



Australian Government

AUSTRAC



AUSTRALIA'S FINANCIAL PLANNING SECTOR >>>

MONEY LAUNDERING AND TERRORISM FINANCING
RISK ASSESSMENT

AUSTRALIA'S FINANCIAL PLANNING SECTOR



\$4.6
BILLION
IN REVENUE*



FINANCIAL
PLANNING
BUSINESSES*



20% 
OF ADULT AUSTRALIANS
SEEK FINANCIAL
A D V I C E**



25,000+
FINANCIAL
PLANNERS***

SUSPICIOUS MATTER REPORTS (SMRs) RELATING TO FINANCIAL PLANNING

FROM 1 APRIL 2014 TO 31 MARCH 2016



SMRs
SUBMITTED



REPORTING ENTITIES (REs)
SUBMITTED AT LEAST 1 SMR



REs SUBMITTED HALF
OF THE SMRs

* IBISWorld, *IBISWorld Industry Report K6419b: Financial Planning and Investment Advice in Australia*, 2016

** Based on the *ANZ Survey of Adult Financial Literacy in Australia* (May 2015), 20 per cent of adult Australians used a financial planner or advisor for financial advice in the last 12 months (2014 ANZ survey) <http://www.financialliteracy.gov.au/media/558752/research-anz-adultfinancialliteracysurvey2014-fullreport.pdf>

*** Australians Securities & Investments Commission Financial Adviser Register, December 2016.

CONTENTS

EXECUTIVE SUMMARY	4
PURPOSE	6
METHODOLOGY	7
REPORTING TO AUSTRAC	8
CRIMINAL THREAT ENVIRONMENT	10
Money laundering	12
Terrorism financing	13
Cyber-enabled fraud	14
Other fraud	15
Tax evasion	16
Welfare fraud	16
VULNERABILITIES	17
Customers	17
Source of funds and wealth	19
Products and services	19
Delivery channel	21
Foreign jurisdiction	22
Use of cash	23
Operational vulnerabilities	23
AML/CTF systems and controls	24
CONSEQUENCES	25
CONCLUSION	26
APPENDIX A: Risk assessment methodology	27

This risk assessment is intended to provide a summary and general overview; it does not assess every risk or product relevant to the financial planning sector. It does not set out the comprehensive obligations 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.

EXECUTIVE SUMMARY

OVERALL RISK RATING



AUSTRAC assesses the overall money laundering and terrorism financing (ML/TF) risk for the financial planning sector as **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.

CRIMINAL THREAT ENVIRONMENT



AUSTRAC has assessed that Australia's financial planning sector faces a variety of threats, some of which involve sophisticated tactics and methods. Intelligence agencies have observed instances of organised crime groups using financial planners to help navigate the financial sector.

Of the suspicious matters reports (SMRs) submitted to AUSTRAC related to the financial planning sector over a two-year period, around one-fifth related to suspected money laundering, often involving high-value transactions. Few incidents of terrorism financing have been reported in the sector; however, financial planners should remain vigilant to this threat.

The most frequently reported offence in the sector was cyber-enabled fraud, which accounted for half of all SMRs. This threat has been growing in scale and sophistication, with financial planners being targeted as they act as a gateway between customers and financial institutions.

Other fraud-related offences included scams, the use of false documents, as well as suspected cases of fraud conducted by financial planners. There were also a small number of SMRs regarding customer tax evasion and welfare fraud.

The true extent of criminal activity in the financial planning sector is likely to be greater than reporting levels indicate, as AUSTRAC assesses that there is significant under-reporting of suspicious matters by financial planners. Over two years, AUSTRAC received 273 SMRs related to the financial planning sector, which is very low considering around 20 per cent of adult Australians seek financial advice from some 25,000 financial planners across the country.

VULNERABILITIES



Financial planners play an important facilitation role for their customers to access financial services. This can make financial planners susceptible to exploitation for criminal purposes.

The specific characteristics of the financial planning sector that make it vulnerable to financial crimes include:

- the large customer base and significant amount of money movement being facilitated by financial planners
- the range and complexity of products and investment strategies being facilitated by financial planners
- the growing trend towards online delivery of financial planning services.

Financial planners who deal with foreign jurisdictions, accept cash, have customers who

are politically exposed persons (PEPs), or make payments to third-party accounts may be exposed to higher levels of risk than those that do not undertake these activities.

Factors that limit the overall vulnerability of the sector include the low level of customer anonymity for personal advice services and the low level of agents acting for customers.

AUSTRAC assesses that, at a sector level, financial planners have only a partial understanding of their anti-money laundering and counter-terrorism financing (AML/CTF) obligations, with many not fulfilling the requirements to have risk-based customer due diligence procedures and to submit SMRs to AUSTRAC. Almost all entities engaged for this assessment saw this lack of understanding as a significant vulnerability which undermines the sector's resilience to criminal financial activity.

CONSEQUENCES



The consequences of ML/TF activity in the sector are assessed as minor overall; however, there can be quite significant personal consequences for customers who incur financial losses due to criminal activity.

Consequences for financial planners could include crime-related financial losses, reputational damage, and increased costs associated with combating criminal activity, particularly IT security costs.

There may also be loss of confidence in the financial planning sector as a whole by both customers and product issuers.

Financial crimes in this sector may also impact the broader Australian economy; for example, through loss of investments as a result of fraud and reduced government revenue from unreported welfare fraud and tax evasion.

PURPOSE

This assessment provides sector-specific information to the financial planning industry on ML/TF risks at the national level. Its primary aim is to assist the sector to combat ML/TF crimes in Australia's financial system.

Financial planners have obligations under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) when they make arrangements for a person to receive a financial product or service in their capacity as a holder of an Australian Financial Services Licence (AFSL).¹ This is listed as designated service item 54 in Table 1, subsection 6(2) of the AML/CTF Act.²

This risk assessment has been developed as a feedback resource for the financial planning 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 financial planners 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.

AML/CTF obligations for financial planners

Reporting entities that **only** provide designated service item 54 have reduced obligations under the AML/CTF Act. They are required to adopt and implement a 'special AML/CTF program' in accordance with Chapter 5 of the AML/CTF Rules.³ Reporting entities that provide another designated service in addition to the item 54 service are required to implement a standard AML/CTF program.

Under a special AML/CTF program, financial planners are required to implement customer due diligence (CDD) procedures⁴, including:

- collecting and verifying customer identification information
- identifying and verifying beneficial ownership
- identifying whether a customer is a PEP
- obtaining information on the purpose and intended nature of the business relationship.

When implementing the special AML/CTF program, reporting entities are also required to consider the ML/TF risks posed by various factors, including (but not limited to):

- customer types
- customers' sources of funds and wealth
- delivery channel
- any foreign jurisdictions the reporting entity deals with.

¹ Or as an authorised representative of an AFSL holder

² For further information on designated service item 54, see <http://www.austrac.gov.au/definitions-and-examples-common-designated-services>

³ For further information, see the AUSTRAC Compliance Guide, Chapter 6 – AML/CTF programs: <http://www.austrac.gov.au/chapter-6-amlctf-programs>

⁴ For the purpose of this risk assessment, the term 'customer due diligence' is used in reference to the requirements as outlined in Chapter 4 of the AML/CTF Rules to conduct 'applicable customer identification procedures' (ACIP). Ongoing customer due diligence requirements (OCDD) do not apply to providers of designated service item 54, in accordance with subsection 36(3) of the AML/CTF Act.

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 assessed 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, designated service delivery channels and the foreign jurisdictions with which the sector 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 is determined for each category, which is then used to determine an overall risk rating for the sector. Further information on the methodology and how this was applied to the financial planning sector is at Appendix A.

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 financial planning entities, as well as industry experts and industry associations.

REPORTING TO AUSTRAC

Under the AML/CTF Act, financial planners, as reporting entities, have an obligation to report suspicious matters to AUSTRAC.⁵ A reporting entity must submit an SMR if they form a reasonable suspicion of money laundering, terrorism financing or other offences such as fraud or tax evasion.

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

For this risk assessment, AUSTRAC analysed in detail all SMRs lodged over a two-year period, where:

- the SMR had been lodged by a financial planner; or
- the SMR had been submitted by another financial institution, but a financial planner had identified the suspicious matter or had been involved in the transaction in some way.

AUSTRAC observed that a large range of values were reported in the SMRs during the sample period. Of the 152 SMRs that reported a dollar-figure value, 44 per cent had a value of less than \$50,000, and 24 per cent reported amounts greater than \$250,000; nine of these were worth over \$1 million.

AUSTRAC also analysed the SMRs to determine who the suspicious party was in each case. In 19 per cent of SMRs, the suspicious party was the customer of a financial planner. That equates to only one SMR being submitted per fortnight by financial planners nationwide in relation to their customers. This is a low rate of reporting, considering around 20 per cent of adult Australians seek financial advice.⁶ Most entities consulted for this assessment agreed that this figure was surprisingly low.

26 per cent of the SMRs in the sample dataset related to cases in which a financial planner was suspected of being involved in an offence. These were generally reported by banks and product issuers, and may reflect more advanced reporting practices by these institutions.

The remaining 55 per cent of SMRs related to offences in which a third party was the suspicious party. This includes parties that were unknown to the customer or financial planner (for example, cyber-criminals), or entities with a connection to a customer (for example, investment scammers).

SMRS RELATING TO FINANCIAL PLANNING

273 Number of SMRs submitted

67 Number of reporting entities submitting at least one SMR

5 Number of reporting entities accounting for half of all SMRs submitted

\$75.9M Total value of transactions reported in SMRs*
* 120 SMRs did not specify a value

1 April 2014 to 31 March 2016

⁵ For more information on when to submit an SMR, see section 41 of the AML/CTF Act and Chapter 7 of the *AUSTRAC Compliance Guide*

⁶ Based on the *ANZ Survey of Adult Financial Literacy in Australia* (May 2015), <http://www.financialliteracy.gov.au/media/558752/research-anz-adultfinancialliteracysurvey2014-fullreport.pdf>

Common misconceptions about suspicious matter reporting

AUSTRAC's engagement with the financial planning sector for this assessment revealed several industry misconceptions about SMR reporting. These misconceptions are likely to contribute to the low level of reporting by financial planners.

1. "The product issuer will report instead."

Some financial planners seemed to consider it the financial institution or product issuer's obligation to report SMRs. However, financial planners are also required to report SMRs to AUSTRAC, and may have information about a customer that the financial institution does not.

2. "I need to have conclusive evidence." An SMR must be submitted when a reporting entity forms a suspicion on reasonable grounds, regardless of whether there is conclusive evidence that any illegal activity has occurred. Information provided by financial planners in an SMR could assist with investigations by authorities.

3. "Reporting will damage the customer relationship." Some financial planners believed that reporting SMRs about their customers may damage the customer relationship and possibly jeopardise their future revenue stream. However, financial planners that submit an SMR are not required under the AML/CTF Act to discontinue the business relationship.

Furthermore, there are provisions in the AML/CTF Act which enable reporting entities to report on suspicious matters without compromising the confidentiality of the customer or the reporting entity. 'Tipping off' provisions prohibit reporting entities from disclosing information relating to an SMR to the customer or to other financial institutions. Should a court case be brought against a customer, the information in the SMR cannot be introduced as evidence in criminal proceedings,⁷ which provides further protection of confidentiality.

4. "Reporting means my business has done something wrong." Reporting suspicious matters to AUSTRAC demonstrates that the financial planner is acting in accordance with its AML/CTF obligations. In contrast, financial planners who do not submit SMRs, despite forming a suspicion on reasonable grounds, may become implicated and potentially put Australia's financial system and national security at risk.

⁷ Section 124 of the AML/CTF Act. An SMR can be used in criminal proceedings for certain AML/CTF Act offences, including tipping off (section 123) and providing false and misleading information offences (section 136).

CRIMINAL THREAT ENVIRONMENT



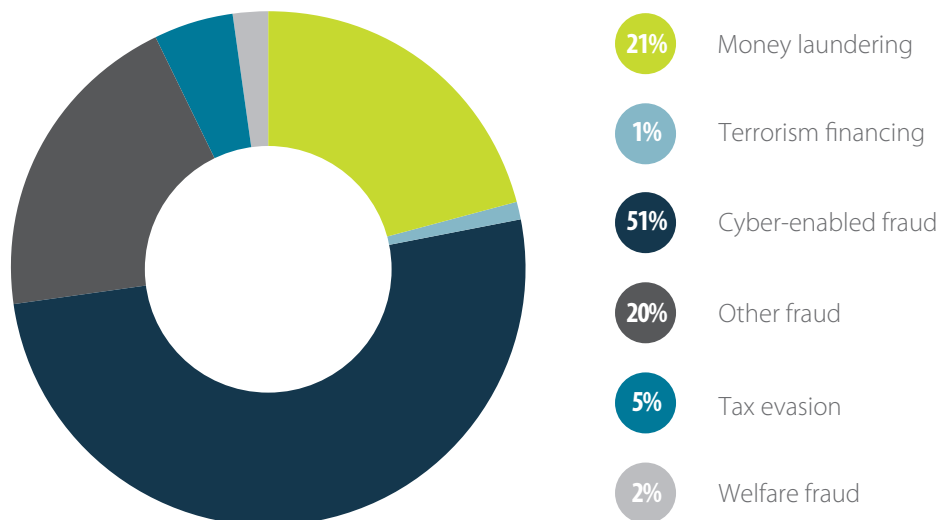
AUSTRAC assesses that there is a **medium** threat of criminal exploitation to Australia's financial planning sector. The sector is facing a variety of criminal threats, with criminals employing a range of sophisticated tactics and methods. Intelligence agencies have observed instances of organised crime groups using financial planners to help navigate the financial sector. Moreover, entities consulted for this risk assessment have observed that criminals are deliberately seeking out financial planners who have weak AML/CTF controls, or who turn a blind eye to suspicious behaviour.

Suspicious matter reporting to AUSTRAC identified six main offence types in the financial planning sector. Suspected money laundering accounted for a significant portion; while terrorism financing was

the subject of only three reports. The most reported suspected offence was cyber-enabled fraud. Other fraud-related offences included scams, the use of false documents, as well as cases of fraud conducted by financial planners. There were a small number of reports regarding tax evasion and welfare fraud.

These offences can occur at any stage of the cycle in which a customer engages a financial planner. Some potential indicators that financial planners should look for are detailed in the following graphic. Such 'red flags' should prompt a financial planner to investigate the matter further and potentially submit an SMR.

SUSPICIOUS MATTER REPORTING BY SUSPECTED OFFENCE TYPE



STAGE:

POTENTIAL THREATS AND RED FLAGS:

Client/planner
relationship
established

1



Customer enquires whether planner accepts large cash deposits



Customer requests advice on overly complex company/trust structures that go beyond their financial needs



Customer is reluctant to provide identification or behaves nervously



Customer requests advice on how to evade tax

Client information
is collected,
analysed and
evaluated

2



Customer documents inconsistent with expected formats, appear altered or have inconsistencies (e.g. date of birth)



Customer has unexplained wealth inconsistent with economic situation



Customer requests unusual/ uneconomic investments



Customer uses company/trust structures with unclear beneficial owners



Customer reveals they are misleading Centrelink for welfare benefits



Customer has suspicious property ownership arrangements



Customer has money in, or corporate entities based in, tax havens



Customer's name appears on a terrorism watch list

Financial planner
provides advice

3



Customer asks how to make an insurance claim before an insurable event takes place



Customer receives advice but chooses to implement the advice without the planner



Customer asks to establish an SMSF without being able to show source of funds/ownership for the initial transfer



Financial planner
arranges products

4



The members or trustees of an SMSF change several times over a short period of time



Funds from several sources are consolidated into customer's account

Financial planner
reviews or makes
variations to
portfolio

5



Product issuer receives email instructions from a financial planner, however it appears financial planner's email has been compromised



Customer changes bank details by email or online soon after changing contact details



Email request from customer expresses urgency



Customer makes structured or large cash deposits into their bank account to facilitate investments



Customer requests radical change to financial strategy

Withdrawal/
closure

6



Customer quickly withdraws funds soon after making initial investment



Planner receives withdrawal request from customer by email, but customer usually makes contact via telephone



Customer requests funds transfer to a conflict zone, or country neighbouring a conflict zone



Planner receives request for funds to be sent to a third party overseas

THREAT KEY:



Money
laundering



Tax
evasion



Fraud



Terrorism
financing



Cyber-enabled
fraud



Welfare
fraud

MONEY LAUNDERING

AUSTRAC SMR data indicates that the financial planning sector is being exploited to launder money and conceal the proceeds of crime. Reporting entities submitted 57 SMRs relating to suspected money laundering during the sample period, representing 21 per cent of the total. These SMRs generally had higher monetary values than SMRs related to other suspected offences; of the twenty SMRs in the sample period with the highest values, fourteen related to suspected money laundering.

Reporting entities nominated a variety of reasons for suspicion when submitting SMRs relating to money laundering (see diagram below).

25 of the money laundering SMRs identified customers as the suspicious party. Some examples of these suspicious matters were:

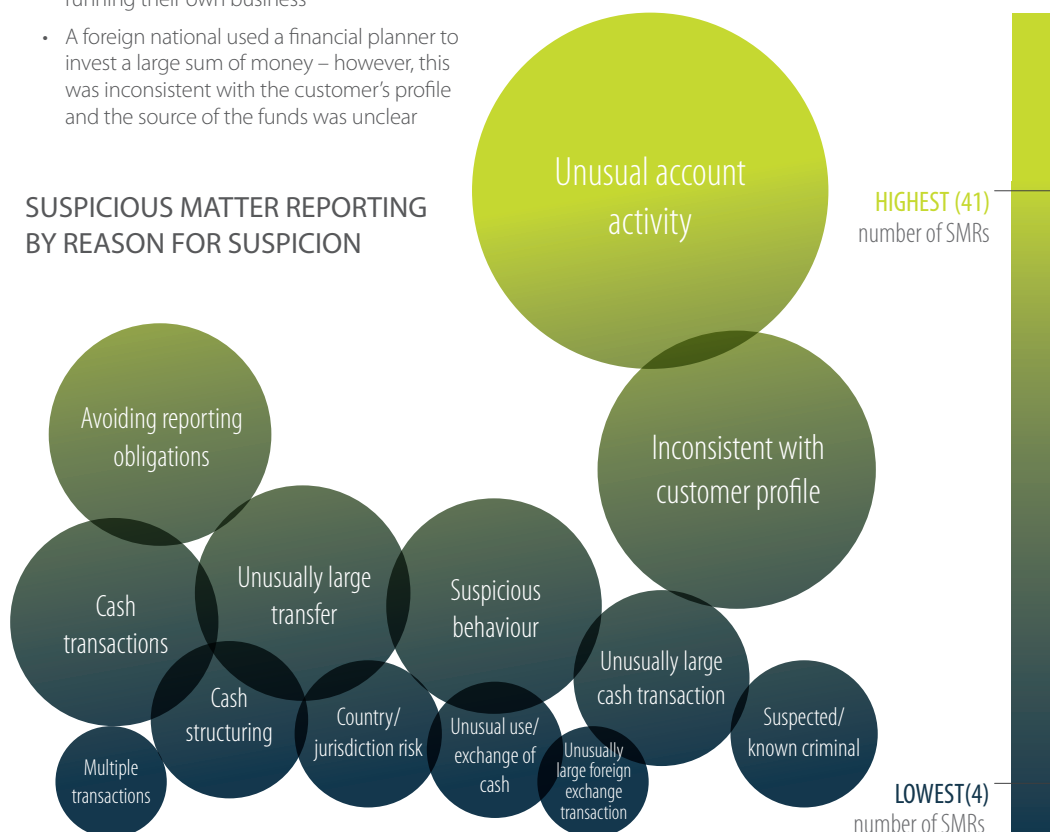
- A financial planner was approached by a prospective customer, who had accumulated cash savings well in excess of their annual income from running their own business
- A foreign national used a financial planner to invest a large sum of money – however, this was inconsistent with the customer's profile and the source of the funds was unclear

- A financial planner received a phone enquiry from an individual who was seeking advice, and that individual was known to be the subject of a corruption investigation.

A further 32 SMRs in this offence category related to cases in which a financial planner was suspected of being involved in a suspicious activity. Most of these involved structured cash deposits into financial planners' accounts. Some specific examples of SMRs include:

- A bank observed that a financial planner received a number of cash deposits of less than \$10,000 made by several different individuals at different bank branches, in an apparent attempt to avoid detection
- A bank received a request by a financial planner to transfer very large sums of money between numerous bank accounts held by the planner's customer, in what the bank suspected was an attempt to obscure the source of the funds.

SUSPICIOUS MATTER REPORTING BY REASON FOR SUSPICION



Note: More than one reason for suspicion can be nominated in an SMR

TERRORISM FINANCING

In the two-year sample period for this risk assessment, there were three SMRs regarding suspected terrorism financing.

In one SMR, a financial planner reported a matter where their customer appeared to either be the victim of, or complicit in, an internet scam. The customer intended to transfer a sum of money for investment purposes from their overseas bank account into their Australian account; however, the funds had been stopped by the originating bank. The financial planner investigated the matter further and found that the name of one of the overseas consultants advising the customer was listed on a crime list for suspected terrorist financing.

Another report came from a financial institution regarding a self-managed superannuation fund (SMSF). Shortly after making an initial rollover into the SMSF, the customer requested a large funds transfer to a high-risk jurisdiction for terrorism financing. The bank conducted enquiries with the customer's financial planner, which revealed inconsistencies around the purpose of the customer's request and prompted suspicion that the transfer would constitute an illegal use of SMSF funds and potentially involve terrorism financing.

In another case, a news article alerted the financial institution that one of their customers – who had been introduced by a financial planner – was involved in a counter-terrorism investigation.

Useful reporting for combating terrorism financing

There was one additional SMR reported by a financial planner outside the sample period of this risk assessment, which is an excellent example of positive reporting behaviour.

This SMR related to a customer who was transferring money overseas to a high-risk jurisdiction associated with terrorism financing. In the SMR, the financial planner noted they did not have detailed information directly linking the customer to terrorism, but still reported it to AUSTRAC due to the risk associated with the jurisdiction. Such information can be invaluable to AUSTRAC and law enforcement agencies, as it may contribute to current or future investigations.⁸

Other key indicators of terrorism financing can be found in the AUSTRAC report *Terrorism Financing in Australia 2014*.

⁸ When completing the SMR form, reporting entities should select 'Financing of terrorism' in the suspected offence type field if they suspect any link to terrorism financing, to ensure that the SMR is detected and escalated for priority action.

CYBER-ENABLED FRAUD

The most frequently reported suspected crime type in the financial planning sector was cyber-enabled fraud⁹, which accounted for 138 SMRs (51 per cent) in the sample period.¹⁰ Reporting entities consulted for this assessment concurred that cyber-enabled fraud was one of the most significant issues for the sector. Although this threat has been apparent in the sector for several years, it has been growing in scale and sophistication.

Financial planners are particularly vulnerable to cyber-enabled fraud attacks when acting as a gateway between customers and financial institutions or product issuers. There were many reported cases in which a third party hacked a customer's email and used it to instruct the financial planner to make a withdrawal or transfer of funds, often into intermediary, or 'mule', bank accounts. There were also cases in which a financial planner's email was hacked and used to email the product issuer to request a funds transfer, purportedly at the request of the customer.

Other sophisticated incidents have involved third parties:

- diverting a customer's phone number, in an attempt to circumvent callback controls
- accessing a customer's email history (including attachments, drafts and sent items) to more accurately impersonate the customer (for example, by referencing personal situations such as home renovations)
- using social media (either by hacking the account or relying on publicly available information) to gather information about the customer
- creating a new email account using the customer's name in order to impersonate the customer

- hacking an email account, and then creating an automatic forwarding rule so that emails from the financial institution are deleted
- hacking a customer's computer to compromise online banking accounts.

Many of the cyber-related SMRs reported by banks referenced the constructive role that financial planners played in resolving cases, as financial planners were often well-positioned to recognise anomalous behaviour. Some reporting entities had policies to ensure that financial planners personally called customers to verify transaction requests received by email. This had proved to be a critical mitigation technique.

Identifying potential cyber-enabled fraud attacks

Financial planners described a number of indicators used to detect instances of cyber-enabled fraud, including:

- customer's email has different tone/language to customer's usual communications
- customer's email has poor grammar, spelling mistakes or uncommon terminology
- customer usually contacts the financial planner by telephone, then suddenly makes contact by email
- customer changes bank details soon after changing other details such as contact address or phone number
- customer emails express urgency – for example, claiming the customer is travelling overseas, attending a funeral, or purchasing a property
- requests for the financial planner to complete application forms on the customer's behalf, then to send back to customer for signing
- email requests to send funds overseas.

⁹ 'Cyber-enabled fraud' refers to crimes where computers or ICT are an integral part of an offence, such as online identity theft.

¹⁰ Reporting entities are required to submit SMRs under Section 41(1)(d) when they suspect that the 'customer' of a designated service is not the real customer. This may occur when a customer has been the subject of a cyber-enabled fraud, such as email hacking or account hacking.

OTHER FRAUD

There were 55 SMRs in the sample period relating to types of fraud other than cyber-enabled fraud. In some of these cases, financial planners were concerned about the identity of customers or suspected that customers were using false documents. These SMRs included forms with signatures that did not match, superannuation clients providing identification with differing dates of birth, and customers who quickly withdrew their request for a financial service when asked to provide identification. Reporting entities also reported seeing cases of fake bank statements being provided to authenticate change of bank detail requests.

There were also cases relating to suspected scams. The most common forms of scams were: online dating and romance scams,¹¹ overseas investment schemes, requests to make large transfers to overseas accounts, and fake bank or legal letters convincing customers to make payments. In most cases, it was a financial planner who had detected that a customer was falling victim to a scam. In other cases, a customer was concerned about a potential scam and contacted their financial planner for advice. A small number of SMRs were from financial planners who suspected that their customer was operating a scam.

AUSTRAC also received SMRs indicating that financial planners were suspected of promoting scams to their customers, particularly international investment schemes.¹² For example, one bank reported that, based on the advice of a financial planner, a customer was investing their superannuation funds into a highly unusual derivatives product overseas. Another SMR related to suspected embezzlement of customer funds by a financial planner for personal use.

Banks and other financial institutions also reported other types of suspected fraud by financial planners. Some SMRs related to financial planners enabling customers to illegally access their superannuation before they had reached retirement age, particularly through SMSFs. More seriously, AUSTRAC also received an SMR where a financial planner transferred money out of a customer's SMSF without the customer's knowledge.

There were also reports of suspected fraud in which the motive of the financial planner was unclear, for example: forging customer signatures in documents; calling financial institutions impersonating the customer; or fraudulently providing employment letters for customers. Some cases involved financial planners having third party authority or power of attorney on customer accounts.

In a concerning trend, criminal intelligence agencies have observed that serious and organised crime groups may be either legally obtaining an AFSL, or claiming to hold one, and using this to promote investment schemes to unwary customers.

¹¹ Where a fraudster, usually based overseas, pretends to be a prospective companion for a victim in order to receive gifts, money or personal information about the victim.

¹² Schemes where promoters call or approach potential investors in order to peddle speculative or fraudulent investment opportunities. Often the promoter will use high-pressure tactics and be persistent to promote the scam.

TAX EVASION

There was a low number of reports submitted in relation to suspicions of tax evasion in the financial planning sector, with only 14 SMRs in the sample period. The transaction values reported in SMRs relating to suspected tax evasion were, on average, higher than the values reported in other SMRs.

Although financial planners may not see conclusive evidence of tax evasion, they generally receive a significant amount of financial and personal information about their customers which, in some circumstances, may be sufficient to form a suspicion that the customers are engaged in tax evasion. In such cases, financial planners are required to submit an SMR.

While customers often ask legitimate questions about tax minimisation strategies, financial planners may also see indicators of potential tax evasion; for example, undeclared cash and foreign income, evidence of excessive tax deductions, or suspicious property ownership arrangements. Financial planners should ensure that their services are not being used to facilitate tax evasion, and should be alert to potential high-risk characteristics such as customers that are complex offshore entities, have several layers of corporate and/or nominee shareholders and directors, or are based in offshore jurisdictions.

WELFARE FRAUD

There were six SMRs in the sample period regarding customers potentially carrying out fraud against the welfare system. These included cases of not declaring income to Centrelink, or continuing to claim a spouse pension after the end of a relationship. This type of detailed personal and financial information is often revealed to financial planners at the initial stages of onboarding a customer.

Financial planners told AUSTRAC that they often informed customers of the need to declare income and change of circumstances to Centrelink; however, financial planners are reminded that suspected welfare fraud by their customers – as an offence against a law of the Commonwealth – should be reported in an SMR to AUSTRAC.

VULNERABILITIES



AUSTRAC assesses that there is a **medium** level of vulnerability to ML/TF in the financial planning 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, designated service delivery channels, use of cash, and the foreign jurisdictions with which it deals. Sector vulnerability also takes into account the operational vulnerabilities that are common among businesses in the sector, as well as the AML/CTF systems and controls in place across the sector.

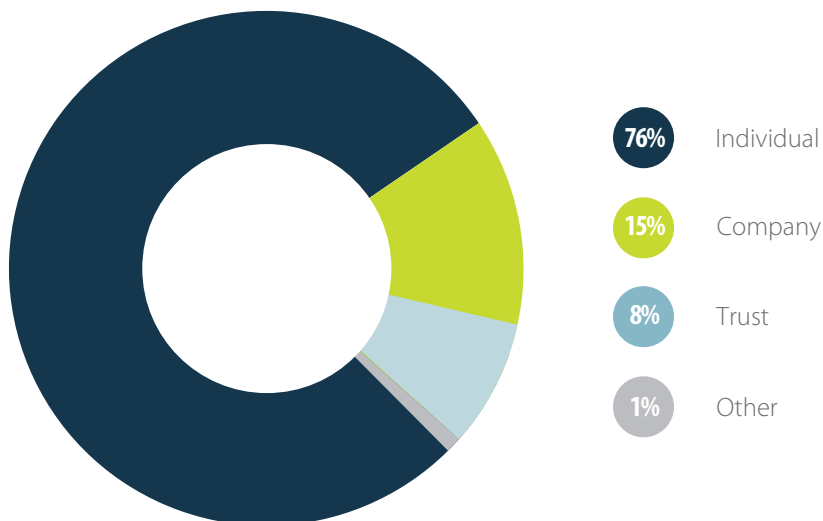
CUSTOMERS

Most SMRs lodged in the financial planning sector in the sample period were in relation to an individual, but companies and trusts were also represented.

INDIVIDUALS

The majority of customers in the financial planning sector are individuals. Reporting entities noted that they tended to have older customers, who were more likely to have acquired wealth or be planning for retirement. SMR reporting indicated that older customers were more vulnerable to cybercrime – for customers aged 61–70 years, 67 per cent of offences related to cyber-enabled fraud, compared to 39 per cent across all age groups (where the customer's age was included in the SMR). One financial institution reported that they were providing customer education services targeted towards older customers on cyber and IT security, to help address this.

SUSPICIOUS MATTER REPORTING BY CUSTOMER TYPE



Wholesale clients

Financial planners are required to submit SMRs with respect to wholesale clients. Although the *Corporations Act 2001* differentiates between wholesale and retail investors, the AML/CTF Act does not. This means that for wholesale clients, there is a requirement to undertake customer due diligence as outlined in the Purpose section of this assessment.

CORPORATE ENTITIES AND TRUSTS

Of the SMRs in the sample period that related to non-individual entities, 42 related to companies; around half of these SMRs reported suspected money laundering offences. Another 23 SMRs related to trusts.

Although not all financial planners deal with companies and trusts, feedback to AUSTRAC from industry was that those financial planners who do deal with corporate customers often did not adequately assess the risks associated with those customers.

A significant challenge for financial planners is identifying the beneficial owner of a corporate entity, which in turn presents a vulnerability for the sector. The vulnerability is increased, for example, where a trust is established to conceal the owner's identity; or a financial planner does not adequately identify the beneficial owner at the onboarding stage; or a customer is reluctant to discuss the role or purpose of the company or trust.

Several institutions suggested that complex ownership structures involving overseas entities are a key risk indicator, as these have been used to conceal the identity of offshore owners and foreign PEPs.

POLITICALLY EXPOSED PERSONS

Financial planners are required under the AML/CTF Rules to screen their customer base for domestic and foreign PEPs. Only a very small number of SMRs submitted by financial planners in the sample period related to PEPs. Although this may be because many financial planners do not deal with PEP customers, feedback to AUSTRAC from industry indicated that many financial planners were not fully aware of their obligations to detect PEPs and therefore may unknowingly have PEP customers.¹³ Financial planners are reminded of their obligation to identify PEPs and apply additional customer due diligence to these types of customers, including in higher risk scenarios such as when the customer is a foreign PEP.

AGENTS

The use of agents is generally considered to be higher risk; however, there were not many SMRs involving agents in the financial planning sector.

A small number of SMRs in the sample period mentioned the involvement of lawyers acting on behalf of customers in issuing instructions to financial planners. Most of these related to customers located or operating in foreign jurisdictions, and some involved money being moved into or out of a lawyers' bank account.

There were also cases of accountants being involved, sometimes acting as an agent for the customer. In some SMRs, financial planners worked with the customer's accountant to verify information and/or help resolve cases.

¹³ Further information about obligations relating to PEPs can be found on the AUSTRAC website (www.austrac.gov.au/part-b-amlctf-program-customer-due-diligence-procedures).

Financial planners in the box seat to know customers and detect suspicious wealth

Financial planners are in a trusted position with customers, often receiving detailed personal and financial information from their customers. This means that financial planners are in a unique position to observe anomalous behaviour and/or detect potentially suspicious sources of funds or wealth. However, industry experts engaged for this risk assessment believed that many financial planners do not adequately utilise this information to assess ML/TF risk and submit SMRs to AUSTRAC. More effective procedures and training in this area would significantly enhance the capability of the sector to detect criminal behaviour.

SOURCE OF FUNDS AND WEALTH

Financial planners are required to consider the risks posed by a customer's source of funds and wealth, and report anomalous client wealth to AUSTRAC. Financial planners generally collect much of this information while preparing a Statement of Advice (SOA). However, there may be other factors relating to the customer which require further consideration or may present a challenge for the planner – for example, if the customer is from a foreign jurisdiction, requests time critical transactions, or is not willing to divulge information about the source of their funds or wealth.

During consultations with AUSTRAC, reporting entities outlined a number of controls they had in place to mitigate the risks associated with a customer's source of funds. These included:

- having systems to detect if new funds appeared unusual
- using call-back procedures to verify source of funds
- questioning customers on source of funds for all international transfers
- issuing new SOAs – or addendums to SOAs – whenever an existing customer adds new funds to an account.

One financial institution also reported having a policy of requiring all aligned financial planners to ask customers how they arrived at their wealth. These planners were also provided with a page of hints and talking points to support this type of engagement with the customer.

PRODUCTS AND SERVICES

When assessing the vulnerability of products and services, AUSTRAC looks at the volume of transactions carried out, how easily a customer is able to make transactions or transfer ownership of the product/service, and whether the product/service allows the customer to remain anonymous.

Financial planners should also be aware that the advice services they provide can themselves be targeted by criminals. The skills, knowledge and detailed understanding that planners have of financial services make them vulnerable to exploitation and manipulation, including by serious and organised crime groups.

With industry revenue of \$4.6 billion in 2015–16¹⁴, financial planners facilitate large volumes of transactions and significant amounts of money move through the sector. The range and complexity of the products and investment strategies managed by financial planners also creates vulnerabilities.

When considering anonymity, personal financial advice services are generally less vulnerable than general financial advice services, as personal advice (particularly comprehensive advice) must take into account the personal situation of the customer, and therefore the customer is known to the planner. However, personal advice that is limited in scope (for example, for just one type of product) may be more easily exploited for criminal purposes, as only certain information may be revealed to the planner.

¹⁴ IBISWorld *IBISWorld Industry Report K6419b: Financial Planning and Investment Advice in Australia*, 2016.

Reporting entities consulted for this assessment emphasised that there was heightened vulnerability when customers issued time critical instructions because the SOA is often provided after the service. One financial institution said they sought to mitigate this vulnerability by only offering time-critical services to established customers.

Of the SMRs submitted in the sample period, 57 per cent were in relation to investment and account services – for example, when financial planners act on customer instructions to move money into or out of accounts, or open accounts.

Stockbroking-related services provided by financial planners were represented in 15 per cent of the SMRs. Some reporting entities highlighted this as a more vulnerable service because it often requires financial planners to execute customer instructions quickly.

A similar number of SMRs related to superannuation services provided by financial planners.¹⁵ Many of these SMRs were in relation to SMSFs, which reporting entities emphasised were particularly vulnerable to abuse, especially for tax evasion. Feedback from industry highlighted some examples of potential high-risk matters relating to SMSFs:

- a customer asks to establish an SMSF in order to transfer ownership of recently purchased collectibles and/or real estate to the SMSF without being able to show proof of ownership or source of funds
- a customer asks whether a trustee can bypass in-specie (asset) transfer rules
- the members or trustees of an SMSF change several times over a short period of time.

AUSTRAC also received feedback from industry that life insurance products present particular risks in the financial planning sector. Potential indicators of criminal activity include:

- a customer asks whether an exclusion period can be reduced or whether a benefit can be paid to someone other than the stated beneficiary or policy owner

- a customer asks how long they need to pay premiums before a claim can be made
- a financial planner submits life insurance applications without sufficient identification details and is unable to produce the customer's data collection forms, or advises the insurer that the policy holder is unable to be contacted for underwriting.

Use of accounts

Customer accounts

Reporting entities have observed that some customers have multiple accounts (including personal accounts, joint accounts and trust accounts) that are linked to the products arranged by financial planners. Some institutions mitigated this risk by encouraging customers to have a single account from which to move funds in and out for various products. Some products also had payout rules which only allowed payments to be made to the customer's primary bank account.

Third party accounts

Reporting entities also highlighted that the use of third-party accounts and making payments to third parties could be a vulnerability, due to potential exploitation by criminals. Some financial planning businesses had policies against making payments to third-party accounts; others that allowed this practice had processes in place to mitigate the risk, such as extra verification procedures.

Financial planner accounts

The use of either trust accounts or personal accounts by financial planners to manage customer funds is also a significant vulnerability. A financial planner receiving client fees through a personal account could be an indication of tax avoidance or avoiding the payment of fees to parent financial institutions. As such, many financial institutions reported that they now had policies against aligned financial planners using personal accounts to receive client fees.

¹⁵ For more information, see page 12 of AUSTRAC's Australian Superannuation Sector: Money Laundering and Terrorism Financing Risk Assessment, <http://www.austrac.gov.au/australias-superannuation-sector>.

DELIVERY CHANNEL

‘Delivery channel’ refers to the methods by which financial planners interact with and deliver services to their customers.

The move towards more online service delivery in the financial planning sector has led to increased vulnerabilities. Innovations in online services have increased the speed and ease with which transactions can be executed, with several reporting entities acknowledging the challenge this poses to conducting customer due diligence and comprehensive onboarding procedures.

The widespread use of email communication between financial planners and customers also creates significant vulnerabilities. For this reason, many financial planners continue to rely on phone communication with their customers in order to verify emailed instructions. Financial planners highlighted that a key indicator of potential suspicious activity was a change to the customer’s contact and bank account details, particularly when these changes are made online.

Face-to-face engagement is considered the least vulnerable channel, as it provides greater opportunity for financial planners to develop a relationship with their customers and understand their circumstances. One financial institution reported that – counter to industry trends – they were investing significantly more in face-to-face interaction, not only for business purposes (as their customers preferred personal engagement), but also as a risk management strategy.

On the other hand, some reporting entities also cautioned that regular and ongoing face-to-face engagement between a financial planner and customer had the potential to develop over-familiarity and complacency by the financial planner, making them less likely to look for or recognise suspicious behaviour.

Robo-advice

Robo-advice refers to the provision of automated financial product advice using technology without the direct involvement of a human adviser.

The provision of robo-advice has grown rapidly in Australia, with a number of AFSL holders developing robo-advice models. Current robo-advice capabilities are relatively basic; however, technological advances are expected to give robo-advisers the capability to propose sophisticated investment solutions based on a customer’s financial circumstances and their investment goals.

Firms should consider their potential ML/TF risks and mitigation strategies related to robo-advice services, particularly if they are likely to attract new customers of a different risk profile to a firm’s current customer base.

FOREIGN JURISDICTION

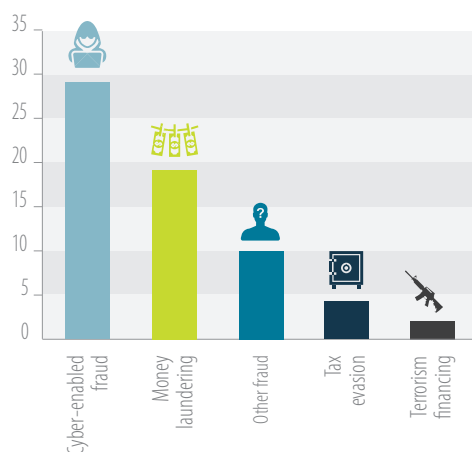
63 SMRs (23 per cent) submitted during the sample period identified the involvement of a foreign jurisdiction, where either the transaction involved a foreign bank account, or where one of the parties involved in the suspicious matter was in a foreign jurisdiction. These SMRs related to a wide spectrum of countries; around half of the SMRs referred to either China, the United States, United Kingdom or Malaysia.

Around half of the SMRs involving foreign jurisdictions were cases of suspected cyber-enabled fraud, in which attempts were made to send funds overseas, facilitated by a financial planner. The most frequently referenced countries for cyber-enabled fraud were the United Kingdom and the United States.

About one-third of the SMRs involving foreign jurisdictions related to suspected money laundering.

Some reporting entities noted during consultations that they only had Australian-based customers, and therefore rarely dealt with foreign jurisdictions. In such circumstances the ML/TF risks faced by the business may be lower.

FOREIGN JURISDICTION SMRs BY OFFENCE TYPE



Customers on significant investment visas

During consultations with AUSTRAC, reporting entities highlighted the difficulties in identifying the source of funds and wealth for customers on significant investment visas (SIVs), as this wealth is often acquired in foreign jurisdictions. Customers on SIVs are high net-worth individuals and some may be foreign PEPs or linked to jurisdictions known to be a high risk for ML/TF activity. Moreover, Australian financial planners often deal with intermediaries or accountants from foreign banks (with a presence in Australia), who represent the overseas-based end client, creating an additional layer of complexity during the customer due diligence (CDD) process.

Some potential indicators of suspicious behaviour by SIV customers include:

- executing investments to satisfy visa requirements, then transferring funds into non-complying investments
- aggregating funds from various sources into a SIV applicant's account
- funds coming through a third country or a high-risk jurisdiction.

Financial institutions consulted for this assessment have implemented a variety of controls for SIV customers, including more rigorous questions to ascertain source of funds, additional checks during the customer identification process, and comprehensive source of wealth checks. Some have also engaged offshore providers to assist with customer due diligence and other checks.

Despite the risks associated with customers on SIVs, there were very few SMRs submitted by financial planners over the last two years about SIV customers. AUSTRAC reminds financial planners that their reporting obligations also apply to SIV customers.

USE OF CASH

Cash transactions are generally a significant indicator of money laundering risk. There was a common view among reporting entities that the use of cash was not a significant vulnerability in the financial planning sector, as cash was rarely accepted by financial planners. Most reported that if a customer approached a financial planner wanting to use cash to purchase a product, that customer would either be denied service or referred to a bank to deposit the cash.

AUSTRAC's analysis of the SMRs in the sample period revealed that 32 SMRs (12 per cent) related to the use of cash. There were 11 SMRs in which the customer was the suspicious party. These included cases where the customer:

- had unexplained wealth
- sought to deposit a large amount of cash from a foreign jurisdiction into an Australian superannuation account, via a financial planner
- revealed to a financial planner that they were receiving undeclared cash income
- requested financial planner to invest \$50,000 in cash, despite being on a Newstart allowance.

16 SMRs were from banks reporting on financial planners who were suspected of money laundering by making large structured cash deposits or withdrawals. A small number of SMRs involved financial planners suspected of being complicit in welfare fraud or tax evasion by their customer.

OPERATIONAL VULNERABILITIES

The nature and structure of financial planning businesses in Australia varies considerably, so the level of operational vulnerability will be specific to each situation.

During consultations with AUSTRAC, reporting entities explained that financial planning businesses often operated with paraplanners and administrative staff collecting customer information (such as identity documents and financial records). Sometimes these staff were the primary point of contact for customers. This could minimise the visibility that financial planners have over a customer's circumstances and behaviour, particularly if support staff lack the training or expertise to identify potentially suspicious or unusual customer wealth or source of funds. Although financial planners who are only required to have a special AML/CTF program are not required to conduct AML/CTF risk awareness training of staff, these entities could consider educating their staff to protect their business.

Another operational vulnerability for some financial planning businesses may arise due to arrangements between the AFSL holder and the authorised representatives operating under that AFSL. Reporting entities consulted for this risk assessment highlighted that there can sometimes be very low levels of awareness of AML/CTF responsibilities among authorised representatives. AFSL holders should ensure that authorised representatives clearly understand their obligations and ensure there are controls in place to manage this vulnerability.

Some businesses offer a wide range of professional services to customers in addition to financial planning, such as accounting, real estate and legal services. Many entities engaged for this risk assessment saw these 'one-stop shops' as a higher risk for financial crime, as the services they offer may be exploited to support criminal activities. Moreover, law enforcement agencies have observed serious and organised crime groups establishing and being involved in one-stop shops, particularly in relation to self-managed superannuation funds.

AML/CTF SYSTEMS AND CONTROLS

AUSTRAC assesses that, at a sector level, there is only partial understanding of the AML/CTF obligations among financial planners; however, there is likely to be significant variation between businesses. Although many financial planners have reduced regulatory obligations because they operate under the special AML/CTF program provisions of the AML/CTF Act, feedback received from industry is that many financial planners are not adequately satisfying even these reduced requirements.

Specifically, there appears to be a perception among many financial planners that collecting and verifying a customer's identification is all that is required to fulfil their AML/CTF obligations. This means that many financial planners are not fulfilling their obligations to have risk-based customer due diligence procedures and to submit SMRs to AUSTRAC. Almost all entities engaged for this assessment saw this as a significant vulnerability that requires attention from the sector.

Reporting entities and industry experts offered insights into potential reasons for this. These included the challenges of needing to arrange many products across different product issuers; the need to abide by other regulations, including the Corporations Act and Future of Financial Advice reforms; and the time pressure that financial planners face to meet their customers' needs. Compliance staff in one financial institution had observed that top performing financial planners, in terms of sales, were often the least compliant; excessive growth in business for a financial planner was a red flag to the Compliance team.

There was also a perception among some in the industry that smaller financial planning businesses and independent financial planners tended to have weaker regulatory controls, due to not having the 'depth of defence' and additional oversight offered by the AML/CTF programs and processes of a larger institution. One large institution reported that they conducted internal audits to ensure that aligned financial planners abided by AML/CTF obligations and submitted SMRs when appropriate.

However, AUSTRAC was informed of incidents of high-risk behaviour by some individual financial planners employed in otherwise vigilant financial institutions. Moreover, the challenge for some larger institutions was ensuring AML/CTF compliance by a vast network of financial planners, especially where planners were geographically dispersed across the country. Some large institutions noted that this was a significant issue.

The grateful customer

Reporting entities told AUSTRAC that customers were often grateful for stringent controls and often responded positively when financial planners called them to check on potential suspicious transactions (while observing the tipping off provisions). Although the process could delay a transaction, customers saw this as the financial planner seeking to protect their money. The relationship between a financial planner and a customer can therefore be a significant asset to managing risk.

CONSEQUENCES



The consequences of ML/TF activity in the sector are assessed as **minor**. Consequence refers to the potential impact or harm that ML/TF and other financial crimes may cause. Financial crime in the financial planning sector has consequences for customers, individual financial planners, financial institutions, and the broader Australian economy.

CUSTOMERS

There are financial and indirect consequences for customers in this sector. These could include:

- financial losses from accounts
- emotional distress
- loss of private information and identity theft.

FINANCIAL PLANNING SECTOR

The severity of the consequences caused by ML/TF will differ for financial planners and institutions depending on the extent to which they understand and assess ML/TF risks, identify and submit SMRs, and have effective controls and strategies in place to combat the various criminal threats outlined in this assessment.

Consequences for financial planners could include:

- crime-related financial losses and subsequent erosion of financial performance (particularly for independent or unaligned financial planners who may have limited capacity to spread risk and/or absorb losses)
- increased costs associated with combating criminal attacks, in particular IT security costs to build cyber resilience

- increased fraud insurance premiums
- increased administrative costs in reviewing accounts upon the discovery of a fraudulent/criminal activity
- reputational damage to a financial planner or institution following an incident, resulting in loss of customers and/or damage to the brand
- for planners who do not report suspicious matters, the possibility of implication in facilitating criminal activities
- for planners who commit offences, potential personal liability either from civil action by aggrieved victims or criminal prosecution by law enforcement authorities.

Consequences for the financial planning sector as a whole include:

- loss of confidence in the financial planning sector by both customers and by product issuers/other financial institutions that accept customer referrals from financial planners
- public relations costs associated with regaining community trust
- increased regulatory action
- increased risk of legal action and compensation for customer losses arising from failed AML/CTF controls.

AUSTRALIAN ECONOMY

Financial crimes in the financial planning sector have the potential to impact the broader Australian economy, including:

- undetected criminal activity, thereby providing a safe haven for the proceeds of crime, particularly for funds originating offshore
- loss of savings or investments from stolen funds
- weakened AML/CTF compliance for product issuers that rely on customer due diligence carried out by financial planners
- reduced government revenue from welfare fraud and tax evasion
- damage to Australia's international economic reputation in relation to the security and safety of investing in Australian financial products and other assets.

NATIONAL SECURITY AND INTERNATIONAL CONSEQUENCES

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

CONCLUSION

The criminal threats facing the financial planning sector in Australia will almost certainly persist in future years. Financial planners are well-placed to detect suspicious behaviour by their customers, and play an important role in supporting Australia's AML/CTF operations. Similarly, financial planners can help protect their customers, particularly from cyber-enabled crimes executed by third parties. Greater vigilance and increased reporting of suspicious activity by financial planners will serve to better protect and strengthen the sector.

AUSTRAC's view is that, despite the challenges, the financial planning sector as a whole must ensure that AML/CTF compliance is a greater part of the organisational culture for financial planners.

AUSTRAC believes that significant opportunity exists for financial planners to leverage this assessment to expand their suspicious matter reporting and strengthen internal controls against financial crime. AUSTRAC will continue to support the sector by providing advice and guidance on their AML/CTF obligations and the ML/TF risks present in the sector. In addition, AUSTRAC will monitor SMR trends after the publication of this assessment to determine if reporting levels have increased across the sector, and this information will inform future intelligence-led compliance activities.

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

APPENDIX A

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 sector 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	Medium 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 politically exposed persons (PEPs)			Some politically exposed persons (PEPs)			Many politically exposed persons (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
TF activity has minimal potential to impact on national security and/or international security	TF activity has the potential to moderately impact on national security and/or international security	TF activity has the potential to significantly impact on national security and/or international security



www.austrac.gov.au