Australian Government
AUSTRAC

FIGHTING FINANCIAL CRIME TOGETHER

BULLION DEALERS IN AUSTRALIA

MONEY LAUNDERING AND TERRORISM FINANCING RISK ASSESSMENT

CONTACT US

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

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

CONTENTS

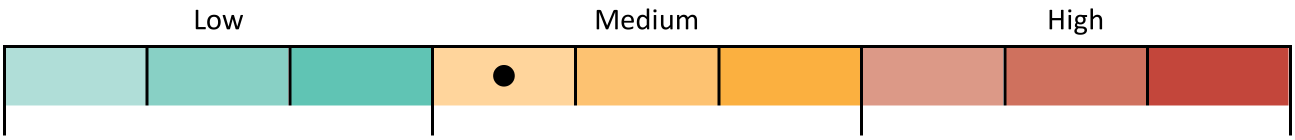
EXECUTIVE SUMMARY

A bullion dealer is an individual, business, or organisation that buys or sells bullion as a bullion-dealing business. AUSTRAC defines bullion as gold, silver, platinum or palladium authenticated to a specified fineness. It comes in the form of bars, ingots, plates, wafers or similar forms, or in coins. It is used for trading. This definition excludes gold granules and gold dust.

For the purposes of this risk assessment, bullion dealers include businesses that are enrolled with AUSTRAC in the precious metal traders sector and in the bullion cohort. One hundred reporting entities were considered in-scope for this risk assessment.

The characteristics and activities of individual bullion dealers vary significantly. This means that the money laundering and terrorism financing (ML/TF) risks associated with individual businesses vary, as does their ability to mitigate these risks. The methodology used in this assessment is designed to capture an overall inherent risk rating for the sector.

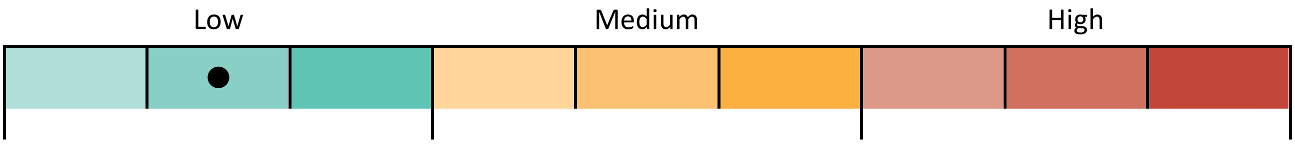
OVERALL RISK RATING



AUSTRAC assesses the overall money laundering and terrorism financing risk associated with the bullion sector as **medium**. This rating is based on assessments of the criminal threat environment, inherent vulnerabilities in the sector and consequences associated with the criminal threat.

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

CRIMINAL THREAT ENVIRONMENT



AUSTRAC assesses the threat of money laundering and terrorism financing facing Australia's bullion sector as **low.**

The criminal threat environment facing the bullion sector includes a low to moderate volume of suspected criminal activity, most of which is unsophisticated. Data-matching with criminal lists suggests the sector is not significantly exposed to national or transnational, serious and organised criminal entities, or entities linked to terrorism or terrorism financing activities. The primary threats facing the sector are tax evasion, money laundering, fraud and scams.

Money laundering

AUSTRAC assesses the nature and extent of money laundering threats facing bullion sector as **medium.**

Money laundering was identified in 29 per cent of the suspicious matter report (SMR) review, 64 per cent of the third-party SMR sample and 70 per cent of the intelligence report (IR) review.[1] Information from partner agencies indicates the bullion sector was not significantly exposed to exploitation by members of transnational, serious organised criminal groups or individuals charged with a money laundering-related offence.

Terrorism financing

AUSTRAC assesses the nature and extent of terrorism financing threats facing the sector as **low**.

This assessment is based on the low number of terrorism financing-related SMRs submitted by the sector and third parties, limited terrorism-related findings from the IR review, feedback from partner agencies as well as open source information. In addition, data-matching to criminal lists suggests bullion dealers are not significantly exposed to known or suspected terrorists or their financiers.

[1] The SMR review comprises SMRs submitted by the bullion sector between 1 July 2018 and 30 June 2021.

The third-party SMR sample includes SMRs about the bullion sector submitted by third parties (non-bullion sector reporting entities) between 1 July 2018 and 30 June 2021.

The IR review includes a review of 31 AUSTRAC and partner agency intelligence reports produced between 1 September 2016 and 28 September 2021

Predicate offences

AUSTRAC assesses the nature and extent of threats posed by predicate offending involving the bullion sector as **low**.[2]

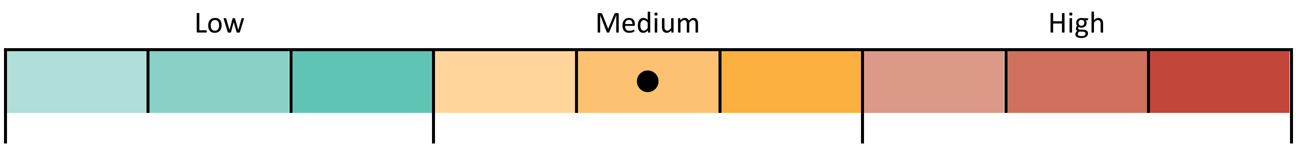
The bullion sector's exposure to predicate offences ranges from a low level of sophistication to more complex schemes. The key predicate offences impacting the sector are tax evasion, fraud, scams, theft and drug trafficking.[3] The overall number of suspected offences and their associated values is moderate.

Personal income tax evasion was the most common suspected offence linked to 52 per cent of the SMR review. Associated values were low – generally below the $10,000 reporting threshold. Structuring transactions to avoid reporting and the use of cash were the most common behaviours associated with instances of personal tax evasion. Corporate tax evasion was much less commonly identified, accounting for just two per cent of the SMR review. Corporate tax evasion was linked to bullion dealers making large cash deposits that were inconsistent with the company profile and bullion-related businesses paying business invoices and expenses using cash.

The most common types of fraud identified included the use of fake or stolen identification documents and credit card fraud. The most common type of scam identified was business email compromise. Theft also impacts bullion dealers, with SMRs reflecting concerns that bullion and jewellery sold to bullion dealers may have been stolen.

In a small number of cases in the SMR review and the third-party SMR sample, suspected drug trafficking was linked to bullion purchases. Approximately one quarter of IRs in the IR review were linked to drug trafficking, including using the proceeds of drug trafficking to purchase bullion.

VULNERABILITIES



AUSTRAC assesses the bullion sector is subject to a **medium** level of inherent ML/TF vulnerability.

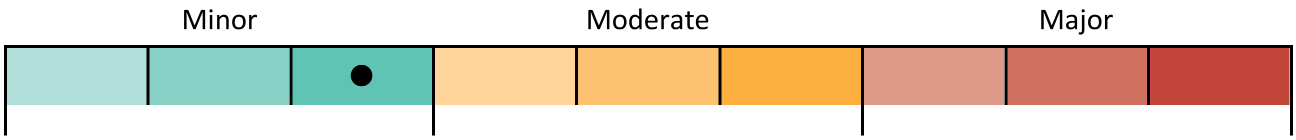
Factors that most expose the sector to ML/TF include:

- a moderately-sized customer base
- the ability to store and move funds
- a high exposure to cash transactions with many bullion dealers operating cash-intensive business models
- a number of bullion dealers are also bullion refiners increasing the foreign jurisdiction risk and risks associated with refining scrap precious metal, such as the difficulty in tracing the origins of scrap gold and silver, and
- the delivery channels through which bullion dealers offer their products and services including face-to-face, online, by phone, and through third-party arrangements.

[2] For the purposes of this report, a predicate offence is a criminal offence that generates proceeds of crime, or other related crimes such as identity fraud.

[3] For the purposes of this report 'tax evasion' is defined as the non-payment or under-payment of taxes, including duties on goods or services. This definition includes the use of cash payments to avoid or under-declare tax on personal or business earnings. The term 'tax evasion' does not include the legitimate use of offshore service providers or tax secrecy jurisdictions to minimise tax obligations.

CONSEQUENCES



AUSTRAC assesses the overall consequences of ML/TF activity in the sector as **minor**.

Consequences for customers can include:

- emotional distress and potential criminal implications for people knowingly and unknowingly used as money mules and victims of financial abuse
- damage to the brand and reputation of corporate customers, e.g. after using a bullion dealer connected to criminal activity.

Consequences for reporting entities and the sector can include:

- direct loss of revenue from criminal exploitation, such as credit card fraud
- difficulty establishing or maintaining a relationship with financial institutions
- reduced revenue from loss of customers deterred by heightened controls and scrutiny
- increased costs to improve AML/CTF compliance management and higher insurance premiums
- increased costs as a result of supply chain disruption from criminal activities, such as law enforcement interventions
- damage to the sector’s reputation, leading to more criminals seeking to exploit weaknesses in the sector.

Consequences for the Australian financial system and community can include:

- reduced government revenue due to tax evasion, affecting the delivery of critical government services
- damage to Australia’s international economic reputation and prosperity by undermining the security, integrity and safety of Australia’s financial sector.

Consequences for national and international security can include:

- enabling transnational, serious and organised crime groups to grow larger and stronger and their activities can impact both national and international security interests
- increased likelihood of a national security event where the bullion sector is used to enable and sustain the activities of Australian foreign terrorist fighters, or terrorist acts in Australia or overseas.

RISK MITIGATION STRATEGIES

The sophistication and implementation of risk mitigation strategies varies significantly between bullion dealers, presenting ongoing and potentially significant risks to the sector. A number of bullion dealers consulted for this report outlined less sophisticated approaches to AML/CTF with scope for improvements to be made to ensure bullion dealers:

- tailor enterprise risk assessments to the business, and ensure these are well documented and updated regularly
- seek an independent review of their Part A AML/CTF program

- provide employees with adequate and regular training in AML/CTF
- better understand and consistently apply politically exposed person and sanctions screening
- have systems in place to detect and report suspicious matters to AUSTRAC, and ensure reporting contains appropriate information and detail.

A small number of larger bullion sector entities outlined relatively comprehensive risk mitigation strategies in place, including internal audits, introductory and ongoing training of staff and the use of dedicated AML/CTF staff to inform their policies and practices.

PURPOSE

This assessment details the money laundering and terrorism financing risks the bullion sector faces at the national level. Its primary aim is to help businesses identify and disrupt criminal activity in the sector, and report suspected crimes to AUSTRAC.

This risk assessment is not intended to provide targeted guidance or recommendations about how reporting entities should comply with their AML/CTF obligations. However, AUSTRAC expects Australia's bullion dealers to review this assessment to:

- inform their own ML/TF risk assessments
- enhance their understanding of risk in the sector
- review and strengthen their risk mitigation systems and controls.

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

BACKGROUND

For the purposes of this risk assessment, bullion includes gold, silver, platinum or palladium authenticated to a specified fineness. Gold is overwhelmingly the dominant precious metal in the bullion sector followed by silver, platinum and palladium. In SMRs where the type of precious metal was specified, the bullion product was gold in 95 per cent of cases, silver in 16 per cent, platinum in one per cent, and palladium in 0.2 per cent.[4]

All four of these precious metals can be used as a store of wealth in addition to having industrial applications. Bullion comes in the form of bars, ingots, plates, wafers or similar forms, or in coins and is widely accepted as a means of exchange.[5]

AUSTRAC does not regulate the purchase or sale of precious metals that are not defined as bullion. For example, granules of fine gold typically used for the manufacture of jewellery are not considered to be bullion because they are not bars, ingots, plates, wafers, coins or similar forms.

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

- suspicious matter reports (SMRs)
- threshold transaction reports (TTRs)
- international funds transfer instructions (IFTIs)
- annual compliance reports. [6]

In 2021 Australia was the world's largest gold producer and produced approximately 321 metric tonnes of gold. Production volumes are forecast to reach 379 metric tonnes by 2023. [7] Australia is also a key player in the global gold and silver refining industry. In 2020, approximately 1,300 metric tonnes of silver were mined across Australia. Almost all of Australia's silver is produced as a by-product of underground lead-zinc or copper mines.[8] Australia produces a relatively small amount of platinum and palladium with South Africa and Russia dominating global production.[9]

[4] Percentages add to more than 100 because some SMRs may include more than one type of precious metal.

[5] AUSTRAC, *Glossary B*, AUSTRAC website, n.d., accessed 25 August 2021.

[6] A reporting entity must provide the AUSTRAC CEO a report relating to the reporting entity's compliance with the AML/CTF Act 2006, the regulations and the AML/CTF Rules during the assessment period.

[7] R Pupazzoni, *Australia in the gold medal position for producing the precious metal, knocking China from top spot*, ABC News website, 2021, accessed 10 September 2021.

Statista, *Production volume of gold across Australia in financial year 2021, with a forecast until 2023*, Statista website, 2021, accessed 6 October 2021.

[8] Statista, *Production volume of silver mined in Australia from 2006 to 2020*, Statista website, 2021, accessed 29 October 2021.

[9] M O'Callaghan, *Panning for platinum – the prospects are good*, CSIRO ECOS website, 2016, accessed 29 October 2021.

METHODOLOGY

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

- **Criminal threat environment** refers to the nature and extent of ML/TF and relevant predicate offences in a sector.
- **Vulnerability** refers to the characteristics of bullion dealers that make them attractive for ML/TF purposes. This includes features that can be exploited, such as customer types, products and services, delivery channels and the foreign jurisdictions with which the sector transacts. This report assesses inherent ML/TF vulnerability only.
- **Consequence** refers to the impact or harm that ML/TF activity through the sector may cause.

This assessment considered 18 risk factors across the three categories. An average risk rating was determined for criminal threat environment, vulnerability and consequence, and the average of these three categories determined the overall inherent risk rating for the sector.

This report also discusses the level of **risk mitigation strategies** implemented across the sector. This includes measures that are explicitly mandated under AML/CTF legislation, and other practices reporting entities implement to mitigate ML/TF risk. This discussion was not included in scoring for the overall risk rating.

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

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

- Analysis of 760 SMRs submitted by the bullion sector between 1 July 2018 and 30 June 2021 (the **SMR review**).[10]
- Analysis was also conducted on 832 SMRs about the bullion sector submitted by third parties between 1 July 2018 and 30 June 2021 (the **third-party SMR sample**).
- A comprehensive review of 31 AUSTRAC and partner agency intelligence reports produced between 1 September 2016 and 28 September 2021 (the **IR review**).[11]
- The results of data-matching (**the data-matching exercise**) whereby TTRs and SMRs that the bullion sector submitted to AUSTRAC between 1 July 2020 and 30 June 2021 were matched against known criminal entities who were:
    - recorded as a member or associate of a significant regional, national or transnational serious and organised crime group as at April 2020;
    - charged with a money laundering or proceeds of crime-related offence between 1 January 2017 and 30 June 2021;[12]

[10] SMRs should be considered indicative of suspicious behaviour only and not conclusive in their own right. This is because reporting entities generally lack visibility of certain threat elements, for example how a customer generates suspected criminal proceeds. To ensure accuracy of ML/TF indicators (threats and vulnerabilities) outlined in the SMR review, AUSTRAC officers manually reviewed and categorised each report.

[11] The number of IRs may not reflect the actual extent of criminality, and may understate the true extent of ML/TF threats and criminal misuse of the sector. This is because AUSTRAC does not have visibility of all partner agency intelligence reporting.

[12] Includes persons charged under Division 400 of the Criminal Code (Cth) and/or sections 81 and 82 of the Proceeds of Crimes Act 2002 (Cth).

    - charged or associated with a terrorism-related offence between 1 January 2017 and 30 June 2021.[13]
- Open source information, including public facing information produced by government agencies, academic institutions, reporting entities and the media.
- Feedback and professional insights offered during interviews and consultations with a range of partner agencies and bullion sector representatives.

LABELLING THE SMR SAMPLE

SMRs are indicative of suspicious behaviour only and are not conclusive evidence of criminal activity in their own right. For example, reporting entities often have no visibility of how a customer generates criminal proceeds. As a result, reporting entities are unable to include specific information regarding suspected threat types.

To ensure accurate and consistent insights from SMRs, AUSTRAC analysts reviewed and categorised each report in the SMR sample against 414 possible labels grouped by:

- criminal threat
- suspicious transactional activity
- products and services
- customer type
- entity attribute
- foreign jurisdictions.

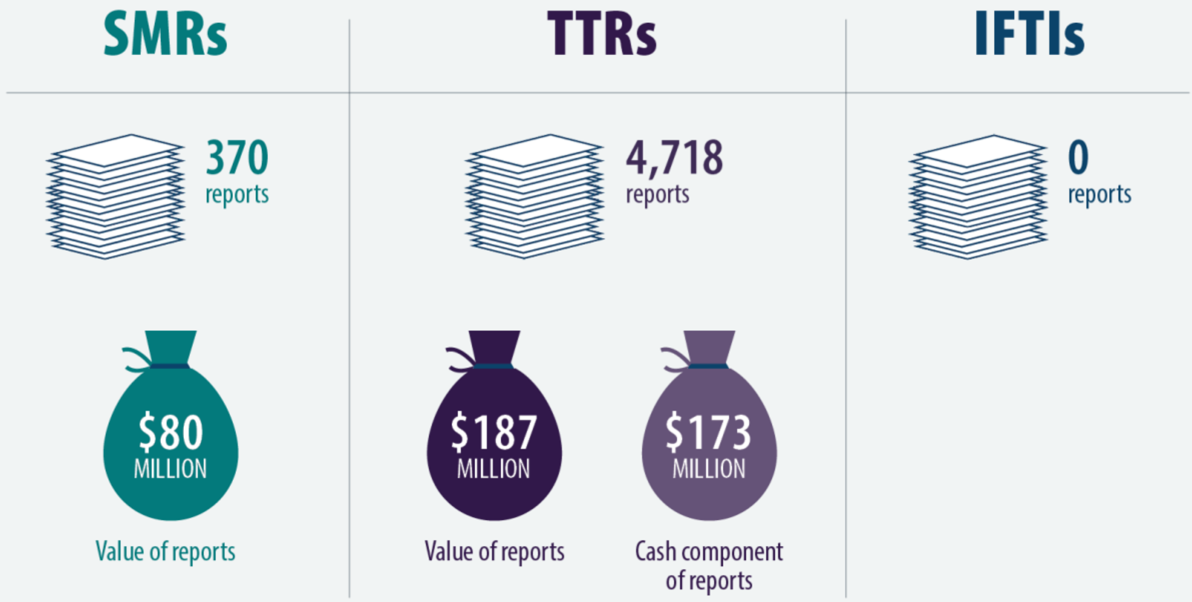
For example, a single SMR could be categorised with multiple labels as follows:

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

[13] Includes persons charged with a ‘Terrorism offence’ in section three of the Crimes Act 1914 (Cth) and/or offences contrary to the Crimes (Foreign Incursion and Recruitment) Act 1978 (Cth).

REPORTING TO AUSTRAC

REPORTS THE BULLION SECTOR SUBMITTED TO AUSTRAC BETWEEN 1 JULY 2020 AND 30 JUNE 2021[14] [15]



FEEDBACK FOR REPORTING ENTITIES REGARDING SMR SUBMISSIONS

The sector submits a relatively low number of SMRs and numbers vary greatly between individual entities of a similar size and scale. Reports submitted by the sector often lack detailed information about the grounds for suspicion. Refer to **Risk mitigation strategies** on page 44 for more details.

SMRs play a crucial role in law enforcement

Under the *AML/CTF Act*, reporting entities have an obligation to report suspicious matters to AUSTRAC. A reporting entity must submit an SMR under a number of circumstances, including if they suspect on reasonable grounds that information they have concerning a service they are providing, or will provide, may be relevant to the investigation or prosecution of a crime.

SMRs provide valuable intelligence to AUSTRAC. Working with its partner agencies, AUSTRAC pieces together intelligence from a range of sources to develop a picture of criminal activities and networks. AUSTRAC's partner agencies – including the Australian Federal Police (AFP), the Australian Criminal Intelligence Commission (ACIC) and the Australian Taxation Office (ATO) – have access to SMRs to generate investigative leads and conduct further analysis and investigation. High-quality, accurate and timely SMRs give AUSTRAC and our partners the best chance to detect, deter and disrupt criminal and terrorist activity.

---

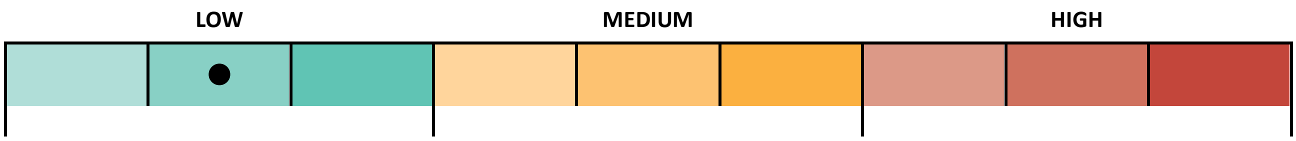
[14] A number of bullion dealers also deal in cryptocurrency. SMRs submitted by bullion dealers that related exclusively to cryptocurrency were removed from the SMR review.

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

What happens after AUSTRAC receives an SMR?

When an SMR is submitted to AUSTRAC, it is processed to detect crime types and surface high priority matters for immediate analysis. Reports and alerts are then assigned to AUSTRAC intelligence analysts to assess and respond in accordance with our national security and law enforcement intelligence priorities. Additionally, through direct online access to AUSTRAC's intelligence system, SMR information is available to over 6,000 users from more than 35 of AUSTRAC's partner agencies to inform their intelligence gathering efforts and investigations.

CRIMINAL THREAT ENVIRONMENT



CRIMINAL THREAT ENVIRONMENT FACTOR	RATING
MONEY LAUNDERING	
TERRORISM FINANCING	
PREDICATE OFFENCES	

AUSTRAC assesses the criminal threat environment facing Australia's bullion sector as **low**.

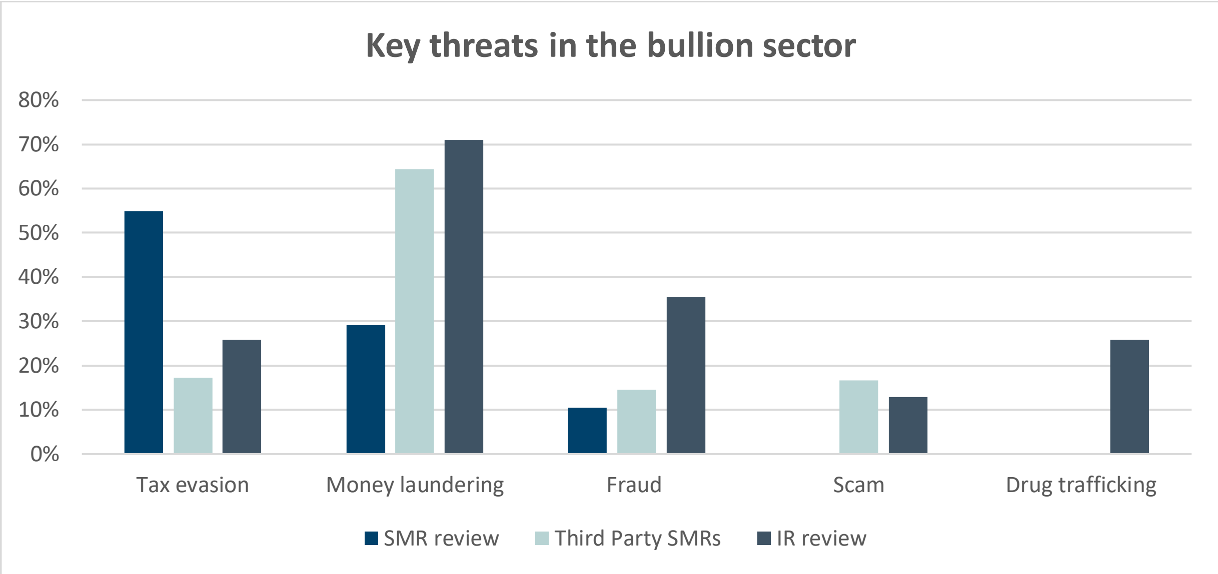
The criminal threat environment refers to the nature and extent of money laundering, terrorism financing, and predicate offences associated with the sector.

The bullion sector is exposed to medium levels of money laundering activity. Information from partner agencies and the IR review indicate the bullion sector was not significantly exposed to exploitation by members of transnational, serious organised criminal groups or individuals charged with a money laundering-related offence.

There are low levels of terrorism financing in the bullion sector. Bullion dealers and third parties submitted very few terrorism financing-related SMRs. The IR review and feedback from partner agencies identified very few instances of terrorism financing linked to bullion trading. In addition, data-matching with criminal lists suggests bullion dealers are not significantly exposed to known or suspected terrorists or their financiers.

There are low levels of exposure to a variety of predicate offences in the bullion sector. These offences range from a low level of sophistication to more complex schemes. The key predicate offences impacting the sector in the SMR review are tax evasion, fraud, scams and theft.

The bullion sector submits a low number of SMRs. During the reporting period, 77 per cent of bullion dealers did not submit an SMR. As a result, SMR statistics are unlikely to reflect the full extent of the criminal threat facing the sector.



Percentages may add to more than 100 because some SMRs and IRs may include more than one threat type.

MONEY LAUNDERING

AUSTRAC assesses the nature and extent of money laundering threats facing the bullion sector as **medium.**

Money laundering was the most common threat in the third-party SMR sample and IR review (64 per cent and 71 per cent, respectively)[16], and the second most prevalent threat in the SMR review – identified in 29 per cent of reports analysed.

The third-party SMR sample included concerns about both customers and bullion dealers themselves. The money laundering methodologies identified in the SMR analysis were generally unsophisticated. In addition, the data-matching exercise indicated the sector had limited exposure to members of transnational, serious organised criminal groups or individuals charged with a money laundering-related offence (see page 30 for a detailed overview of data-matching results).

Trading bullion to conceal the source of funds is an established money laundering methodology.[17] Criminals may buy and sell bullion to launder money as it has a high intrinsic and stable value, can be converted and melted down into various forms and enables anonymity when transferring value. This makes it easy to conceal and move across domestic or international borders, and convert back to legitimate funds.

[16] In the SMR sample, a report was labelled as 'money laundering' when AUSTRAC analysts deemed the nature or extent of suspicious indicators suggested money laundering was likely. Such indicators can include unexplained wealth, an attempt to obscure the source of funds or purpose of transaction, where the source of funds was possibly linked to proceeds of crime, or when money laundering methodologies were identified (e.g. cuckoo smurfing or rapid movement of funds).

[17] M Treanor, *Gold and Money Laundering*, Ballard Spahr website, 2019, accessed 22 September 2021.

The bullion sector can be exploited at all stages of the money laundering process. The purchase and sale of bullion provides opportunities for placement, layering and integration of criminal funds. Placement occurs when cash derived from criminal proceeds is used to purchase bullion. Transactions are structured to try and evade detection.[18] The purchase of bullion potentially adds legitimacy to illicitly-sourced funds. Layering can occur when mules or third parties are used to purchase bullion, making it difficult to identify the true source of funds. In the integration stage, the funds are reintroduced into the economy to appear to belong to legitimate sources, often by selling bullion that was purchased during the layering stage.

Money laundering was identified as the second most prevalent threat facing the sector in the SMR review. This included cases where gold bullion was purchased in multi-kilogram amounts over an unusually short period of time and where the customer may have been purchasing bullion on behalf of a third party who did not want to conduct the transaction under their name.

One per cent of the SMR review and one per cent of the third-party SMR sample included the suspicion that the customer was part of a criminal group, including a customer who was identified as being on an international wanted list when their identification was verified (see **Higher-risk customers** on page 29). Partner agency consultations indicate limited serious organised crime exploitation of bullion dealers. The serious and organised crime entities that use bullion to launder money are likely to do so in conjunction with other methodologies.

Criminals are attracted to bullion because it can be easily purchased with cash and is subsequently almost impossible to trace. Cash transactions featured prominently in SMRs linked to suspected money laundering. Approximately half of the SMRs in the SMR review involved cash payments, while 40 per cent of money laundering-related SMRs involved cash. Likewise, 48 per cent of money laundering-related SMRs that third parties submitted included instances of face-to-face cash deposits at a bank branch and 20 per cent included cash deposits at ATMs into the bullion dealer's bank account.

SMR analysis and consultations with industry indicate that both the methodologies and actors involved in cash-based money laundering are generally unsophisticated. While sophisticated methodologies and actors are harder to detect and therefore may be underreported in SMRs, partner agencies consulted suggested sophisticated money laundering activity in the sector is limited.

STRUCTURED CASH TRANSACTIONS TO PURCHASE BULLION

In 2021, a bullion dealer submitted an SMR about a customer who opened a personal account for the purchase of bullion. The individual made it clear they were interested in making cash-only purchases and structured their purchases below $10,000 to avoid any reporting obligations. The customer indicated they had previously dealt with another bullion dealer but believed they had been reported in an SMR and, as a result, changed bullion dealers.

In another SMR, a customer conducted a number of in-person transactions in a short space of time and changed their physical appearance between transactions, in an attempt not to be recognised as the same person and avoid the reporting obligations.

Structuring was identified in 18 per cent of the SMR review and 25 per cent of the third-party SMR sample where money laundering was suspected. Structuring activity the sector identified reflects unsophisticated attempts to avoid reporting obligations. In some cases, customers would openly discuss their intention to structure their transaction and ask the bullion dealer for advice on how to avoid reporting obligations. Instances were also reported where customers admitted to undertaking

[18] Structuring is defined in the Glossary at Appendix A.

several bullion purchase transactions under the reporting threshold, at a number of different bullion dealers.

CUSTOMER IDENTIFICATION PROCEDURES FOR PURCHASES AND SALES OF BULLION VALUED LESS THAN $5,000

Bullion dealers are not required to carry out the applicable customer identification procedures for purchases or sales of bullion when the retail value of the transaction is less than $5,000 AUD or the foreign currency equivalent.

This exemption does not apply where a bullion dealer determines in accordance with its appropriate risk based systems and controls that for ongoing customer due diligence purposes, it should obtain, update or verify any 'know your customer' information about a customer.

The SMR review identified examples of customers undertaking transactions to stay under the $5,000 threshold, and informing the bullion dealer they do not want the transaction to be traceable.

WHAT THE CUSTOMERS ARE SAYING

A number of SMRs included customers discussing their reasons for using cash and structuring their bullion purchase transactions. In such cases, customers may not understand a reporting entity's obligations to report suspicious matters. Several reports contained instances of customers:

- asking the bullion dealer if the transaction is being reported
- splitting the bullion purchase with a partner so the transaction would not be visible to Australian government agencies
- visiting a bullion dealer and asking several questions about AUSTRAC, stating clearly they did not want anything reported
- advising that cash had come from business activities and that they needed to spend the cash on a bullion purchase rather than have it deposited in the bank
- stating they wanted to avoid raising red flags, they didn't want the transaction tracked or they didn't want the government knowing what they were doing.

Third parties and 'money mules'

The SMR review and third-party SMR sample indicated that bullion dealers suspect criminals are recruiting third parties or 'money mules' to buy or sell bullion in order to launder money. The third party often has no direct connection to the criminals and may include 'cleanskins' such as foreign students.[19] The criminal provides the third party with funds, in some cases cash, to buy the gold bullion. The third party may use their own identification details to buy the gold bullion and then hands over the bullion to the criminal. In other cases, the third party may sell the gold bullion on the criminal's behalf and transfer the proceeds to the criminal. The third party is paid a commission for their services. This enables the criminal to distance themselves from the transaction and reduce their chance of detection.

[19] A 'cleanskin' is a person without a criminal history or identifiable links to criminals, who acts on behalf of a criminal entity in order to provide a veneer of legitimacy to such activities.

In one case, it was suspected that an individual deposited in excess of $200,000 in cash into the bank account of a bullion dealer over two days. Law enforcement found that the individual suspected of making the deposits was incarcerated at the time of the transactions, suggesting an unidentified third party had made the cash deposits using the account holder's details.

The following themes were identified in the SMR review and the third-party SMR sample, when third parties or money mules were suspected:

- cash transactions
- unknown source of funds
- customers that are either unusually young or old
- customers that provide their occupation as students
- customers who are not concerned with the bullion price or transaction fees
- unknown third parties conducting transactions through the customer's account.

Trade-based money laundering

Trade-based money laundering is the process of disguising the proceeds of crime by moving the proceeds through trade transactions in an attempt to legitimise the funds or finance criminal activity.[20] In December 2020, FATF and the Egmont Group published a report *Trade-based Money Laundering: Trends and Developments* which identifies new and emerging risks in trade-based money laundering, including through gold and other precious metals. The report also identified the use of gold within the money laundering process as an alternate form of value 'i.e. not just a commodity to exploit in moving value, but also a proxy for cash'.[21]

Trade-based money laundering was identified in three SMRs about the bullion sector submitted by third parties. These included concerns about gold misclassification, over- and under- valuing commodities, and misrepresentations about the price, quantity or quality of the gold.

The sector did not submit any SMRs relating to trade-based money laundering. This activity is likely to be under-represented due to the difficulty of detection.

POSSIBLE TRADE-BASED MONEY LAUNDERING LINKED TO THE BULLION SECTOR

An SMR was submitted when a company involved in mineral exploration received multiple large cash deposits in a short period of time and the source and legitimacy of the cash deposits could not be established. The beneficial owner of this exploration company is also the beneficial owner of multiple entities including a bullion dealer.

The entity that submitted the SMR was concerned that trade-based money laundering may be occurring through the misrepresentation of the price, quantity or quality of the gold involved in trade transactions. The transactions were a sudden and significant change in the customer's transaction activity and not consistent with their profile. The customer provided weak or no justification for the movement of funds.

[20] FATF, '*Trade Based Money Laundering*', FATF website, 2006.

[21] FATF/Egmont Group, '*Trade-based Money Laundering: Trends and Developments*', FATF website, 2020, p.21.

TERRORISM FINANCING

AUSTRAC assesses the nature and extent of terrorism financing threats facing the bullion sector as **low**.

This assessment level is based on the low number of terrorism financing-related SMRs the sector submitted, the low number of terrorism financing-related SMRs in the third-party SMR sample, findings from the IR review, feedback from partner agencies and open source information.

AUSTRALIA'S TERRORISM FINANCING ENVIRONMENT

Since the territorial collapse of Islamic State of Iraq and the Levant's (ISIL) caliphate in Syria and Iraq, there has been a sharp decline in the number of foreign terrorist fighters departing Australia. However, the security environment continues to evolve and the emergence of the COVID-19 pandemic, while inhibiting some aspects of the terrorism threat through the restricted cross-border movement of people, has also presented a platform for recruitment and the promotion of extremist narratives online. Amid this evolving environment, supporters and sympathisers in Australia are likely to continue to send funds internationally in support of terrorist activity.

The primary threat to Australia stems from lone actors or small groups. These actors and groups primarily conduct small-scale, low-cost terrorist attacks. The national terrorism threat level at the time of publication is assessed by the National Threat Assessment Centre as **probable**.

It is unlikely significant amounts of terrorist-related funds are flowing into, through or returning to Australia from offshore. Financial outflows may increase if returned foreign fighters begin sending funds to regional countries or radicalise vulnerable members of the community. Restrictions on cross-border movements imposed in response to the COVID-19 pandemic are likely to have limited the ability for foreign fighters to return to Australia. These restrictions also likely affected the ability for cash to be moved into or out of Australia for terrorism financing purposes.

One terrorism financing-related SMR from the sector involved an overseas bank that was a customer of a bullion dealer and was linked to a terrorist organisation through media reports.

Six SMRs were identified in the third-party SMR sample, with suspicions about the following activities:

- An individual identified with account activity that was inconsistent with their customer profile and transactions that included the purchase of bullion. The individual was also transferring funds between Australia and a higher-risk jurisdiction for terrorism.
- A customer was identified making suspicious purchases of chemicals, weapons, replica law enforcement badges, and survival literature. The customer also purchased gold bullion coins, bars and rounds. These purchases were all made in an online marketplace using a prepaid and a debit card.
- A reporting entity linked a number of individuals, businesses and a charity with possible terrorism financing. One business was identified as part of a criminal syndicate defrauding GST in a gold bullion scam. This business and a number of individuals were linked to a charity suspected of terrorism financing.
- An individual purchasing possible far-right extremist material online. The individual had recently purchased firearms, made payments to an indoor shooting range and made a significant cash advance from their credit card before transferring these funds to a bullion dealer.
- An SMR was submitted as a result of a law enforcement request for information as part of an investigation into an arson attack on critical infrastructure. The group linked to the arson attack was suspected of engaging in the financing of terrorist acts. Of interest was an online debit card transaction at a bullion dealer.

- A government agency requested the transaction history of an individual suspected of engaging in potential terrorism financing. An open source search linked the individual to extremist views and membership of an extremist group. The transactions revealed multiple domestic transfers and cash deposits into a single account from 23 different third parties with transaction descriptions in line with extremist ideology. The individual used a debit card linked to this same account to purchase bullion from a bullion dealer.

Terrorism financing in the sector appears to be very limited, with just one intelligence report identifying suspected terrorist actors linked to bullion.

SYDNEY-BASED GANG, SUPPORTIVE OF ISIL, INVOLVED IN CRIMINAL ACTIVITY PURCHASING BULLION

An intelligence report alleges that a Sydney-based gang involved in criminal activity including extortion, fraud, firearm offences and the manufacture and distribution of illicit drugs was sending funds to ISIL. An individual extorted by the gang was manufacturing fraudulent identity documents and activating stolen credit cards. Funds stolen from bank accounts were placed onto the stolen credit cards and then these were used to purchase high-value goods including gold bullion.

Open source materials report al Qaeda and ISIL are expanding in Africa and are actively working to take over artisanal gold mining operations in countries like Mali, Burkina Faso and Niger.[22] In Australia, a number of bullion dealers provide refining services to foreign entities. The risk exists that terrorist groups can misrepresent the origin of the gold-bearing material to be refined to create profits or launder the proceeds of crime here in Australia.

Identifying terrorism financing

Terrorism financing can be difficult to identify. It can be difficult to link the source of funds and transactional activity in Australia to the end use, and terrorist activities often require little to no funding. Terrorism financing funds are often acquired through legitimate means such as wages, government benefits, loans, family support and business earnings, which further complicates detection.

In some instances, funds are acquired through fraudulent means such as loan fraud, credit card fraud and fundraising under the guise of charitable giving. Fundraising activities through non-profit organisations and online campaigns can occur. Please refer to Australia's non-profit organisation sector money laundering/terrorism financing risk assessment for more detail.

[22] D Lewis and R McNeill, *How jihadists struck gold in Africa's Sahel*, Reuters website, 2019, accessed 29 September 2021.

PREDICATE OFFENCES

AUSTRAC assesses the nature and extent of threat posed by predicate offending involving bullion dealers as **low**.

The main predicate offences linked to the sector include tax evasion, fraud, scams, and theft. To a lesser extent, drug trafficking was also identified.

Predicate offences involving the bullion sector ranged from simple to more complex schemes. Personal income tax evasion was the most common suspected offence, and associated values were low – generally below the $10,000 reporting threshold.

IDENTIFYING PREDICATE OFFENCES – A CHALLENGE FOR REPORTING ENTITIES

Reporting entities may not be able to identify specific criminal offending, even when funds are suspected to be the proceeds of crime. It can be difficult to determine the predicate offence in the absence of law enforcement intelligence or media reporting. This challenge is amplified where the predicate offence has no nexus to the reporting entity. For example, cash derived from drug trafficking is very difficult for a bullion dealer to detect because they have no visibility of the offending.

Reporting entities do not need to establish the predicate offence before submitting an SMR. Individual pieces of information may collectively help authorities to determine the offence. Reporting entities should remain vigilant of key criminal market trends in Australia and report any suspicions of related financial transactions to AUSTRAC in a detailed SMR. Guidance on submitting SMRs can be found on AUSTRAC's website.

Tax evasion

Personal tax evasion was the most common predicate offence identified in 52 per cent of the SMR review, 13 per cent of third-party SMRs and 13 per cent of the IR review. Structured transactions and the use of cash were the most common activities associated with personal tax evasion. In a number of cases, the customer indicated to the reporting entity that the transaction was being structured. Cash income was also being used to purchase bullion for reasons that could not be clearly established in the SMRs. Industry consultations indicated it is possible bullion is purchased as a means to store value outside of the banking and taxation system, and to avoid scrutiny by banks and government agencies.

Industry consultations also indicated bullion could also be used as a personal tax evasion method for inter-generational wealth transfer. In some cultures gold in particular is seen as a way to pass on and preserve wealth from one generation to the next.[23] While Australia does not currently have any kind of inheritance tax, assets that are passed on to beneficiaries that change a person's financial position would be subject to the relevant taxes.[24] One reporting entity indicated it was likely that the purchase and transfer of this bullion by the benefactor is being used to avoid tax by the beneficiary. In such cases, structuring the sale or purchase of bullion is a method to avoid notifying authorities of the transaction.

Corporate tax evasion was identified in two per cent of the SMR review, five per cent of third-party SMRs and 16 per cent of the IR review. In a number of cases, bullion dealers making large cash deposits inconsistent with the company profile raised suspicions. Jewellery businesses were also identified in a number of cases for purchasing gold from bullion dealers in quantities far exceeding

[23] T Daltorio, *8 Good Reasons To Own Gold*, Investopedia website, 2021, accessed 29 September 2021.

[24] Australian Taxation Office, *If you are a beneficiary of a deceased estate*, ATO website, 2021, accessed 12 July 2021.

what would be considered normal for a business of that size, and for paying business invoices using cash.

THE SHADOW ECONOMY

Bullion dealers should be aware of how their products and services can enable the shadow economy and take steps to mitigate the harms the shadow economy can cause. In its final report, the Black Economy Taskforce stated that the shadow economy could be as large as three per cent of GDP.[25]

In response to the recommendations of the Black Economy Taskforce's final report the Federal Government announced the ATO would lead the cross-agency Black Economy Standing Taskforce (BEST) to combat the shadow economy.[26] [27] BEST brings together government agencies, including AUSTRAC, to exchange information and deliver a coordinated approach to identifying and addressing serious, complex and high-value shadow economy activity.

Fraud

Fraud was identified in 11 per cent of the SMR review, 15 per cent of third-party SMRs and 35 per cent of the IR review. The most common types of fraud included the use of fake or stolen identification documents and credit card fraud. When conducted in person there were also indicators of suspicious customer behaviour, such as nervousness or aggression.

FRAUDSTERS TAKING ADVANTAGE OF DELIVERY CHANNELS TO PURCHASE BULLION

A bullion dealer reported a case of a customer placing an order for bullion on the company's website. Two days after the order was placed, the bullion dealer's bank notified them that the cheques used to pay for the transaction were fraudulent. The bullion dealer was notified in time to stop the transaction.

In another case, a bank informed the bullion dealer that their customer's phone had been hacked and that two significant orders for bullion had been made through the use of a third-party electronic biller. The bullion dealer was notified in time to cancel the transaction prior to dispatching the bullion. The use of third-party electronic billers was a common indicator among several of the reported fraudulent transactions in the SMR review (see **Complexity of product delivery arrangements** on page 36).

Four per cent of the SMR review, three per cent of third-party SMRs and six per cent of the IR review related to credit card use. In a number of cases suspicions were raised when the customer chose to pay using a credit card rather than an alternative method that did not incur fees, which was inconsistent with typical customer behaviour. Criminals may use stolen credit cards, open credit cards with stolen identity information, or use the proceeds of crime to pay off credit cards.

Industry consultations indicated the sector considers accepting credit card payments for bullion purchases to be higher-risk for fraud and a number of reporting entities do not accept credit card payments for bullion.

---

[25] Black Economy Taskforce, *Black Economy Taskforce: final report–Oct 2017*, The Treasury, 2017, p. 35.

[26] Black Economy Taskforce, *Black Economy Taskforce: final report–Oct 2017*, The Treasury, 2017.

[27] Australian Government, *Budget 2018-19 Budget Paper 2: Budget Measures*, Budget Archive, 2019, p. 181.

STOLEN CREDIT CARD USED TO PURCHASE BULLION

An elderly bank customer received a call from a person claiming to be from the bank and querying a credit card transaction. The customer was deceived into providing all of their credit card account details, including their PIN, to the caller. The customer was informed that a bank representative would pick up the card in person. While they were still on the phone, a person knocked on the door, introduced themselves as being from the bank and took possession of the customer's credit card.

A number of transactions were then conducted on the stolen credit card before the card could be blocked. An attempt to use the stolen credit card to purchase bullion was blocked before it could be completed.

During industry consultations, one reporting entity indicated they suspect some customers are committing welfare fraud by purchasing bullion to keep their bank balances and visible assets low enough to continue qualifying for welfare benefits.

MULTI-MILLION DOLLAR NATIONAL DISABILITY INSURANCE SCHEME (NDIS) FRAUD

In December 2020, the AFP, in partnership with the National Disability Insurance Agency, AUSTRAC and Services Australia, launched Operation Pegasus to investigate several suspected fraudulent NDIS providers based in Western Sydney. The AFP arrested six people allegedly involved in a crime syndicate after it was alleged they fraudulently claimed more than $10 million in NDIS funding.

Over $2 million in suspected tainted assets were seized during the search warrants including eight kilograms of gold bullion from a vault at a secure premises, worth approximately $600,000.[28]

Reporting entities are encouraged to consider Fintel Alliance's NDIS fraud financial crime guide to identify suspicious activity and report it to AUSTRAC.

Scams

Scams were identified in less than one per cent of the SMR review, 17 per cent of third-party SMRs and 13 per cent of the IR review. The most common type of scam was business email compromise where the criminal proceeds were then used to purchase bullion. In a number of cases, law enforcement notified bullion dealers that the funds were the proceeds of scams.

Partner agency consultations indicate the bullion sector has been used to launder the proceeds of business email compromise scams during the COVID-19 pandemic. Business email compromise scams occur when criminals use email to target organisations, often by issuing fraudulent invoices or impersonating a vendor. The victim pays the fraudulent invoice into the criminal's bank account.[29] The criminal then moves the funds out of the account as quickly as possible.

Other identified scams included a Ponzi scheme where the proceeds were withdrawn to purchase bullion.[30] A number of SMRs related to romance scams where victims deposited funds into bank accounts and then the perpetrators used the funds to buy bullion.

---

[28] Australian Federal Police, *Western Sydney fraud syndicate dismantled, six charged*, [media release], AFP website, 2021, accessed 27 October 2021.

[29] Australian Signals Directorate, *Protecting Against Business Email Compromise*, Australian Cyber Security Centre website, 2021, accessed 12 July 2021.

[30] A 'Ponzi' scheme is a scam in which the promoters attract investors to a scheme by promising a very high return on investment, while guaranteeing the security of the investment. The scammers use some of the funds deposited by early investors to pay initial dividend cheques or interest. At this early stage the ponzi scheme only requires a few investors to operate successfully. The promoter continues paying the investors impressive dividends for a couple of months until the investors, encouraged by the early dividends, decide to invest more. The investors may also

Like other predicate offences, bullion purchased using the proceeds of scams can be difficult for the reporting entity to identify, particularly when the scammers are using mules. It was often banks who initially identified scams and then informed the bullion dealer that a transaction was under investigation, which led to the dealer submitting an SMR.

BUSINESS EMAIL COMPROMISE SCAM

A criminal gained access to the email account of a public sector employee. The criminal intercepted a genuine invoice from a vendor which was then changed to include the criminal's bank details before sending on to the victim. The victim processed the false invoice paying a large sum into the bank account of the criminal. Through a mule, the criminal used the majority of the funds to purchase bullion. The mule then travelled overseas and remains offshore, where it is likely they are based. It is unknown if the gold bullion was moved offshore or remains with Australia-based syndicate members.

PURCHASE OF GOLD BULLION TO LAUNDER PROCEEDS OF BUSINESS EMAIL COMPROMISE SCAMS

In 2020, a multi-agency taskforce was established to combat and mitigate the impact of business email compromise scams in Australia. The taskforce identified cases where gold bullion and foreign currency were purchased with the proceeds of business email compromise scams, highlighting an emerging trend for this cashing out methodology in Australia.

Fraud and scam threats are continually evolving. Bullion dealers should remain vigilant to specific fraud and scam methods relevant to their business and customers. and AUSTRAC encourages the sector to:

- promote customer education and awareness
- report suspected scam-related activity in SMRs
- continue strengthening fraud mitigation systems and controls
- report scams to the Australian Competition and Consumer Commission (ACCC) through the Scamwatch website.

Theft

Due to their inherent value, precious metals are attractive to thieves at all stages of the mining, refining and retail process. The precious metals mining industry is vulnerable to theft because the product is relatively easy to identify, easy to sell, and can be mixed with legitimately acquired gold and other precious metals.[31]

SMRs submitted by the sector and partner agency consultations include concerns that bullion and jewellery offered for sale to bullion dealers may be stolen. Recent media articles include a case of a number of individuals in the bullion sector being charged with knowingly buying stolen gold jewellery

encourage their friends and relatives to invest. Soon there is a steady flow of funds into the scheme and an ever-growing number of investors. If the promoter is disciplined and retains sufficient funds in the scheme to continue to pay out 'dividends', a ponzi scheme can continue for many years.

[31] B Coetzee and R Horn, *Theft of precious metals from South African mines and refineries*, Institute for Security Studies website, 2007, accessed 3/09/2021.

from criminals. This included avoiding asking suspicious customers for identification and organising the prompt melting down of gold jewellery they believed was stolen.[32] [33]

Media reports also indicate that on a number of occasions, trusted insiders stole bullion from bullion dealers (see **Employee due diligence and training** on page 45).[34]

Drug trafficking

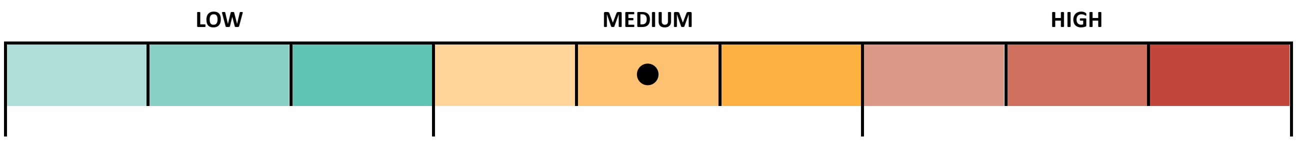
Less than one per cent of the SMR review and one per cent of the third-party SMR sample related to drug trafficking. In one case, the reporting entity believed the proceeds of drug trafficking had been laundered through a bank account and used to purchase bullion. More than a quarter of the IR review included links to drug trafficking. These cases included the use of bullion dealers and jewellers to allegedly launder the proceeds of crime linked to drug trafficking.

[32] D Estcourt, *Man jailed over scheme to sell stolen jewellery as gold bullion*, The Age website, 2020, accessed 30 June 2021.

[33] J Menagh, *Perth Mint thief stole $55,000 in gold coins, bars to fund fiancee's lifestyle demands*, ABC News website, 2018, accessed 3 September 2021.

[34] C Houston and A Cooper, *Renaissance man turned robber gets four years for $3.2m gold theft* , The Age website, 2020, accessed 29 October 2021.

VULNERABILITIES



VULNERABILITY FACTOR	RATING
CUSTOMERS	
PRODUCTS AND SERVICES	
DELIVERY CHANNEL	
FOREIGN JURISDICTIONS	

Vulnerability refers to the characteristics of a sector that make it susceptible to criminal exploitation.

AUSTRAC assesses the bullion sector is subject to a **medium** level of inherent vulnerability related to money laundering, terrorism financing, and other predicate offences.

AUSTRAC's vulnerability assessment falls into four broad categories: customers, products and services, delivery channels, and exposure to foreign jurisdictions.

CUSTOMERS

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

IMPACTS OF COVID-19

The COVID-19 pandemic has had a significant impact on the size of the bullion sector's customer base, the way bullion dealers offer their products and services, bullion dealers' exposure to international customers and the way customers choose to pay for their bullion. AUSTRAC judgements around inherent vulnerabilities remain true and are independent of the pandemic.

Size of the customer base

The lack of available data regarding sector-specific customer numbers makes it difficult to quantify the exact size of the customer base. The bullion sector likely has a medium-sized customer base, exposing it to a medium level of inherent ML/TF vulnerability. Given the customer base generally shifts in line with external factors such as market prices and macroeconomic conditions, it is also difficult to estimate the future trajectory of the sector's customer base.

Unlike some parts of Asia and Europe, bullion is still considered a relatively niche investment in Australia, limiting the size of the customer base.[35] [36] Bullion dealers serve more customers during periods of economic and political uncertainty because bullion is seen as a stable asset, and is sought out as a store of value.

Industry consultation indicated that a small number of bullion customers hold unconventional views about the stability of society or financial systems. This can result in unusual behaviour when purchasing or selling bullion, which may initially look like suspicious behaviour for ML/TF purposes. This can complicate the detection of suspicious transactions, possibly allowing those who are using the sector for illicit purchases to transact undetected.

THE IMPACT OF COVID-19 ON BULLION DEMAND

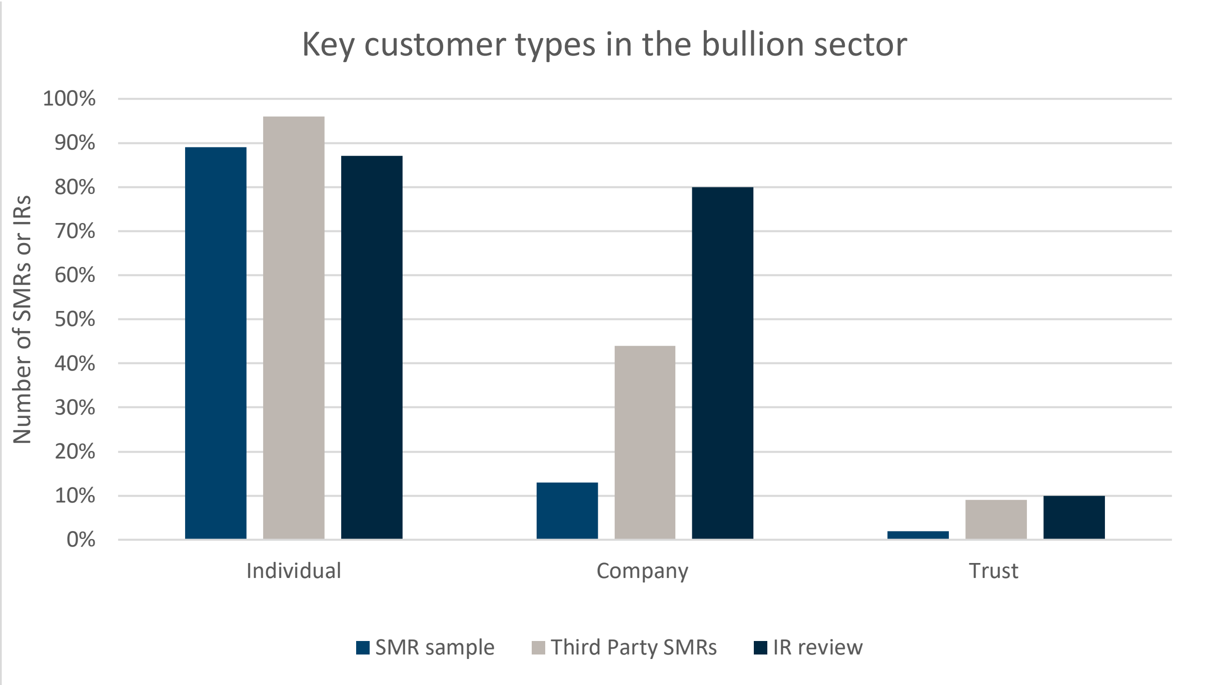
The COVID-19 pandemic drove a significant increase in the number of customers investing in bullion in an effort to insulate themselves from perceived or actual social and market volatility. One bullion dealer consulted for this assessment reported a four-fold increase in customers following the emergence of COVID-19 and almost all bullion dealers noted an increase in bullion demand over this period. On the other hand, COVID-19 has reduced consumer demand for jewellery which has negatively impacted bullion dealer sales to jewellery stores.

A larger customer base can increase the sector's exposure to criminal activity, and make this activity more difficult to detect.

The SMR review indicated the majority of bullion dealer customers were individuals (89 per cent), followed by companies (13 per cent), trusts (2 per cent) and one case of an association (0.13 per cent). Responses to the 2020 Compliance Report indicated 82 per cent of reporting entities in the bullion sector serviced companies as customers and 75 per cent serviced trustees as customers.

[35] Sunshine Profits, *Germany and Gold*, Sunshine Profits website, accessed 31 August 2021.

[36] World Gold Council, Geographical diversity, World Gold Council website, accessed 31 August 2021



Higher-risk customers

AUSTRAC assesses the bullion sector is exposed to a limited number of higher-risk customers. This assessment is based on SMR analysis, the IR review, results from the data-matching exercise, and qualitative insights from industry and partner agencies.

Thirteen per cent of bullion dealers said they had higher-risk customers in their responses to the 2020 Compliance Report. Importantly, customers that transact under the $5,000 threshold are not required to provide identification, therefore bullion dealers may not be able to fully assess the risk of these customers. As a result, the volume of higher-risk customers transacting in the bullion sector may be underestimated.

Although limited in number, higher-risk customers are present across a range of customer categories, including:

- foreign-based customers
- known or suspected criminals
- politically exposed persons (PEPs)
- companies, trusts and other legal entities
- jewellers and scrap precious metal dealers.

Foreign-based customers

During consultations, reporting entities highlighted foreign-based customers as posing a higher level of inherent ML/TF vulnerability than Australian-based customers. The most significant vulnerabilities relate to customer due diligence (CDD) checks because foreign-based customers cannot be physically identified and there are challenges in authenticating foreign identification documents.

Foreign-based entities were observed in approximately six per cent of the SMR review, 13 per cent of the third-party SMR sample and 39 per cent of the IR review. Common themes identified in these reports include:

- connections to higher-risk jurisdictions
- unusual transactions, sometimes involving credit cards

- concerns regarding the use of foreign identification documents
- suspected involvement in money laundering, tax evasion, scams or fraud.

Known or suspected criminals

The bullion sector is likely to have limited exposure to known or suspected criminals, presenting a low inherent ML/TF vulnerability.

AUSTRAC conducted a data-matching exercise using TTRs and SMRs submitted to AUSTRAC by the bullion sector between 1 July 2020 and 30 June 2021 matched against known criminal entities to identify the proportion of customers who were:

- recorded as a member or associate of a significant regional, national or transnational serious and organised crime group as at April 2020;
- charged with a money laundering or proceeds of crime-related offence between 1 January 2017 and 30 June 2021;
- charged or associated with a terrorism-related offence between 1 January 2017 and 30 June 2021.

This resulted in one bullion sector customer being identified as an outlaw motorcycle gang member. The customer made three purchases of bullion from a bullion dealer using cash, totalling over $160,000.

Approximately one per cent of the SMR review, one per cent of the third-party SMR sample and 39 per cent of the IR review related to members of a criminal network or gang. The subjects of law enforcement IRs are more likely to be members of a criminal network or gang compared to the subjects of SMRs submitted by reporting entities. Partner agency consultations indicated limited exposure to known or suspected criminals in the bullion sector.

Companies, trusts and other legal entities

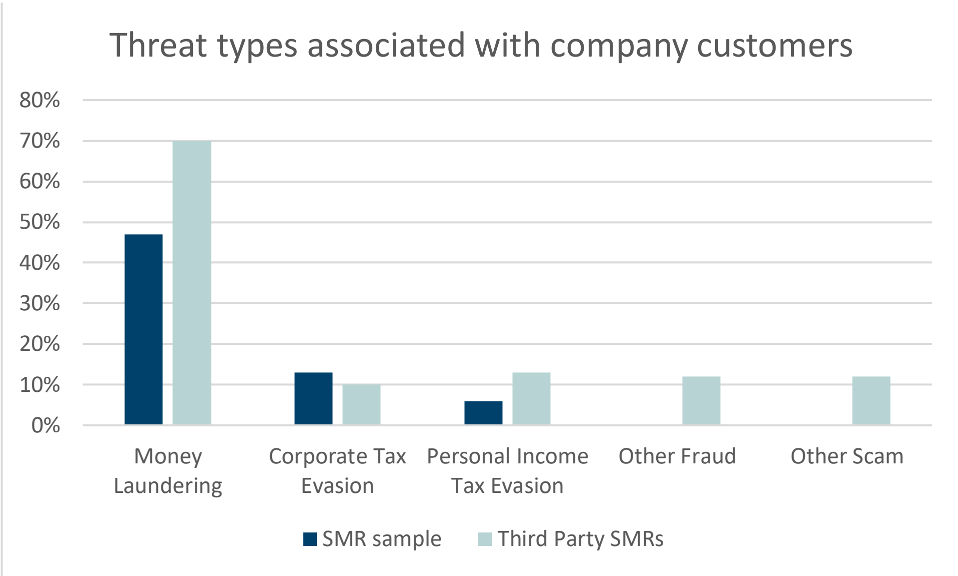
Companies, trusts and other legal entities can expose bullion dealers to higher inherent ML/TF vulnerability. The extent of vulnerability depends on multiple factors including the industry, business model, and transparency of beneficial ownership.

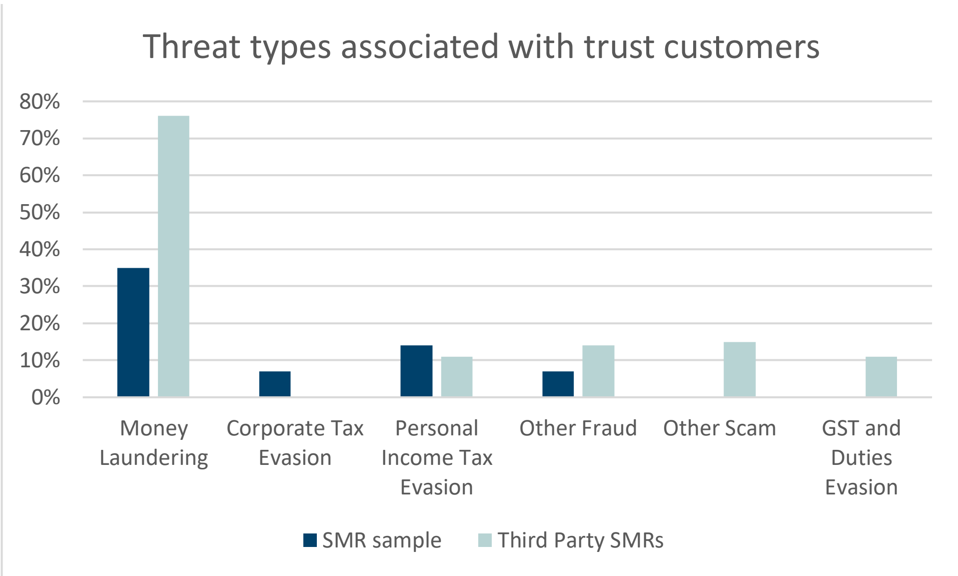
Companies, trusts and other legal entities generally conduct larger and more frequent transactions. This can complicate detection of suspicious activity and obscure the source, destination and beneficial ownership of funds, particularly when combined with a complex structure of entities, or an offshore nexus.

WHAT IS A COMPANY, TRUST AND LEGAL ENTITY CUSTOMER?

Companies, trust and legal entities customers are non-natural persons. They can be public companies, incorporated or unincorporated partnerships, incorporated or unincorporated associations or entities using trust structures. There are many legitimate reasons for a corporate customer to purchase or sell bullion, for example, as a secure investment, particularly during market volatility and as a hedge in times of economic uncertainty and inflation.

Company customers were identified in 13 per cent of the SMR review and trusts in two per cent of the SMR review. The third-party SMR sample identified company customers in 44 per cent of SMRs and trusts in nine per cent of SMRs reviewed.





Note: Percentages may add to more than 100 because many SMRs related to more than one customer type.

Self-managed superannuation funds (SMSFs) continue to grow in popularity as an alternative to traditional APRA-regulated superannuation funds. Consultations indicate that some SMSF trustees often include bullion in their portfolios. One SMR in the SMR review identified the use of superannuation accounts, while four per cent of the third-party SMR sample related to superannuation accounts. A number of these SMRs related to funds derived from superannuation accounts being used to purchase bullion.

Common themes observed in reports relating to companies, trusts and other legal entities include:

- false invoice scams using corporate customers
- corporate customers paying invoices for bullion using cash
- fraudulent set up of an auto-debit against a bank account linked to a trust fund
- corporate customers making purchases that are inconsistent with their customer profile
- corporate customers purchasing bullion and not being concerned about price, delivery or storage costs

- purchasing bullion in an individual's name and then immediately selling the bullion to their self-managed superannuation fund.

While not unique to bullion dealers, criminals will take advantage of the vulnerabilities associated with companies to launder illicit funds. For example:

- Criminals will often appoint a family member or 'cleanskin' associate as a director or shareholder to distance themselves from the purportedly legitimate entity.
- Criminals can use stolen identities to establish a company that is subsequently used to launder criminal proceeds.
- Foreign nationals can register Australian companies. Transnational, serious and organised crime groups compel or pay individuals on temporary visas to register companies they can then use to place, layer and integrate illicit funds.
- When a criminal organisation or their affiliates control multiple entities, they can be used to under-invoice, over-invoice or double-invoice to transfer value. This method of trade-based money laundering (TBML) can be used to move illicit money across borders undetected and to evade taxes.

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

AUSTRAC expects bullion dealers to take steps to mitigate the risks of serving corporate customers and other legal entities, and strengthen systems and controls related to transparency and beneficial ownership on an ongoing basis.

If you form a suspicion because of complex beneficial ownership structures or cannot determine the source of funds, you must submit an SMR. Information on identifying beneficial owners is available on the AUSTRAC website.

Jewellers and scrap precious metal dealers

Industry and partner agency consultations, SMR analysis and IR review indicate that customers that are jewellers and scrap precious metal dealers can expose the sector to higher inherent ML/TF vulnerability. It is difficult for a bullion dealer to determine what the bullion being sold to jewellery businesses is being used for. In certain cases, it is suspected that serious and organised crime groups have infiltrated jewellery businesses in order to launder the proceeds of crime.

Granules of fine gold typically used for the manufacture of jewellery are not considered to be bullion for the purposes of the AML/CTF Act and therefore are not subject to CDD procedures (see **Money laundering** on page 16 for more).

JEWELLERY SHOPS USED TO LAUNDER SMUGGLED GOLD

An intelligence report indicated the possibility of significant quantities of gold being smuggled into Australia in order to launder the proceeds of crime derived offshore. Cash derived from the proceeds of crime from a number of higher-risk jurisdictions was converted to gold in the Middle East before being smuggled into Australia using a variety of different methods. The gold was then distributed to a number of different jewellery shops in Australia, operating under the control of the syndicate. The value of the gold was then remitted by the jewellery shop owners through multiple bank accounts controlled by the syndicate.

Politically exposed persons (PEPs)

A PEP is an individual who holds a prominent public position or role in a government body or international organisation, either in Australia or overseas.[37] They can be an attractive target for bribery and corruption given their capacity to influence government spending and budgets, procurement processes, development approvals and grants.

PEPs were identified in less than one per cent the SMR review and third-party SMR sample, and three per cent of the IR review. Responses to the 2020 Compliance Report indicated 52 per cent of reporting entities in the bullion sector did not carry out PEP checks.

Consultations with reporting entities indicated that, in some cases, bullion dealers find it difficult to identify PEPs or are unsure as to what constitutes a PEP. Further information about PEP and sanctions screening is provided in the **Risk Mitigation Strategies section** on page 44.

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

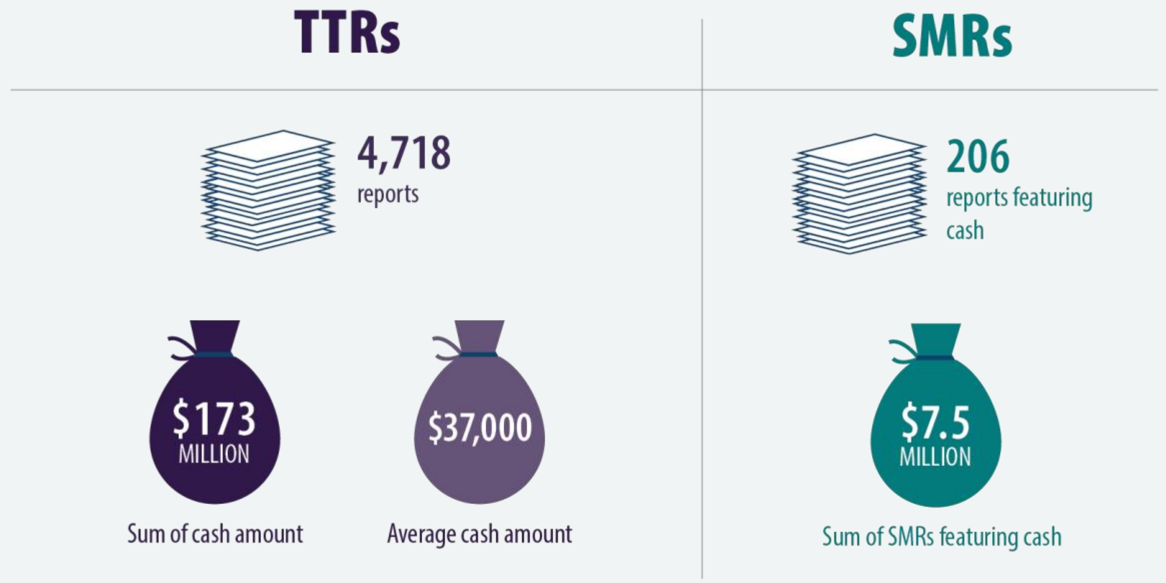
PRODUCTS AND SERVICES

AUSTRAC assesses the nature and extent of the products and services offered by the bullion sector pose a **high** inherent ML/TF vulnerability.

ML/TF vulnerability stems from the sector's exposure to cash, as well as products and services that are sought out to store value and, to a lesser extent, can enable the movement of value.

Use of cash

TTRs AND CASH-RELATED SMRs THE BULLION SECTOR SUBMITTED BETWEEN 1 JULY 2020 AND 30 JUNE 2021[38]



SMR analysis indicates the bullion sector is cash intensive, with 53 per cent of the SMR review involving cash transactions. Industry consultations indicated the use of cash increased with the onset of the COVID-19 pandemic. SMRs featuring cash transactions rose from 34 per cent in 2015 to 51 per cent in 2020. This trend is inconsistent with the general decline in cash transactions across the Australian economy and is inconsistent with AUSTRAC's findings around cash use in other sectors, such as banks and remittance dealers.

A small number of bullion dealers indicated they do not accept cash because they consider it higher-risk. This policy may be in place for security considerations as taking large amounts of cash physically to be deposited in a bank may increase the risk of theft. Bullion dealers that do not accept cash may provide the option to customers of depositing the cash into the bullion dealer's bank account.

Ability to store and move funds

The high intrinsic value of gold bullion makes it popular for criminals to store and invest the proceeds of crime. Both legitimate investors and criminals see gold as a hedge against inflation, currency risk, and a store of value during economic and political uncertainty.

Bullion is also relatively easy to conceal and move – including across domestic and international borders – and to convert back to legitimate funds. There is no AML/CTF Act requirement for

[38] A number of bullion dealers also deal in cryptocurrency. SMRs and TTRs submitted by bullion dealers that related exclusively to cryptocurrency were removed from the SMR and TTR review.

international travellers to declare gold bullion at the border, although customs legislation does require any imported goods valued over $1,000 and goods being exported valued over $2,000 to be declared (see **Movement of funds internationally** on page 37).[39]

Consultations with bullion dealers indicated customers may purchase bullion in amounts that are easy to conceal and carry as a commercial passenger on an aircraft, such as half a kilogram of gold.

Precious metal certificates

Precious metal certificates verify the ownership of a certain amount of precious metal – usually gold, silver or platinum. The authority that issues the certificate usually stores these in a safe location. Some certificate programs allow investors to hold their precious metal offshore using an international distributor network, exposing the bullion dealer to foreign jurisdiction risk.

Criminals can use third parties to purchase the certificates and launder the proceeds of crime. This allows criminals to distance themselves from the asset and obfuscate the true source of funds that was used to acquire it. Criminals can arrange for the purchase of gold certificates through third parties, or 'cleanskins' and mules.

Gold and silver scrap jewellery and bullion refining

Some bullion dealers are also bullion refiners. In addition to refining gold ore mined in Australia, these entities also refine gold mined offshore, exposing them to foreign jurisdictions risk (see page 37 for more).

Refiners can also refine gold scrap jewellery sourced from Australia and internationally. A number of bullion dealers buy gold and silver scrap jewellery from the public, which can be melted down and refined. This business model exposes bullion dealers to significant money laundering vulnerabilities because it is difficult to trace the true source of scrap gold or silver, which could be stolen or be used as part of a money laundering scheme. Once refined, the true source of this metal is impossible to trace.

Bullion dealers indicated they often consider the physical appearance of a customer when considering whether the customer could be involved in criminal activity. It's important to focus on a range of factors, not just physical appearance, which may be used to hide more sophisticated efforts to sell stolen scrap jewellery.

DELIVERY CHANNELS

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

Delivery channels refers to how a sector delivers products and services to their customers. Over the past two years, COVID-19 restrictions have forced many transactions online or to a click-and-collect model. These channels increase anonymity, which can make it more difficult to detect suspicious transactions.

Level of customer contact

The bullion sector uses multiple delivery channels to provide their products and services to customers, including in-store, over the phone and online. Responses to the 2020 Compliance Report indicated 63 per cent of bullion dealers provided both online and face-to-face services, 18 per cent provided only face-to-face services and five per cent only offered online services.

[39] Customs Act 1901.

Face-to-face transactions

Compared to other sectors, the bullion sector has a high rate of face-to-face customer interaction. This is partly due to the preference of many customers to purchase bullion in person, particularly for smaller transactions and when using cash. Face-to-face settings allow bullion dealers to have more interactions with their customers and provide more opportunity to form suspicions that may not be possible when dealing with customers over the phone or online. Consultations with industry indicate it is not uncommon for a customer to order bullion online, or over the phone, and then collect their purchase in person.

Online transactions

With no face-to-face interaction or CCTV monitoring, online transactions introduce an additional element of anonymity that is attractive to criminals. For example, an individual buying or selling bullion online in Australia may not be subject to visual identification as it is possible to purchase bullion online with no identification for orders under $5,000. Online transactions increase a bullion dealer's vulnerability to cyber-enabled fraud.

IMPACT OF COVID-19 ON CUSTOMER CONTACT

Throughout certain periods during the COVID-19 pandemic, bullion dealer retail outlets have been restricted from opening to the public. Bullion dealers that are able to operate normally have implemented measures to reduce face-to-face customer contact. These include encouraging customers to use phone and online services, and operating a click-and-collect model. Consultations with the bullion sector indicate that COVID-19 has reduced the number of face-to-face transactions.

Complexity of product delivery arrangements

The bullion sector has a relatively low level of outsourcing of product delivery channels. The competitive nature of the industry discourages the use of intermediaries such as brokers and other third parties. The sector uses standard couriers, secure carriers or, in some cases, postal services to deliver bullion to customers.

Outsourcing can create ML/TF vulnerabilities by lengthening and complicating the product delivery chain, making it harder for a bullion dealer to detect and act on suspicious activity. Poor governance arrangements can exacerbate this vulnerability.

Third-party electronic billers

Third-party electronic billers enable payments to be made via online, mobile or phone payment systems to businesses such as bullion dealers. Consultation with the sector and information in SMRs demonstrates that identifying the source of payments made through third-party electronic billers is more difficult than when payments are made through other channels, such as direct debit, due to the limited information the sector receives about the sender.

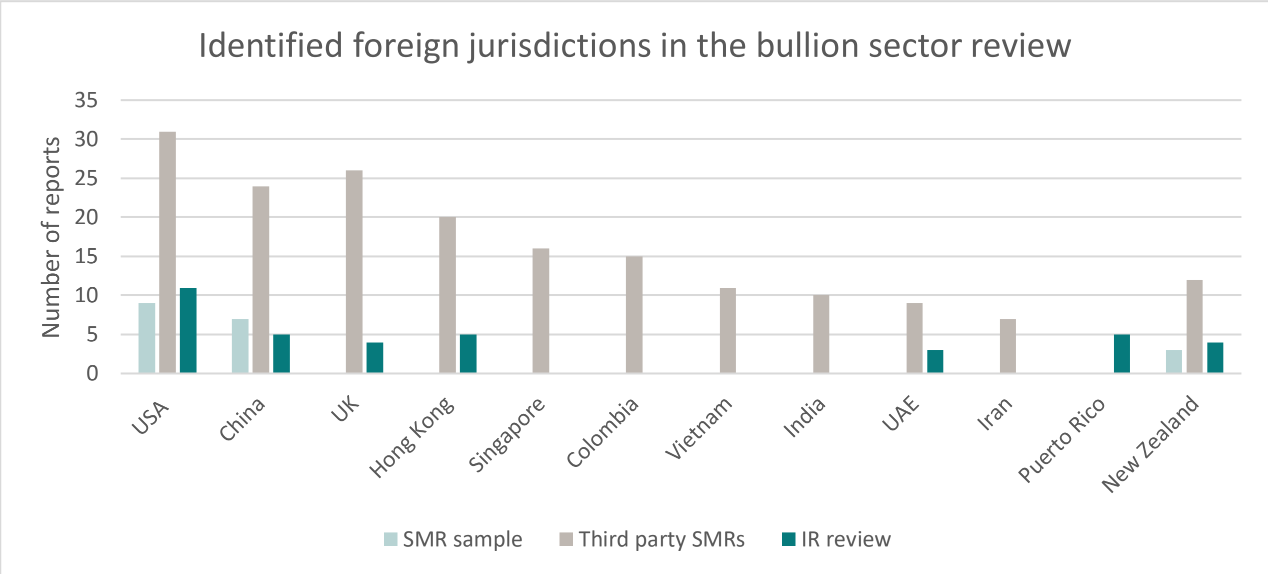
Two per cent of SMRs in the SMR review referred to third-party electronic billers. In the majority of these cases, banks had contacted the bullion dealer to inform them that fraudulent payments were made for bullion using an electronic bill payment system. In these cases, the bullion dealer only became aware of the fraud after the bank informed them, and in a number of instances the bullion had already been supplied.

FOREIGN JURISDICTIONS

AUSTRAC assesses bullion dealers have a **medium** inherent ML/TF vulnerability to foreign jurisdiction risk.

Exposure to foreign jurisdictions poses ML/TF risk because it creates opportunities for international movement of criminal proceeds and the funding of overseas terrorist activity. Further, international transactions add complexity, which can obscure beneficial ownership and beneficiary customers, and increase the potential for offshore tax evasion. The movement of funds across borders can also create challenges for law enforcement to exercise their powers of investigation or arrest.

Movement of funds or value internationally



Bullion dealers submitted no international funds transfer instruction (IFTI) reports for the period 1 July 2020 to 30 June 2021.

Industry consultations indicate that a number of bullion dealers do not trade with overseas customers due to concerns about ML/TF and fraud risk. The SMR review shows few international transactions, with six per cent of SMRs linked to foreign jurisdictions. The third-party SMR sample indicates a higher number of international transactions, with 26 per cent of the SMR sample linked to foreign jurisdictions. Third parties have greater visibility of where transactions and funds originate and accordingly report a higher number of transactions with overseas jurisdictions.

Bullion dealers in Australia that are members of the London Bullion Market Association (LBMA) have a higher level of foreign jurisdiction exposure than their counterparts that are not members. These dealers can sell bullion to traders on the international market and to governments, central banks, the IMF and large financial institutions, whereby the bullion dealers' banks would likely be submitting IFTIs to reflect these transactions. The LBMA is the international trade association representing the global over-the-counter bullion market, and defines itself as the global authority on precious metals. The LBMA maintains and publishes the Good Delivery List for gold and silver. These lists comprise accredited gold and silver refineries that meet the acceptance criteria. The London Good Delivery standard is universally acknowledged as the de facto international benchmark for the quality of large gold and silver bars.[40] Major banks around the world that dominate precious metals trading tend to handle only gold and silver bullion from refineries on the LBMA's Good Delivery List.

When trading bullion at the retail level, bullion dealers lose visibility of metal once it is physically handed to a customer. It is likely customers carry some of this bullion offshore or that, in some

[40] London Bullion Market Association, *About Good Delivery*, London Bullion Market Association website, accessed 27 October 2021.

instances, bullion brought into Australia will be sold to local bullion dealers. The level of compliance with customs requirements regarding the import and export of bullion is difficult to gauge. As a result, it is not possible to accurately estimate the amount of bullion individuals are purchasing for export or import.

IMPACTS OF COVID-19 ON CROSS-BORDER MOVEMENT OF BULLION

COVID-19-related travel restrictions are highly likely to have dramatically reduced the amount of bullion being carried by persons crossing Australia's international borders. Consultations with industry indicated travel restrictions have reduced the number of overseas-based customers buying bullion in person. The travel restrictions may have resulted in some of this activity being displaced to cargo and mail. It is likely that the levels of bullion being carried across Australian borders will increase once COVID-19 travel restrictions are lifted.

Refiners

Concern about potential links between gold and armed conflict, such as civil wars, terrorist and militia activity has resulted in the development of the OECD's Due Diligence Guidance for Responsible Supply Chains for Minerals from Conflict-Affected and High-Risk Areas. [41] This guidance recommends that companies identify the refiners in their supply chain, including information on country of mineral origin for products processed at these refiners. Media reports have identified instances of refiners purchasing gold linked to armed groups and mining operations linked to child labour, environmental degradation and civil conflict.[42] The LBMA has previously suspended its accreditation of gold refiners for failing to meet their responsible sourcing standards.[43]

In addition to newly-mined gold and silver, Australian bullion refiners can also refine gold and silver scrap jewellery sourced internationally. A potential vulnerability is the difficulty in tracing the true source of the metal to be refined. In certain cases newly-mined gold imported for processing is refined locally and then re-exported.[44]

Transactions with higher-risk jurisdictions

Australia is both a significant gold exporter and importer. The bullion sector, particularly those involved with refining, also transacts with higher-risk jurisdictions.[45] A number of gold producing countries and international gold dealing hubs are located in higher-risk jurisdictions. Media reports have raised concerns about gold being smuggled from conflict-affected and high-risk areas to disguise their origins.[46] The SMR review and the third-party SMR sample included instances of the sector's transactions with higher-risk jurisdictions.

[41] Organisation for Economic Co-operation and Development, *Gold industry and sector initiatives for the responsible sourcing of minerals*, OECD website, 2014, accessed 9 September 2021.

[42] Global Witness, *New Global Witness investigation reveals how one of the world's leading gold refiners, Switzerland's Valcambi, sources from UAE's Kaloti, which is linked to Sudanese 'conflict gold'*, Global Witness website, 2020, accessed 9 September 2021.

[43] London Bullion Market Association, *Kyrgyzaltyn JSC Suspended from Good Delivery List*, [media release], London Bullion Market Association website, 2021, accessed 2 November 2021.

[44] T Nguyen, *The Australian Gold Industry, Trade, And Markets*, Singapore Bullion Market Association website, 2019, accessed 10 September 2021.

[45] Observatory of Economic Complexity, *Where does Australia import Gold from?*, Observatory of Economic Complexity website, 2019, accessed 10 September 2021.

[46] T Treadgold, *Forget Diamonds, The New Conflict Commodity Is Gold*, Forbes website, 2020, accessed 9 September 2021.

DETERMINING HIGH-RISK JURISDICTIONS

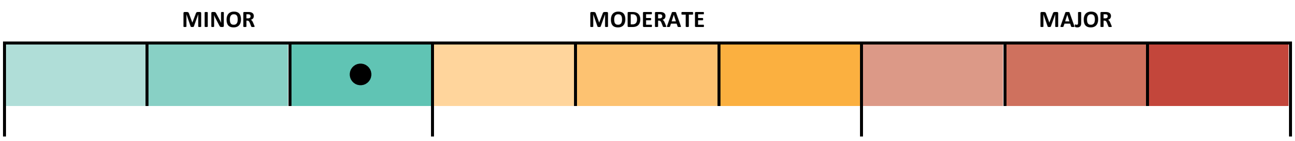
There is no one-size-fits-all list of high-risk jurisdictions. Reporting entities should adopt a risk-based approach when determining which jurisdictions to consider high risk for their business. AUSTRAC encourages the use of a range of sources that assess jurisdictions on different AML/CTF factors, including but not limited to their regulatory frameworks, threat environment, and domain-specific vulnerabilities.

Some reporting entities may choose to use off-the-shelf solutions that risk rate jurisdictions. If doing so, reporting entities should consider their own risk profile and ensure they can customise default risk ratings to accurately reflect their business.

AUSTRAC has made its own determination about which jurisdictions are considered higher-risk for this report. This takes into account Australia-specific factors, such as top source or destination jurisdictions for higher-risk financial flows, as well as global factors, such as the strength or weakness of a jurisdiction's AML/CTF regulatory regime. Open source information AUSTRAC has drawn on to inform these decisions include:

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

CONSEQUENCES



CONSEQUENCES FACTOR	RATING
CUSTOMERS	
INDIVIDUAL BUSINESSES AND THE SECTOR	
THE AUSTRALIAN FINANCIAL SYSTEM AND COMMUNITY	
NATIONAL AND INTERNATIONAL SECURITY	

AUSTRAC assesses that the consequences of criminal activity in the bullion sector are **low**.

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

Financial crime in the bullion sector has consequences for customers, individual businesses, the sector as a whole, and the broader Australian economy. Bullion dealer services used for terrorism financing or serious transnational crime has consequences for national and international security.

CUSTOMERS

AUSTRAC assesses that ML/TF and predicate offences impacting bullion dealers have **moderate** consequences for customers of the sector.

Criminal activity can have varying degrees of impact on customers of the sector. This can depend on the type of customer, their ability to detect criminal activity and their capacity to absorb potential financial losses. For example, corporations may be better able to detect and prevent criminal activity and absorb financial losses. Individual customers generally have less capacity to overcome financial losses from offences such as fraud and scams. During consultations, bullion dealers identified elderly customers as being particularly susceptible to such crimes, especially those involving cyber-enabled activity.

The type of criminal activity affects the level of harm to customers. For example, while a customer purchasing bullion in an attempt to evade tax is unlikely to experience significant harm, victims of fraud and scams are likely to suffer serious, and often unrecoverable, financial losses. The impacts of criminal activity on customers of bullion dealers can include:

- financial losses from fraud, identity theft, or scams
- bullion dealers that pass on the higher costs of increasing their resources dedicated to risk mitigation
- reputational damage for corporate customers after using a bullion dealer connected to criminal activity
- emotional distress and potential criminal implications for people knowingly and unknowingly used as money mules or victims of financial abuse.

INDIVIDUAL BUSINESSES AND THE SUBSECTOR

AUSTRAC assesses that ML/TF and predicate offences impacting bullion dealers have **moderate** consequences for individual reporting entities and the bullion sector as a whole.

The impacts of criminal activity on businesses and the wider sector can be reputational, financial, or operational. Of these, reputational damage constitutes a key risk. During consultations, bullion dealers emphasised the potential for criminal activity to tarnish the industry and negatively impact the ability of individual dealers, and the sector as a whole, to attract and keep customers. Many customers are drawn to bullion due to the perception it offers greater stability and privacy compared to other assets and is considered less vulnerable to shocks associated with economic and political instability.

Reputational costs may include:

- dissatisfaction from, and loss of, customers, partners or investors
- difficulty beginning or maintaining a relationship with financial institutions
- damage to a bullion dealer's brand or the reputation of the sector generally
- increased interest from criminal elements seeking to exploit weaknesses, further degrading the sector's reputation.

Financial costs may include:

- increased insurance premiums
- increased public relations costs
- possible civil penalties for serious non-compliance
- loss of revenue from crime such as credit card fraud

- customers deterred by increased controls and scrutiny leading to reduced revenue
- increased costs to combat criminal attacks, such as costs to enhance physical security
- increased costs caused by disruption from criminal activities and law enforcement interventions
- increased costs to improve AML/CTF compliance management, including investigating suspicious activity.

Operational impacts may include:

- loss of staff or change of senior management personnel
- heightened regulatory oversight or law enforcement action
- tightening of systems and controls on certain products, services or delivery channels.

AUSTRALIAN FINANCIAL SYSTEM AND THE COMMUNITY

AUSTRAC assesses that money laundering, terrorism financing and predicate offences impacting bullion dealers have **minor** consequences for the Australian financial system and the community.

Despite limited levels of suspected criminality in the bullion sector, money laundering helps criminals preserve illicit assets, finance new crimes, and can lead to the corruption of public officials and private enterprise. Significant or systemic breaches of AML/CTF obligations in the sector could result in some damage to Australia's international economic reputation and, by association, the security and safety of Australia's financial system.

Other consequences of criminal activity on the Australian financial system and the community can include:

- loss of confidence in the integrity of the Australian financial system
- harm inflicted on the community through offences such as fraud or scams
- reduced government revenue due to tax evasion, affecting the delivery of critical government services.

NATIONAL AND INTERNATIONAL SECURITY

AUSTRAC assesses that ML/TF and predicate offences impacting bullion dealers have **minor** consequences for the Australian financial system and the community.

Serious organised criminal groups in Australia can increase in size and strength when they are able to launder their illicit funds. Their activities can impact both national and international security interests. For example, gang-related violence can threaten domestic security (e.g. outlaw motorcycle gangs).

The potential harm to national and international security from terrorism financing is significant. Potential impacts can include:

- enabling terrorist acts both in Australia and overseas
- enabling and sustaining the activities of Australian foreign terrorist fighters.

Bullion sourced without proper due diligence of the supply chain can help perpetuate armed conflict, violence, and human rights abuses abroad. In politically unstable jurisdictions, the precious metals trade can be used to support corruption, money laundering and finance armed groups, and can fuel forms of exploitation such as forced labour.[47]

[47] European Commission, *Conflict minerals regulation*, European Commission website 2020, accessed 6 September 2021.

RISK MITIGATION STRATEGIES

Risk mitigation strategies include both measures that are mandatory under AML/CTF legislation, and additional measures businesses may implement to mitigate their money laundering and terrorism financing risks.

The sophistication and implementation of risk mitigation strategies varies significantly between bullion dealers, presenting ongoing and potentially significant risks to the sector. A number of bullion dealers consulted for this report outlined less sophisticated approaches to AML/CTF, including immature customer due diligence practices, general staff training, and a basic understanding of their AML/CTF obligations.

A small number of larger bullion sector entities outlined relatively comprehensive risk mitigation strategies in place, including internal audits, introductory and ongoing training of staff and the use of dedicated AML/CTF staff to inform their policies and practices. Additionally, bullion dealers often conduct due diligence for business protection purposes, which also helps to protect them from financial crime.

There is scope for improvements to be made to ensure:

- enterprise risk assessments are tailored to the business, are well documented and updated regularly
- better understand and consistently apply politically exposed person and sanctions screening
- seek an independent review of their Part A AML/CTF program
- provide employees with adequate and regular training in AML/CTF
- have systems in place to detect and report suspicious matters to AUSTRAC, and ensure reporting contains appropriate information and detail.

RISK ASSESSMENTS

Industry consultations revealed a limited understanding and approach to risk assessment processes among many bullion dealers. Approximately 15 per cent of bullion dealers that submitted a compliance report in 2020 indicated they did not have a documented process for conducting risk assessments.

A robust risk assessment is the centrepiece of an effective AML/CTF regime. It is important that risk assessment processes have the capacity to generate a genuine understanding of ML/TF exposure at an individual reporting entity level. This means that bullion dealers need to be considering their own experience including what has been identified within the business, sector-wide experience and a robust understanding of the Australian ML/TF landscape. Not only do risk assessments need to be business-specific, they also need to be updated regularly to ensure changes in risk profiles and systems, as well as the nature of products or delivery channels, are addressed in a timely and effective way.

PEP AND SANCTIONS SCREENING

One half of bullion dealers who submitted a compliance report in 2020 indicated they did not carry out PEP checks. Consultations with reporting entities indicated that, in some cases, bullion dealers find it difficult to identify PEPs or are unsure as to what constitutes a PEP.

Bullion dealers using a single source to detect PEPs or sanctioned entities need to be aware of the shortcomings of this approach. Some databases rely on methodologies to determine PEP status that differs from the AML/CTF Act's definition. In addition, spelling and translation errors can compromise matching of names and, in some cases, certain PEP categories are not included for screening.

Bullion dealers are strongly encouraged to adopt comprehensive screening practices and are reminded all customers should be subject to PEP and sanctions screening. For further guidance see identifying and assessing the ML/TF risk of PEPs.

INDEPENDENT REVIEWS

Reporting entities must regularly have Part A of their AML/CTF program independently reviewed. An independent review is an impartial assessment of Part A of an AML/CTF program. It checks that a reporting entity is complying with their program and that it:

- properly addresses money laundering and terrorism financing risks
- complies with legal obligations
- is working as it should.

The independent reviewer must be someone who is operationally independent and appropriately suitable. How an independent review is conducted and how often it is conducted depends on the size, nature and complexity of a business or organisation. If a business or organisation has changed significantly or is currently having or previously had difficulties complying, then reviews may need to be completed more often.

EMPLOYEE DUE DILIGENCE AND TRAINING

Appropriate initial and ongoing employee training is critical for all businesses regulated under the AML/CTF Act. Regular refresher training is essential to ensure experienced staff do not become complacent or unaware of emerging ML/TF methodologies, threats and trends.

While criminal misuse of the sector is generally considered an external threat, staff actions may also inadvertently increase ML/TF risks. There are also instances where bullion sector employees are directly targeted to facilitate money laundering (see **Money laundering** on page 16). Ensuring employee probity and integrity is also an important ML/TF risk mitigation strategy. An employee due diligence program documents the procedures used to screen employees to identify and minimise a business or organisation's exposure to ML/TF risk.

TRUSTED INSIDERS – ENABLERS OF CRIME IN AUSTRALIA'S FINANCIAL SYSTEM

The trusted insider is an individual with legitimate or indirect access to a business's privileged information, techniques, technology, assets or premises, and whose access can facilitate harm.

Serious and organised crime groups will continually seek opportunities to exploit trusted insiders across Australia's financial sectors. Criminals may specifically target bullion dealers to facilitate money laundering.

AUSTRAC expects bullion dealers to report any suspicions of professional facilitators or enabling parties to illicit activity, and encourages mature risk mitigation strategies for limiting insider threats.

SUSPICIOUS MATTER REPORTING TO AUSTRAC

It is likely there is under-reporting and non-reporting of suspicious matters across the bullion sector. The sector reports a relatively low number of SMRs, with numbers varying greatly between individual entities of a similar size and scale. Only 23 of the 100 in-scope reporting entities submitted an SMR for the three-year assessment period, with just two reporting entities submitting 73 per cent of the SMRs during this time. The SMRs submitted by the sector generally lack detail. Of the bullion dealers that submitted a compliance report to AUSTRAC in 2020, 71 per cent said their transaction monitoring program did not detect any matters, while 68 per cent said their staff did not report any unusual or suspicious activity.

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

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

AUSTRAC also considers the content of SMR submissions could be improved. For example:

- **Summarising suspicions.** Include a short summary at the top of the grounds for suspicion section of the SMR. This helps AUSTRAC and partner agencies expedite review and assessment of reports.
- **Including a more detailed grounds for suspicion**. This section provides valuable intelligence for AUSTRAC and its partner agencies. Reporting entities are encouraged to explain what aspects of the transaction or customer behaviour was suspicious and include any information from enhanced customer due diligence activities and financial investigations in the grounds for suspicion.

- **Avoiding trigger-based reporting**. Trigger-based reporting occurs when a reporting entity submits a SMR solely on the basis of a trigger generated by their transaction monitoring system without conducting further investigation to form suspicion on reasonable grounds. Similarly, template reporting occurs where there is little unique detail in the grounds for suspicion. Such reports provide little intelligence value.
- **Including documents that provide additional context**. If relevant, include identity verification documents or any other materials which may be available to provide AUSTRAC analysts with a more detailed and complete picture of suspicious transactions.

Reporting entities should have policies and procedures in place to assist staff to identify and report suspicious matters.

FURTHER RESOURCES ON SUSPICIOUS MATTER REPORTING

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

- Frequently asked questions about suspicious matter reporting
- Tips on how to make effective suspicious matter reports to AUSTRAC
- SMR reference guide with real-life examples
- SMR checklist containing key elements and details required

AUSTRAC encourages all bullion dealers to review these resources and consider if their reporting could be improved.

APPENDIX A: GLOSSARY

AML/CTF	Anti-money laundering and counter-terrorism financing.
AML/CTF program	A document that sets out how a reporting entity meets its AML/CTF compliance obligations.
Business email compromise scam	Business email compromise scams are when criminals use email to abuse trust in business processes to scam organisations out of money or goods. Criminals can impersonate business representatives using similar names, domains and/or fraudulent logos as a legitimate organisation or by using compromised email accounts and pretending to be a trusted co-worker.[48]
Customer due diligence (CDD)	Customer due diligence (CDD) is the process where pertinent information of a customer's profile is collected and evaluated for potential ML/TF risks.
Enhanced customer due diligence (ECDD)	Enhanced customer due diligence (ECDD) is the process of undertaking additional customer identification and verification measures in certain circumstances deemed to be high risk.
Financial Action Task Force (FATF)	The Financial Action Task Force (FATF) is an inter-governmental body focused on fighting money laundering, terrorism financing and other related threats to the integrity of the international financial system, by ensuring the effective implementation of legal, regulatory and operational measures.
Inherent risk	Inherent risk represents the amount of risk that exists in the absence of AML/CTF controls implemented by the reporting entity.
Integration	The final stage of the money laundering cycle, in which illicit funds or assets are invested in further criminal activity, 'legitimate' business or used to purchase assets or goods. At this stage, the funds are in the mainstream financial system and appear to be legitimate.
International funds transfer instruction (IFTI)	An international funds transfer instruction (IFTI) involves either: • an instruction that is accepted in Australia for money or property to be made available in another country, or • an instruction that is accepted in another country for money or property to be made available in Australia.
Layering	The second stage of the money laundering cycle, which involves moving, dispersing or disguising illegal funds or assets to conceal their true origin.
ML/TF	Money laundering and terrorism financing.
Mules	Third parties used to transfer illicit funds between locations or accounts.
Politically exposed person (PEP)	A politically exposed person (PEP) is an individual who holds a prominent public position or role in a government body or international organisation, either in Australia or overseas. Immediate family members and close associates of these individuals are also considered PEPs. PEPs often have power over government spending and budgets, procurement processes, development approvals and grants. The AML/CTF Act identifies three types of PEPs: • Domestic PEP – someone who holds a prominent public position or role in an Australian government body. • Foreign PEP – someone who holds a prominent public position or role with a government body in a country other than Australia.

[48] https://www.cyber.gov.au/acsc/view-all-content/publications/protecting-against-business-email-compromise accessed 7 December 2021

	• International organisation PEP – someone who holds a prominent public position or role in an international organisation, such as the United Nations, the World Trade Organisation or the North Atlantic Treaty Organisation.
Placement	The first stage of the money laundering cycle, in which illicit funds first enter the formal financial system.
Ponzi scheme	A ‘Ponzi’ scheme is a scam in which the promoters attract investors to a scheme by promising a very high return on investment, while guaranteeing the security of the investment. The scammers use some of the funds deposited by early investors to pay initial dividend cheques or interest. At this early stage the ponzi scheme only requires a few investors to operate successfully. The promoter continues paying the investors impressive dividends for a couple of months until the investors, encouraged by the early dividends, decide to invest more. The investors may also encourage their friends and relatives to invest. Soon there is a steady flow of funds into the scheme and an ever-growing number of investors. If the promoter is disciplined and retains sufficient funds in the scheme to continue to pay out ‘dividends’, a ponzi scheme can continue for many years.
Predicate offence	For the purpose of this risk assessment, predicate offence is any offence that generates proceeds of crime.
Residual risk	Residual risk is the amount of risk that remains after a reporting entity’s AML/CTF controls are accounted for.
Serious and organised crime group (SOCG)	A group of people who work together for an extended period of time to plan, coordinate and conduct serious crime. Typically, these groups are motivated to commit these serious crimes in order to obtain, directly or indirectly, a financial or other material benefit.
Structuring	Making or receiving a series of cash transactions intentionally structured to be below the $10,000 reporting threshold.
Suspicious matter report (SMR)	A report a reporting entity must submit under AML/CTF Act if they have reasonable grounds to suspect that a transaction may be related to money laundering, terrorism financing, tax evasion, proceeds of crime or any other serious crimes under Australian law. An SMR must also be submitted if the reporting entity has reasonable grounds to suspect the customer or an agent of the customer is not who they say they are.
Threshold transaction report (TTR)	A report that must be submitted to AUSTRAC when a designated service provided to a customer involves a transfer of physical currency of $10,000 or more, or the foreign currency equivalent.
Trade-based money laundering (TBML)	The process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illicit origin.
Trigger-based reporting	A practice in which a reporting entity submits a suspicious matter report to AUSTRAC solely on the basis of a trigger generated by their transaction monitoring system without conducting further investigation.

APPENDIX B: RISK ASSESSMENT METHODOLOGY

The methodology used for this risk assessment follows Financial Action Task Force guidance, which states that ML/TF risk at the national level should be assessed as a function of criminal threat, vulnerability and consequence.

This risk assessment considered 18 risk factors across these three categories and each risk factor was assessed as low, medium or high, as per the table below. These assessments were based on quantitative and qualitative intelligence inputs, including analysis of SMRs and other reporting data, intelligence assessments from partner agencies and feedback from industry. The average scores of the criteria provides the total risk score for each category, and the average of the three risk scores for each category provides the overall risk rating for the sector.

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

VULNERABILITIES		
LOW	**MEDIUM**	**HIGH**
Few higher-risk customers	A moderate number of higher-risk customers	A high number of higher-risk customers
Sector has a small customer base.	Sector has a medium customer base.	Sector has a large customer base.
Provision of product/service rarely involves cash, or involves cash in small amounts	Provision of product/service sometimes involves cash, or involves cash in moderate amounts	Provision of product/service often involves cash, or involves cash in large amounts
Funds and/or value are not easily stored or transferred	Funds and/or value can be stored or transferred with a small amount of difficulty	Funds and/or value are easily stored or transferred
Product/service is provided predominantly through direct contact, with minimal remote services	Mix of direct and remote services	Predominantly remote services, with minimal direct contact
Sector tends to have simple and direct delivery arrangements	Sector tends to utilise some complex delivery arrangements	Sector tends to utilise many complex delivery arrangements
Funds and/or value are generally not transferred internationally	Moderate amount of funds and/or value can be transferred internationally	Significant amounts of funds and/or value are easily transferred internationally
Transactions rarely or never involve higher-risk jurisdictions	Transactions sometimes involve higher-risk jurisdictions	Transactions often involve higher-risk jurisdictions

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

AUSTRAC.GOV.AU