFD and FX markets, and share registries.

There is a focus on retail customers throughout this assessment as a result of the SMRs submitted to AUSTRAC and other available intelligence. There are several sections and findings that also apply to wholesale customers. Managed investment schemes were out of the scope of this assessment.

This risk assessment has been developed as a feedback resource for the securities and derivatives sector. AUSTRAC expects that reporting entities will use this assessment to refine their own compliance controls and mitigation strategies.

This risk assessment also aims to help reporting entities identify and monitor risks that may be applicable to their individual businesses, and to subsequently report suspicious matters to AUSTRAC. Reporting entities should apply information in this assessment in a way that is consistent with the nature, size and complexity of their businesses, and the ML/TF risk posed by their designated services and customers. Future AUSTRAC compliance activities will assess how reporting entities in the sector have responded to the information provided here.

METHODOLOGY

The methodology used for this risk assessment follows Financial Action Task Force (FATF) guidance that states that ML/TF risk at the national level should be seen as a function of: criminal threat, vulnerability and consequence. According to this methodology:

- **Criminal threat environment** refers to the extent and nature of ML/TF and other 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 it deals. Vulnerability is also influenced by the AML/CTF systems and controls in place across the sector.
- **Consequence** refers to the impact or harm that ML/TF activity may cause.

This assessment considered 26 risk factors across these three categories. An average risk rating was determined for each category, which was then used to determine an overall risk rating for the sector. Further information on the methodology and how this was applied to the sector is in the Appendix.

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

- analysis of SMRs, as well as other AUSTRAC information and intelligence
- reports and intelligence from a variety of partner agencies including intelligence, revenue, law enforcement and regulatory agencies across government
- feedback and professional insights offered during interviews and consultations with a range of entities operating in the securities and derivatives sector, as well as industry experts and industry associations.

REPORTING TO AUSTRAC

Businesses operating in the securities and derivatives sector have reporting obligations under the AML/CTF Act. Submitting SMRs to AUSTRAC is a critical obligation under the Act.

AUSTRAC analysed two years of SMRs submitted by entities in the securities and derivatives sector.

AUSTRAC and its partner agencies piece together intelligence from a range of sources to develop a picture of criminal activities and networks. Many partner agencies – including ASIC, Australian Tax Office (ATO), Australian Federal Police (AFP) and Australian Criminal Intelligence Commission (ACIC) – have access to AUSTRAC SMRs to conduct further analysis and investigation.

663 SMRs submitted

68 Reporting entities submitted at least one SMR

16 Reporting entities submitted 10 or more SMRs

7 Reporting entities accounting for half of all SMRs submitted

1 April 2014 to 31 March 2016

CRIMINAL THREAT ENVIRONMENT

AUSTRAC assesses there is a **MEDIUM** threat of criminal exploitation to Australia's securities and derivatives sector. The sector attracts various criminal threats, with a moderate level of sophisticated tactics and methods used to commit offences.

As the chart below shows, reporting entities in the sector nominated six main offence types in the 663 SMRs analysed for this risk assessment. Suspected cases of money laundering accounted for a large portion, while terrorism financing was suspected in only three SMRs. Fraud-related offences were suspected in just over half of SMRs, with a significant number enabled by cybercrime. Twenty-one per cent of reports related to insider trading and market manipulation. A small number of SMRs related to various other types of suspected offences, including tax evasion and scams.

MONEY LAUNDERING

AUSTRAC data indicates that the securities and derivatives sector is being exploited to launder money and move the proceeds of crime. There were 141 SMRs received in relation to suspected money laundering in the sample period. Significantly, some of the SMRs in the dataset related to a money laundering syndicate involved in serious and organised crime, which were of high intelligence value to AUSTRAC. In this case, a syndicate was found to be operating throughout the Asia-Pacific region, making large cash deposits into accounts held with an Australia-based market participant.

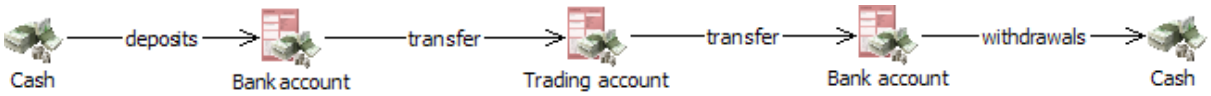
A significant number of SMRs described the placement of cash into general transaction accounts, which were subsequently transferred into trading accounts. These SMRs were reported by various types of financial institutions including banks, market participants and CFD/FX providers.

Many of these SMRs described a common methodology that includes the placement and layering stages of money laundering, summarised below.

- Large or structured cash amounts are deposited into the customer's general transaction account (placement).
- These funds are transferred into a trading-based bank account often with minimal or no trading activity conducted (layering).
- The funds are transferred back into the original, or another, bank account and then withdrawn in structured or large cash amounts (layering).

This type of activity ranged from one-off transactions to ongoing patterns of this behaviour.

A COMMON MONEY LAUNDERING METHODOLOGY



Almost all of these cash-related SMRs were reported by market participants which were part of a broader corporate group that includes retail banking. This underlines the visibility these institutions can have over transactions to and from multiple accounts, including general transaction accounts and trading accounts.

The following characteristics were commonly cited in SMRs where the customer was suspected of money laundering:

- transaction activity conducted in a short amount of time, including on the same day
- customer's occupation recorded as unemployed
- transactions made at different bank branch locations
- deposits conducted by third parties
- transaction activity that is inconsistent with the customer profile
- the source of funds is not known.

Industry has also suspected customers may be engaged in money laundering as a result of other unusual activity, such as:

- opening multiple trading accounts within a short time frame
- repeated changes to a customer's profile information and data
- fake identification/information used to set up trading accounts
- the value of funds transferred into a trading account far exceeds the level and value of trading activity
- transfers of funds into a trading account followed by requests for withdrawals with little or no trading activity
- uneconomic trading
- requests for funds to be transferred to third parties.

Several entities engaged for this assessment advised that wholesale customers are highly unlikely to be dealing in cash; however, many of the unusual activity indicators above also apply to wholesale customers.

TERRORISM FINANCING

The level of terrorism financing reported in SMRs by entities in the securities and derivatives sector is very low. In the two-year sample period, only three SMRs (less than one per cent) related to possible terrorism financing. These reports were submitted by three different reporting entities and all applied to retail customers.

One SMR was submitted by a reporting entity that discovered it had a customer whose name was recorded on the Australian Government's Consolidated List of all persons and entities who are subject to targeted financial sanctions or travel bans under Australian sanctions laws. The customer had a trading account with the firm but was not actively trading at the time the report was submitted.

Routine media monitoring conducted by another reporting entity detected that one of its customers had recently been arrested for planning a terrorist attack in Australia inspired by Islamic State of Iraq and the Levant (ISIL). The customer had not used the trading platform for several months and there was no imminent risk of terrorism financing. The SMR submitted by the reporting entity provided intelligence relevant to an investigation.

In another SMR, a large market participant was approached by a family member of a customer who was concerned that the customer was mentally unstable and possibly preparing to travel overseas to fight against a large terrorist organisation. The family member believed the customer intended to sell their shares (worth over $200,000) to fund this travel. The market participant subsequently reported this in an SMR. There was no evidence the shares were sold and cashed, or used to facilitate travel to a conflict zone.

Despite the limited reporting on terrorism financing in SMRs, the sector should not be complacent about the potential risk. Awareness of this risk may result in increased detection and SMR reporting.

FRAUD

By far the most common offence reported in SMRs from this sector was fraud, representing 51 per cent of SMRs. Half of these fraud-related SMRs were enabled by cybercrime. The activities in these SMRs can be grouped into two broad trends:

- A cybercriminal hacks a customer's email account and sends fraudulent instructions to financial institutions to close out the client's trading positions and/or transfer client funds to other accounts or third parties. This issue could occur with retail and wholesale customers.
- A cybercriminal hacks a customer's online trading account and conducts trades, closes out positions and/or transfers funds to other accounts or third parties. In some cases this activity was enabled by fraudsters finding out the answers to the customer's security questions by trawling through the customer's social media. This generally applies to retail customers only.

Reporting entities engaged for this risk assessment perceived cyber-enabled fraud as a serious issue. Some entities assessed the threat of cyber-enabled fraud to be increasing – in both the volume and the level of sophistication.

"THE INDUSTRY WAS SURPRISED TO SEE HOW FAR CYBERCRIMINALS WOULD GO TO COMMIT CRIMES"

– Representative of a large financial institution

In response to these types of criminal threats, in late 2016 the ASX and ASIC invited the 100 largest ASX-listed companies to participant in a cyber-health check survey. The companies consequently received a report benchmarking their cyber security practices, to arm them in making their businesses cyber-resilient. The ASX also released a public report in April 2017 highlighting the themes that emerged from this data and providing information to help companies take practical steps to improve their cyber security[3].

TRADING INSTRUCTIONS FROM A COMPROMISED EMAIL ACCOUNT

One SMR described that a customer's personal email account had been hacked by an unknown third party who fraudulently sent a 'change of bank account instruction' to the customer's stockbroking firm via his financial planner. The instructions formally advised the stockbroking firm to use a new account, held with a different financial institution, when settling trades. The fraudster subsequently sent another instruction to sell some of the customer's shares and pay the proceeds of the sale into the newly opened account. The trade was executed and the real customer received notification of the bank account changes. The customer notified the stockbroking firm that they did not open a new bank account. Although the fraudster was successful in executing a trade, the proceeds from the sale were stopped before being paid into the fraudulent account.

There were also a significant number of fraud-related SMRs about stolen and/or fraudulent identification documents being used to set up trading accounts or to withdraw funds from trading accounts. Many SMRs also related to the use of fraudulent credit cards to fund trading and subsequently withdrawing funds (with or without trading activity).

INSIDER TRADING AND MARKET MANIPULATION

Insider trading and market manipulation generate proceeds of crime and are significant criminal offences under the *Corporations Act 2001*. Since 2011, 35 people have been criminally prosecuted for insider trading as a result of ASIC investigations, with a conviction rate of over 85 per cent.[4]

Intelligence from AUSTRAC's partner agencies indicates that an increasing number of attempts to manipulate the market were initiated in foreign countries, particularly China, Hong Kong, Canada, Europe and Russia. These attempts are increasingly facilitated by online trading platforms that allow overseas-based individuals to access Australia's financial markets.

Insider trading and market manipulation offences made up 21 per cent of the SMRs submitted to AUSTRAC during the sample period. Most of these were in relation to exchange traded securities; however, 23 SMRs related to CFD and FX trading products.

3 ASX, *ASX 100 Cyber health check report*, 2017, www.asx.com.au/ASX100-Cyber

4 ASIC, *Market integrity update – Issue 73*, 2016, http://asic.gov.au/about-asic/corporate-publications/newsletters/market-integrity-update/market-integrity-update-issue-73-july-2016/

Some common tactics and behaviour in these SMRs are detailed below. These apply to both retail and wholesale customers. More detailed indicators and scenarios on insider trading and market manipulation are in ASIC's Regulatory Guide 238.[5]

Insider trading (13 per cent of SMRs):

- Customers buying and selling shares while in possession of unpublished price sensitive information
- Senior employees of a company listed on the ASX buying or selling shares in their company just before a significant market announcement
- Significant and aggressive trading just before a price sensitive market announcement
- Stockbrokers having access to price sensitive information and passing this on to their clients
- Customers opening trading accounts and leaving them dormant for an extended amount of time, then suddenly purchasing shares and looking to sell a few days later
- Trading activity that is inconsistent with the usual trading activity of the customer
- Pre-arranged trading where sellers already have buyers lined up for their shares
- Stockbrokers suspected of 'front running', where they undertake trading activity using information about their customer's impending trade orders for the benefit of their firm or themselves.

Market manipulation (eight per cent of SMRs):

- 'Wash trading' involving buying and selling stock simultaneously to manipulate and artificially inflate the share price to encourage other investors to trade
- Conducting trades at the close of the day, impacting the closing price for the day
- Unusual trades that do not make economic sense but have an impact on the overall share price
- Customers buying/selling shares in ASX listed companies in which they hold senior positions or are major shareholders
- Selling a significant number of share units and buying approximately the same number of share units at corresponding sale prices within a very short time frame, where there is no change of beneficial ownership
- Customers placing buy/sell instructions themselves via different trading platforms
- A large number of orders (often for very small volumes) entered and cancelled with no readily identifiable commercial rationale
- Buying shares above the offer price to cause price increases
- Placing orders and cancelling the order shortly after
- Buying a small volume of shares near the close of day
- Targeting stocks that are low-priced illiquid 'penny' stocks.

REPORTING TO AUSTRAC AND ASIC

Market participants have an obligation to report SMRs to AUSTRAC if they form a suspicion on reasonable grounds, relating to insider trading or market manipulation, among other suspected offences.

Suspicious activity reports (SARs) are also reportable to ASIC regarding suspicious activity relating to insider trading and market manipulation. Market participants are not required to submit a SAR to ASIC if the information has been reported to AUSTRAC in an SMR. However, market participants must always report an SMR to AUSTRAC to satisfy their obligations under the AML/CTF Act, even if they have already reported the matter in a SAR to ASIC.[6]

There are some matters reportable to ASIC in a SAR, but are not required to be reported to AUSTRAC – for example, where a person or entity is not a customer of the market participant, and where there is no 'customer' (such as when a market participant is engaged in proprietary trading).

5 See in particular pages 11-16, http://download.asic.gov.au/media/3549356/rg238-published-24-february-2016.pdf

6 ASIC, *Regulatory Guide 238 –Suspicious activity reporting*, 2015, http://download.asic.gov.au/media/3549356/rg238-published-24-february-2016.pdf

TAX EVASION

The level of SMR reporting on tax-related offences was low. Ten SMRs were submitted to AUSTRAC in the two-year sample period with tax evasion as the suspected offence type. Analysis of the 'grounds for suspicion' revealed the following tactics, all of which apply to both retail and wholesale customers:

- the use of OSPs to hide beneficial ownership
- transfer of shares from an Australia-based account to an account held in a low-tax country
- wash trading where a customer sells their shares and acquires them again at a lower price, to create a capital loss in order to obtain a tax benefit. The ATO has released a Taxpayer Alert in relation to this issue.[7]

Although the level of SMR reporting to AUSTRAC is low, other AUSTRAC and partner agency intelligence indicates the threat may be more significant, primarily due to customers using OSPs to conceal beneficial ownership of shares to evade tax.

One AUSTRAC case study (available on AUSTRAC's Case Study Hub website)[8] describes how a suspect used offshore companies to avoid paying millions of dollars in tax. The individual used an OSP to establish several offshore companies. The suspect then sold ASX shares to the offshore companies below the true market value in an off-market transfer. By doing this, the suspect reduced their tax liabilities in Australia, yet still maintained control of the shares. The shares were then sold at market value via the offshore companies, and the funds were returned to the suspect in Australia disguised as loans from the offshore companies. By doing so, the individual avoided paying tax on the proceeds in Australia.

Similarly, recent AUSTRAC partner agency investigations identified Australian individuals using a combination of foreign entities, nominee arrangements and OSPs, some of which were in low-tax jurisdictions. This was to create offshore structures to disguise beneficial ownership, in an effort to evade domestic tax obligations. The tactics and methods employed to set up these arrangements can be highly sophisticated, involving the creation of multiple entities across several jurisdictions.

The jurisdiction section of this assessment highlights the lack of SMRs submitted on this issue, and flags this as an area for improvement by reporting entities.

MITIGATING THE THREAT OF TAX EVASION

One reporting entity engaged for this assessment outlined significant measures it had undertaken to combat tax evasion, including:

- revised the terms and conditions that customers sign up to, including a requirement that all new customers sign a declaration that the funds they are investing are 'tax compliant'
- revised terms and conditions sent to all existing customers
- rolled out extensive training to relationship managers, resulting in increased reporting of potentially suspicious matters relating to tax evasion
- implemented enhanced screening of customers, including 'negative news' about customers, which resulted in an increase in suspicious matter alerts
- developed a list of tax evasion indicators and applied these to the entire customer database, which resulted in significant changes to the customer base, with a number of customers exited.

These and other measures were rolled out within the private banking business of the firm, which included customers trading in securities and derivatives markets through the firm. The measures led to a considerable shift in the culture within the organisation.

OTHER OFFENCES

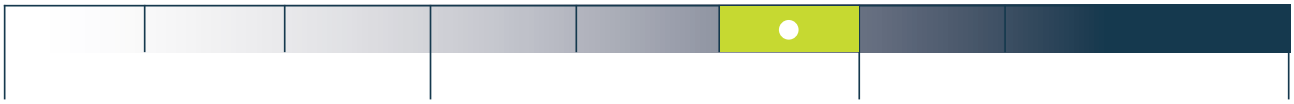
Five per cent of SMRs reported various other types of suspicious activity. Some of these related to concerns that customers had fallen victim to online share trading scams. Some SMRs also reported suspicions that customers were providing trading services to other customers, without holding an AFSL.

Other suspicious indicators reported in these SMRs included customers not being able to verify employment, or customers asking detailed questions about AML reporting. The issues outlined in these SMRs generally apply to retail customers.

7 ATO, *Taxpayer alert*, 2008, http://law.ato.gov.au/atolaw/view.htm?DocID=TPA/TA20087/NAT/ATO/00001

8 AUSTRAC, *Case studies hub - Suspect used offshore companies to avoid paying millions in tax*, 2013, http://www.austrac.gov.au/case-studies/suspect-used-offshore-companies-avoid-paying-millions-tax. This case study was not part of the SMR dataset analysed for this risk assessment.

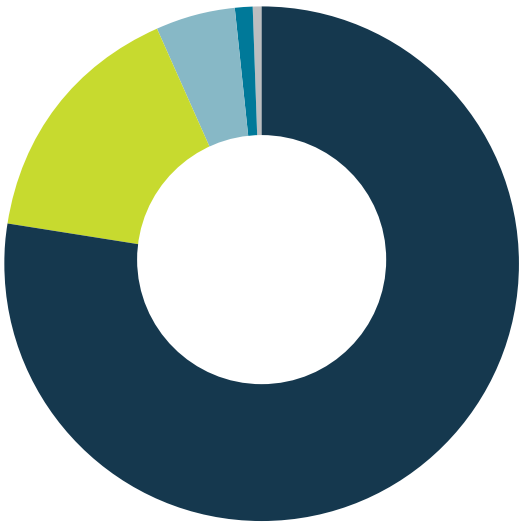
VULNERABILITIES

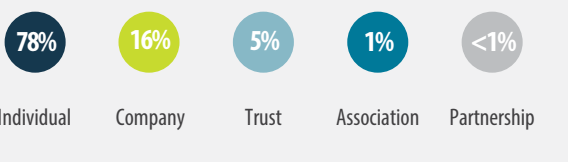


AUSTRAC assesses that there is a **MEDIUM** level of vulnerability to ML/TF in the securities and derivatives sector. Vulnerability refers to the characteristics of a sector that make it susceptible to criminal exploitation. This includes customer types, source of funds and wealth, products and services, delivery channels, use of cash, and the foreign jurisdictions with which it deals. Sector vulnerability also takes into account the operational vulnerabilities common among businesses in the sector, as well as the AML/CTF systems and controls in place across the sector.

CUSTOMERS

The chart below shows the extent to which different customer types appeared as the suspected party in the SMRs analysed for this assessment. It shows a range of customer types present in the securities and derivatives sector.





INDIVIDUALS

According to the ASX, 6.7 million Australians own shares or other listed investments.[9] The size of the customer base presents a significant vulnerability for reporting entities seeking to identify customers who are potentially engaged in criminal activity.

Individuals were reported as the customer type in 78 per cent of SMRs in the sample period. Of these SMRs, the majority related to suspected cases of fraud and money laundering. However, individuals were reported across all criminal threats outlined in the previous section.

A customer's occupation can be an important factor in determining the risk posed by individual customers. Of the SMRs that contained information about the customer's occupation (35 per cent of the total), the majority either:

- worked in the finance industry
- were owners, managers or directors of businesses and/or companies
- were unemployed.

CORPORATE ENTITIES AND TRUSTS

Of the SMRs (16 per cent) in which the customer type was a company, the most reported suspected offences were insider trading/market manipulation and money laundering. Many of these customers are likely to be wholesale customers.

A small percentage (five per cent) of SMRs related to trusts, with the majority of these related to suspected cases of fraud.

A substantial proportion of the ASX market is owned by foreign entities, nominees and custodial service providers. Partner agency intelligence has identified cases where Australian residents have used these types of entities to obscure their beneficial ownership, in order to anonymously commit a range of illegal activity including money laundering, insider trading, market manipulation and tax evasion.

9 ASX, *Corporate Overview,* 2016, http://www.asx.com.au/about/corporate-overview.htm

COMPLEX OWNERSHIP STRUCTURES USED TO OBSCURE BENEFICIAL OWNERSHIP

Unnecessarily complex ownership structures involving companies and trusts are an indicator that the customer is potentially involved in illicit activity. This applies regardless of whether the customer is based onshore or offshore.

Reporting entities are required to identify and verify the beneficial owners of these corporate entities. This can be achieved by asking additional questions to understand the control structure, requesting information from the customer, and other due diligence. To minimise this vulnerability, it is critical to have robust processes that ensure beneficial ownership and ownership structures are well understood.

There are often situations in this sector in which the customer is in fact another market participant or CFD/FX provider, and therefore also a reporting entity. Several SMRs analysed for this assessment were submitted by a reporting entity with respect to another market participant or CFD/FX provider which was suspected of criminal activity. These SMRs were generally in relation to insider trading and market manipulation offences.

Such situations can also mean that monitoring the overall financial activity of the ultimate customer can be difficult for the reporting entity, due to the multiple layers of separation. Some entities also described far more complex arrangements involving multiple parties based onshore and offshore.

Further complicating this issue is the fact that some wholesale customers routinely execute business through a number of market participants. While trading may appear suspicious to one broker, an examination of trading in aggregate through many brokers often reveals conduct that does not warrant formal investigation by ASIC. Reporting entities are, however, encouraged to continue reporting matters they believe to be suspicious.

However, some corporate entity customers in the securities and derivatives sector could be considered lower risk than other customer types when:

- they are also regulated entities under Australia's AML/CTF regime
- they are subject to oversight by other regulators, such as ASIC or APRA
- they have strong internal governance arrangements and controls, including detailed compliance programs
- they have employee screening, engagement and accountability mechanisms, and customer transaction monitoring programs.

POLITICALLY EXPOSED PERSONS (PEPs)

Only a very small number of SMRs submitted in the sample period related to PEPs. Reporting entities engaged for this risk assessment described a range of controls to mitigate risks posed by PEP customers, including:

- checking customer names against PEP lists at onboarding and periodically throughout the customer relationship
- applying high-risk customer due diligence for all PEPs even if they were not formally assessed as high risk
- declining PEP accounts where there is credible information that the PEP's source of wealth/funds was derived from the misuse of their position
- monitoring sensitive incidents involving local government representatives, such as bribery and corruption charges, and raising the risk rating accordingly
- not accepting PEPs for securities and derivatives products.

Reporting entities are reminded of the requirement under the AML/CTF Rules to screen their customer base for domestic and foreign PEPs, including for immediate family members and close associates of PEPs. PEPs may also be embedded in the ownership structure of a corporate customer.[10]

AGENTS AND THIRD PARTIES

The use of agents and third parties by customers can create higher levels of risk due to the added level of separation between the customer and the reporting entity.

Some reporting entities noted that the use of agents based offshore to introduce and refer new clients presented very significant risks. These included difficulties obtaining relevant and correct certification of identification, and issues with third-party authorisation documents. To address this, a few reporting entities described reviews and other assurance activities they had undertaken offshore, including in China, to properly understand and treat the risks posed by offshore-based agents. Despite this, issues associated with translated documents, common customer names, and a general lack of understanding of the local environment, meant reporting entities still struggled to fully understand and mitigate the risk.

The use of agents was reported in a small number of SMRs submitted during the sample period. Some common scenarios in these SMRs involved an agent or third party having an authority to act on a customer's account, unauthorised activity taking place by an unknown third party (fraud), and an off-market transfer to a third party.

10 The requirement for reporting entities to screen for domestic PEPs commenced on 1 June 2014. Under the *Policy (Additional Customer Due Diligence Requirements) Principles 2014*, reporting entities needed to take reasonable steps to comply with these requirements and be fully compliant with them after 31 December 2015.

A small number of SMRs highlighted the involvement of a financial planner in the provision of share trading services. Many of these reports related to cyber-enabled fraud involving an attempt to hack a customer's account and/or email.

One reporting entity highlighted that it did not accept customers who have someone trading/acting as an agent on their behalf. The reporting entity advised that in this scenario it would end the relationship and submit an SMR.

SOURCE OF FUNDS AND WEALTH

Reporting entities are required to consider information relating to a customer's source of funds and/or wealth in identifying its ML/TF risk.

Analysis of AUSTRAC data showed that the majority of SMRs relating to source of funds/wealth concerns involved structured and large cash deposits, ranging from $20,000 to around $700,000.

Many reporting entities engaged for this risk assessment disclosed that establishing source of funds was a difficult task. The lack of visibility some reporting entities have over the movement of funds from general transaction accounts into trading accounts contributes to this problem. Some entities described significant challenges in identifying the source of funds and wealth of offshore-based customers.

Some reporting entities described useful procedures to determine the source of funds and wealth, such as:

- obtaining information about the savings and earnings of a customer at the onboarding stage
- updating savings and earning information annually to maintain an up-to-date customer profile
- calculating the amount of funds a customer would be able to deposit based on their stated wealth and income
- requiring customers to provide copies of bank statements of general transaction accounts (for example, held with the customer's bank), which are used to fund the customer's trading account (with a market participant or CFD/FX provider). This allows the market participant or a CFD/FX provider to determine whether any financial transactions appear unusual or suspicious.

PRODUCTS AND SERVICES

AUSTRAC assesses that the securities and derivatives sector offers four main products and services that are vulnerable to criminal misuse: accounts, trading, off-market transfers, and third-party payments.

ACCOUNTS

During consultations with AUSTRAC, industry advised that customers may hold a variety of accounts to facilitate investments in securities and derivatives. These accounts can carry significant vulnerabilities for reporting entities as customers often transfer funds to and from general transaction accounts and trading accounts via electronic funds transfers, BPAY and credit card payments. As the table below shows, 355 SMRs in the sample period nominated this type of activity. [11]

Account-related transaction types nominated in SMRs

Transaction type	No. of SMRs
Account deposit	163
Account withdrawal	117
Account opening	37
International funds transfer out of Australia	26
International funds transfer into Australia	12
Total	**355**

SMRs in relation to account deposits and withdrawals were mostly suspected cases of money laundering, particularly large and structured deposits. Of the SMRs relating to the opening of accounts, many involved the use of fake identification to open these accounts.

11 Not all SMRs contained information about the transaction type.

During consultations with AUSTRAC, reporting entities highlighted various processes they had in place to mitigate the risk that transaction or trading accounts could be misused or compromised. These included:

- having policies requiring customers to set up both a transaction and a trading account with the same financial institution to enhance their visibility over the customer's transactions
- maintaining trust accounts for customers to prevent deposits being made directly into the financial institution's corporate account
- only accepting deposits from bank accounts held in the same name as the trading account holder
- placing limits on the amount of money that could be deposited into accounts.

One reporting entity advised that it had controls in place to mitigate the risk of accepting suspicious withdrawal requests. For example, before processing large cash withdrawals, the reporting entity notified customers when changes to their account details were initiated, to ensure it was the real customer making the request.

Reporting entities also noted it could be difficult to determine the origin or destination of a funds transfer when trading activity was funded or settled by credit cards, BPAY or electronic funds transfers. Some reporting entities told AUSTRAC that in such instances, they requested copies of credit cards or bank account statements from the customer, to ensure the name on the credit card or bank statement matched the trading account name.

TRADING

Trading is another service provided by market participants and CFD/FX providers that is vulnerable to financial crime. With some 929,000 trades conducted per day on the ASX, the volume of trading activity presents significant vulnerabilities for reporting entities.[12]

As the table below shows, 143 SMRs in the sample set contained a trading-related transaction type. Not surprisingly, these SMRs were largely associated with suspected insider trading and market manipulation offences.

Trading related transaction types nominated in SMRs

Transaction type	No. of SMRs
Acquire securities	47
Dispose securities	53
Acquire derivatives/futures	38
Dispose derivatives/futures	5
Total	**143**

A large number of the 'dispose securities' SMRs were related to suspected cyber-enabled fraud offences. The majority involved customer emails being hacked by a fraudster, who then requested positions to be closed out and the proceeds of the transaction to be transferred to other accounts.

Some reporting entities noted it was difficult to identify criminal misconduct from trading activity alone. They stressed the importance of conducting appropriate levels of due diligence on the customer before trading occurred.

Several entities advised that the need to execute client orders very quickly, particularly in volatile markets, often stretched an organisation's capacity to properly scrutinise a customer's trading behaviour and identify potentially unusual or suspicious behaviour.

A further challenge is that many customers use a number of brokers and market participants to trade. As such, detecting suspicious trading activity can be problematic as reporting entities do not have the full picture of the customer's trading activity and open positions.

12 ASX, *Corporate Overview*, 2016, http://www.asx.com.au/about/corporate-overview.htm

OFF-MARKET TRANSFERS

A small number of SMRs related to off-market transfers. The activity described included:

- conducting an off-market transfer to move value to a foreign jurisdiction or different entity in a suspected effort to launder funds
- conducting an off-market transfer to move value to offshore companies located in low-tax jurisdictions, potentially to avoid tax
- a third party attempting to illegally transfer ownership of shares by submitting a fraudulent off-market transfer form.

One reporting entity engaged for this assessment had significant concerns about the use of falsified documents and potential cases of fraud in the off-market transfer process.

Despite the small number of SMRs that relate to off-market transfers, AUSTRAC assesses that there is a significant level of vulnerability associated with off-market transfers. This is primarily due to the ability to effectively transfer wealth or value without trading on an exchange.

Off-market transfers carried out by market participants as a service to their clients present significant vulnerabilities if the identity of the receiving party is unknown or unclear, or is not also a customer of the financial institution. Some firms advised AUSTRAC that, in these cases, extra due diligence and controls would be applied to the third party. ASIC observed that off-market transfers could also be used to avoid market surveillance scrutiny.

THIRD-PARTY PAYMENTS

During AUSTRAC consultation with industry, many reporting entities highlighted that payments to third parties were a major risk in the sector. Payments were generally in relation to trading activity. In such cases, reporting entities described controls in place to mitigate risks, including allocating registered accounts to the third party, or requiring prior approval from the customer and identification of the third party. This issue can apply to retail and wholesale customers.

AUSTRAC was also advised that some market participants arrange payments to third parties entirely unrelated to any trading activity. This is essentially an added service the institution provides to a valued customer, and may include sending funds overseas. Due to the risks involved in transferring funds to overseas accounts, this type of service requires significant oversight. Where the customer's name is not included in the international funds transfer instruction report to AUSTRAC, this type of transfer would be non-compliant with AML/CTF obligations.

Some entities noted that in certain circumstances third-party payments may be normal behaviour. Reporting entities should be able to readily identify when third-party payment requests from a customer are unusual and require greater scrutiny.

DELIVERY CHANNEL

'Delivery channel' refers to the methods by which reporting entities deliver services and products to their customers. Most customers in the securities and derivatives sector trade online with minimal or no face-to-face interaction with a broker. Three of the financial institutions engaged for this assessment delivered their products exclusively online.

Online delivery of services makes this sector vulnerable in a number of ways, including:

- the absence of a face-to-face relationship between a customer and a stockbroker can make it difficult to identify the legitimacy of transactions or form suspicions about customers
- the frequent use of email communication between financial institutions and customers creates a favourable environment for cybercrime
- the online creation of accounts may allow fraudulent accounts to be created because audits and customer due diligence are conducted after the event.

However, some entities engaged for this risk assessment noted that online services allow them to deploy technology-based controls, which can be highly effective in mitigating risks.

Entities that allow their customers to trade via DMA – a form of electronic trading – may be exposed to additional vulnerabilities associated with online trading. A small number of SMRs related to suspected offences of insider trading and market manipulation when customers were trading via DMA. Some market participants engaged for this risk assessment noted that post-trade monitoring is particularly important to identify suspicious trading conducted via DMA.

MITIGATING DELIVERY CHANNEL RISK

Reporting entities engaged for this assessment described a range of controls they had in place to mitigate risks posed by online services and trading activity, including:

- procedures to call back customers to ensure that the actual customer was requesting the order or transaction
- frequent communication with customers in an effort to gain knowledge of customers' financial situations and preferred methods of transacting
- electronic alerts identifying the location of IP addresses and the legitimacy of email addresses
- providing warnings to customers about the legitimate email domains they use, to help customers identify fraudulent emails
- in certain circumstances, blocking trades when there is a suspicion of fraudulent activity.

FOREIGN JURISDICTION

Australia has the Asia-Pacific region's second most active stock market (after Japan) and attracts many international investors.[13] Some 45 per cent of the ASX market is owned by foreign entities.[14] One reporting entity noted that 22 per cent of new accounts opened over an 18-month period were for customers based overseas, mostly in AsiaPacific countries. Other entities engaged for this assessment noted that they only accepted Australia-based customers.

In the dataset, 206 SMRs (31 per cent) reported activities which related to a foreign jurisdiction, including where one of the parties listed in the SMR was a foreign citizen or based in a foreign jurisdiction. The majority of these reports related to suspected cases of fraud, such as accounts funded with fake credit cards, or trading accounts set up with fake identification documents. However, some SMRs related to other suspected offences including money laundering, insider trading and market manipulation.

49 foreign jurisdictions were mentioned in these SMRs. As the table below shows, almost three quarters of these SMRs (148) referenced just 12 countries, with China and Hong Kong combined accounting for a quarter of all these SMRs.

Country	Number of reports
China	31
UK	24
Hong Kong	19
Canada	13
South Africa	11
Singapore	10
Indonesia	9
New Zealand	7
India	7
Russia	6
USA	6
Netherlands	5
Other	58
Total	**206**

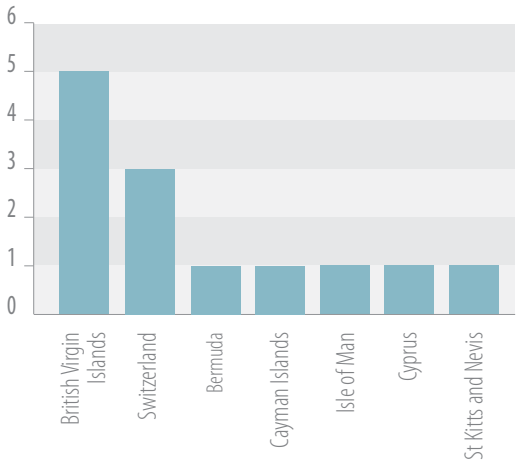
13 IBIS World, *Industry Report K6411a - Investment Banking and Securities Brokerage in Australia*, 2015, https://www.ibisworld.com.au/industry-trends/market-research-reports/financial-insurance-services/investment-banking-securities-brokerage.html

14 As of June 2016, provided by ASX

Customers with a link to low-tax jurisdictions also present higher risks. While there may be legitimate reasons for setting up corporate structures in low-tax jurisdictions, they are also highly vulnerable to being misused to support and facilitate criminal activity.

As the chart below shows, there were only 10 SMRs relating to low-tax jurisdictions. Of these, only two related to tax evasion. The remaining eight SMRs detailed other offences including money laundering, fraud and insider trading. Multiple low-tax jurisdictions were named in three of these SMRs (which is why the number of SMRs in the chart totals 13).

SMRs RELATING TO LOW-TAX JURISDICTIONS



There is significant scope for improvement in the submission of SMRs to AUSTRAC in relation to low-tax jurisdictions. The case below is a good example of improved SMR reporting. Developing a sound understanding of this vulnerability is a critical first step.

OFFSHORE LOW-TAX JURISDICTIONS – DETAILED SMR ASSISTS LAW ENFORCEMENT

One SMR in the dataset for this risk assessment provides an excellent example of a reporting entity undertaking additional checks to investigate the offshore element of a customer's ownership structure, and subsequently revealing a criminal threat. The information provided in the SMR was of high intelligence value to AUSTRAC and its partner agencies.

The SMR related to a case investigated by an AUSTRAC partner agency. In this case, Australian residents were suspected of tax evasion by using OSPs to set up corporate entities to obscure the beneficial ownership of shares. The reporting entity provided the following details in the SMR:

- several customer accounts used specialist OSPs as the registered address
- all companies linked to the customer accounts were found to be incorporated in the British Virgin Islands
- the directors of the companies were other companies incorporated in foreign jurisdictions with weak AML/CTF regimes
- the reporting entity had legal documentation linking some of the companies to an individual with an address in St Kitts and Nevis, despite not being able to find evidence of that address or individual in St Kitts and Nevis.

The reporting entity worked with a partner agency to effectively identify and suspend multiple accounts.

USE OF CASH

Cash transactions are a significant indicator of money laundering, particularly at the 'placement' stage, which involves entering illicit funds into the financial system.

Financial activity involving cash was part of the basis of suspicion in approximately 10 per cent of the SMRs analysed for this assessment. The most common suspected offence for cash-related SMRs was money laundering.

Cash can be placed into general accounts (that are linked to trading accounts) and through a series of transfers, made to look like the proceeds of securities and derivatives trading. Most of these involved suspicious behaviour involving large or structured cash transactions and unusual account activity. Further information on SMRs involving the use of cash is detailed in the money laundering section of this assessment.

All market participants and CFD/FX providers consulted for this assessment said they do not accept cash from customers, making them highly unlikely to be the target of placement activity. The key point of vulnerability for the sector is the retail banking sector, where cash can be placed and then moved electronically to the trading accounts of other entities. Where a customer carries out this transaction activity between entities in the same corporate group, the group has significant visibility over the customer's behaviour. This scenario was described in the majority of the cash-related SMRs.

There is a heightened level of vulnerability where a customer engages in cash transactions with one bank and transfers the funds to trading accounts held with unrelated entities, such as market participants and CFD/FX providers.

OPERATIONAL VULNERABILITIES

Engagement with partner agencies and industry indicates that there is extensive 'white labelling' of trading platforms in the sector, and that this is increasing. White labelling was viewed by several reporting entities as one of the highest internal risks faced by the industry.

Industry engagement indicates that there are various white-labelling arrangements in place across the sector, including variations in the roles and responsibilities of white labellers and market participants (or CFD/FX providers) regarding AML/CTF compliance activities. Poorly developed agreements and contracts that do not clearly indicate which entities are responsible for AML/CTF obligations could significantly undermine the AML/CTF framework.

Even where the terms of an agreement are comprehensive and robust, oversight might not be adequate to ensure entities are carrying out their reporting obligations. In addition, independent reviews may only look at one side of the relationship and not look at all entities involved in the white-labelling agreement. In this scenario, the independent review may not be effective in identifying all the AML/CTF issues.

Reporting entities emphasised the importance of having effective agreements as the critical control to mitigate this vulnerability. Other measures included having intermediaries complete due diligence questionaries, and maintaining ongoing and effective communication between parties to ensure a high standard of AML compliance is achieved by all parties involved in a white-labelling agreement.

Engagement with partner agencies revealed a potential vulnerability around smaller retail CFD/FX providers that are either foreign owned or foreign controlled. A number of foreign-owned or controlled AFSL holders lack an understanding and awareness of their Australian regulatory obligations. It is possible for these entities to be exploited and used to facilitate money laundering or other illegal activities.

AML/CTF SYSTEMS AND CONTROLS

The level of SMR reporting in the sector suggests that AML/CTF reporting mechanisms need to be strengthened to better detect financial crime and increase reporting to AUSTRAC.

Over the two-year sample period:

- 60 per cent of market participants did not submit an SMR to AUSTRAC
- 74 per cent of CFD/FX providers registered with ASIC did not submit an SMR to AUSTRAC.

AUSTRAC assesses that there is considerable scope for entities operating in these markets to improve their AML/CTF systems and controls to be able to identify and submit SMRs to AUSTRAC.

Front office staff, such as traders and advisers, can represent a vulnerability. Some reporting entities observed that client-facing front office staff can sometimes be complacent about AML/CTF due to their greater focus on retaining client business.

An AUSTRAC partner agency provided examples of front office staff facilitating criminal activity by assisting Australia-based customers to set up trading accounts in the name of their offshore companies, which are used to hide their beneficial ownership of shares in an effort to evade tax. Back office and compliance staff were not aware of this activity.

Issues surrounding front office staff are exacerbated in organisations that experience high turnover of front office staff, or who fail to adequately train these staff. Several entities engaged for this assessment expressed these concerns.

However, entities also emphasised that front office staff act as the first 'line of defence' in an organisation, especially in relation to attempted insider trading, market manipulation and tax evasion. Many SMRs detailed how front office staff were crucial in identifying and reporting on criminal threats.

CONSEQUENCES

The consequences of ML/TF in the sector are assessed as **MODERATE**. 'Consequences' refers to the potential impact or harm that ML/TF and other financial crimes may cause. Financial crime in the securities and derivatives sector has consequences for customers, reporting entities, the sector as a whole, and the broader Australian economy.

CUSTOMERS

Financial and indirect consequences for customers can include:

- financial losses from accounts and investment portfolios, and emotional distress as a result of fraud-related crimes
- loss of confidence in their financial institution if cases are prosecuted and appear in the media
- insider trading and market manipulation defrauding investors of their rightful gains, which are not 'victimless' crimes and undermine the integrity of the financial markets.[15]

SECURITIES AND DERIVATIVES SECTOR

The severity of the consequences vary from one reporting entity to another in the sector, depending on the extent to which they understand the ML/TF risks they face, have effective controls and strategies in place to mitigate these risks, and identify and submit SMRs.

Consequences for individual reporting entities could include:

- reputational damage, resulting in fewer customers
- public relations costs associated with regaining the confidence of investors and the community
- increased regulatory action
- increased internal and external audit costs
- erosion of financial performance and reduced dividend distribution for shareholders if financial institutions are required to:
  - undertake compliance remediation projects
  - increase investment in AML/CTF compliance controls such as transaction monitoring systems
  - review potentially thousands of transactions or customer identification records
- increased costs associated with combating cyber-enabled crime
- increased fraud insurance premiums.

Consequences for the securities and derivatives sector more broadly could include:

- inhibiting the capital-raising process for listed companies
- a diminished level of market integrity leading to a general loss in trust and confidence in the sector, and lower rates of investment and participation
- an adverse impact on earnings and revenue across the market.

15 ASIC, *Director share trading*, 2016, http://asic.gov.au/regulatory-resources/corporate-governance/corporate-governance-articles/director-share-trading/

AUSTRALIAN ECONOMY

Financial crime in the sector has the potential to have an impact on the broader Australian economy, including:

- reduction in taxation revenue, impacting on the delivery of critical government services
- adverse impact on the reputation of Australia's financial markets, which may result in reduced investment in these markets
- 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.

NATIONAL SECURITY AND INTERNATIONAL CONSEQUENCES

The national security and international consequences of terrorism financing in the securities and derivatives sector is assessed as minor, given the relatively low level of terrorism financing activity currently observed. However, the sector must remain vigilant to this threat, as undetected terrorism financing activity could have significant consequences.

FEEDBACK

AUSTRAC is committed to continual improvement and values your feedback on our products. We would appreciate notification of any outcomes associated with this report. Contact us at riskassessments@austrac.gov.au

APPENDIX

RISK ASSESSMENT METHODOLOGY

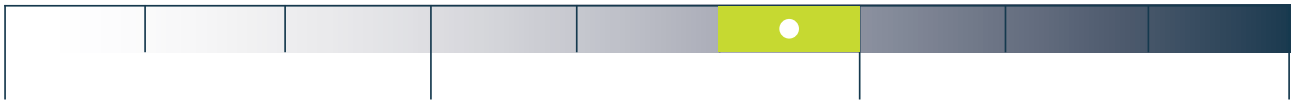
The methodology below covers 26 risk factors across three categories: criminal threat environment, vulnerabilities, and consequences. Each risk factor was assessed as low, medium or high, as per the table below. These assessments were based on quantitative and qualitative intelligence inputs, including analysis of SMR and other reporting data, intelligence assessments from partner agencies, and feedback from industry.

In assessing the **criminal threat environment**, six risk factors were considered - each was given equal weight. The average of these six ratings gave an overall rating for 'Threat'.

Sixteen factors were considered when assessing the sector's overall ML/TF **vulnerabilities**. These were grouped into eight subsections – customers, source of funds and wealth, products and services, delivery channel, foreign jurisdiction, use of cash, operational vulnerabilities, and AML/CTF systems and controls. The average of these eight subsections provided an overall rating for vulnerability.

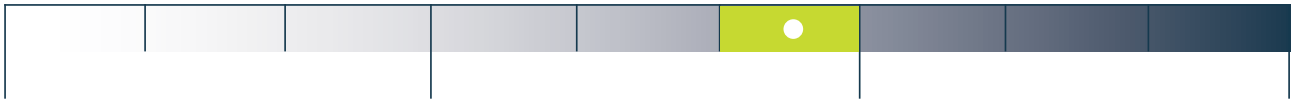
Four factors were considered in assessing the **consequences** of ML/TF activity within the sector - each factor was given equal weight. The average of these ratings gave an overall rating for ML/TF consequences.

CRIMINAL THREAT ENVIRONMENT



LOW	MEDIUM	HIGH
Unsophisticated tactics and methods used	Some sophisticated tactics and methods used	Highly sophisticated tactics and methods used
Low volume of cyber-enabled criminal activity	Moderate volume of cyber-enabled criminal activity	High volume of cyber-enabled criminal activity
Minimal targeting by serious and organised crime groups and/or foreign criminal entities	Some targeting by serious and organised crime groups and/or foreign criminal entities	Widespread targeting by serious and organised crime groups and/or foreign criminal entities
Low volume of money laundering	Moderate volume of money laundering	High volume of money laundering
Very few instances of raising and/ or transferring funds for terrorism financing	Some instances of raising and/ or transferring funds for terrorism financing	Many instances of raising and/ or transferring funds for terrorism financing
Low volume and/or limited variety of other offences	Moderate volume and/or some variety of other offences	High volume and/or large variety of other offences

VULNERABILITIES



LOW MEDIUM HIGH

Customers		
Simple customer types, mostly individuals	Mixture of customers types, with some complex companies and trusts	All customer types represented, including large numbers of highly complex companies and trusts
Minimal involvement of agents acting for customers	Moderate involvement of agents acting for customers	Significant involvement of agents acting for customers
Small customer base	Medium-sized customer base	Very large customer base
Very few PEPs	Some PEPs	Many PEPs
Source of funds and wealth		
Source of funds/wealth can be readily established	Some difficulty in establishing the source of funds/wealth	Source of funds/wealth difficult to establish
Products and services		
Product/service does not allow a customer to remain anonymous (ownership is transparent)	Product/service allows a customer to retain some anonymity (ownership can be obscured)	Product/service allows a customer to remain anonymous (ownership is opaque)
Small volume of transactions	Moderate volume of transactions	Large volume of transactions
Movement of funds cannot occur easily and/or quickly	Movement of funds can occur relatively easily and/or quickly	Movement of funds is easy and/or quick
Transfer of ownership of product cannot occur easily and/or quickly	Transfer of ownership of product can occur relatively easily and/or quickly	Transfer of ownership of product is easy and/or quick
Delivery channel		
Regular face-to-face contact, with minimal online/telephone services	Mix of face-to-face and online/telephone services	Predominantly online/telephone services, with minimal face-to-face contact
Foreign jurisdiction		
Very few or no overseas-based customers	Some overseas-based customers	Many overseas-based customers
Transactions rarely or never involve foreign jurisdictions	Transactions sometimes involve foreign jurisdictions, or a high-risk jurisdiction	Transactions often involve foreign jurisdictions, or high-risk jurisdictions
Use of cash		
Provision of product/service rarely involves cash, or involves cash in small amounts	Provision of product/service often involves cash, or involves cash in moderate amounts	Provision of product/service usually involves cash, or involves cash in very large amounts
Operational vulnerabilities		
There are very few operational factors that make the sector susceptible to criminal activity	There are some operational factors that make the sector susceptible to criminal activity	There are many operational factors that make the sector susceptible to criminal activity
AML/CTF systems and controls		
Sector is subject to all or most AML/CTF obligations	Sector is subject to partial AML/CTF obligations	Sector is not subject to AML/CTF obligations
At a sector level, significant systems and controls have been implemented to mitigate against criminal threats	At a sector level, moderate systems and controls have been implemented to mitigate against criminal threats	At a sector level, limited systems and controls have been implemented to mitigate against criminal threats

CONSEQUENCES

MINOR	MODERATE	MAJOR
Criminal activity results in minimal personal loss	Criminal activity results in moderate personal loss	Criminal activity results in significant personal loss
Criminal activity does not significantly erode the sector's financial performance or reputation	Criminal activity moderately erodes the sector's financial performance or reputation	Criminal activity significantly erodes the sector's financial performance or reputation
Criminal activity does not significantly affect the Australian economy	Criminal activity moderately affects the Australian economy	Criminal activity significantly affects the Australian economy
Terrorism financing activity has minimal potential to impact on national security and/or international security	Terrorism financing activity has the potential to moderately impact on national security and/or international security	Terrorism financing activity has the potential to significantly impact on national security and/or international security

www.austrac.gov.au

JULY 2017