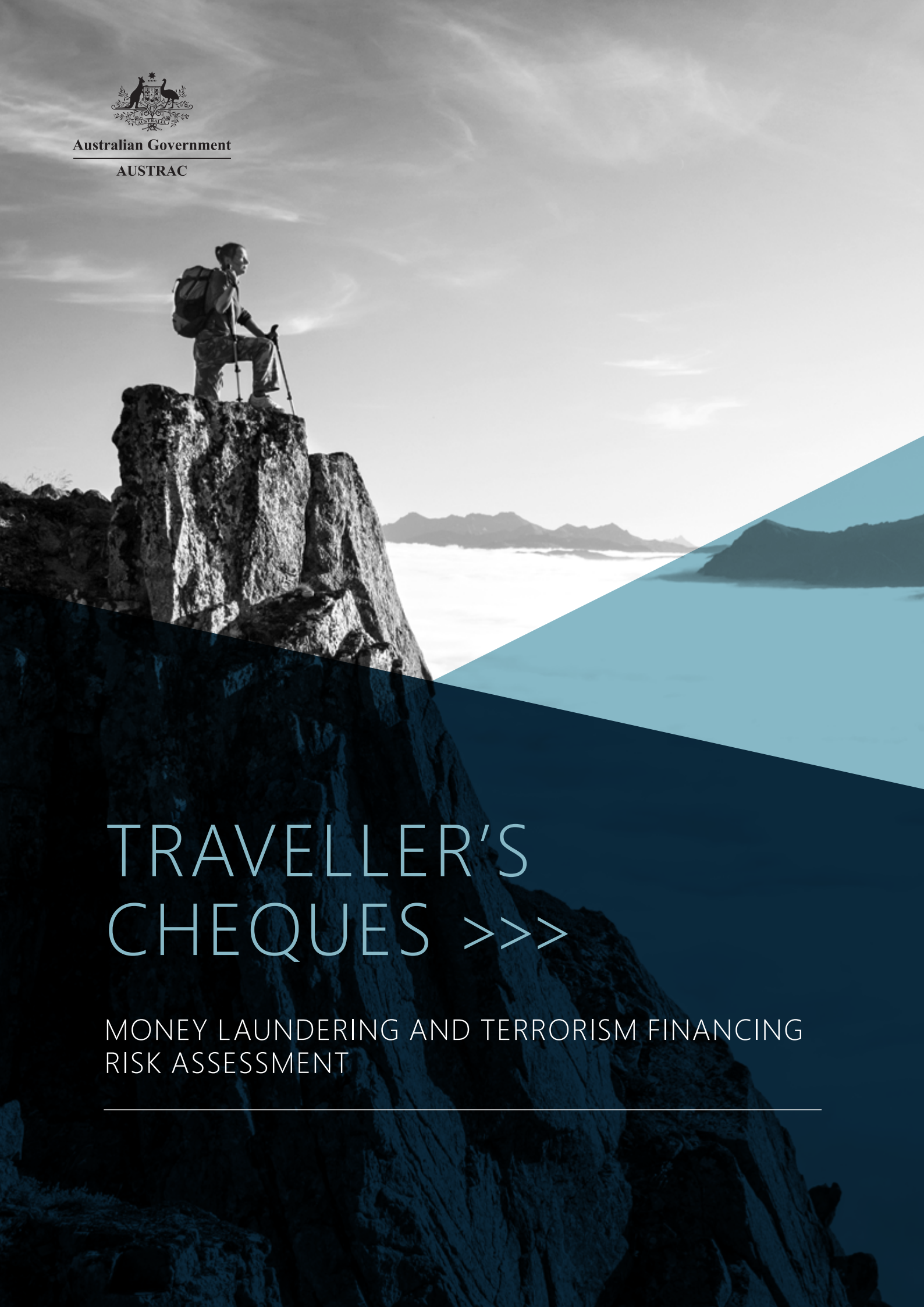


Australian Government

AUSTRAC

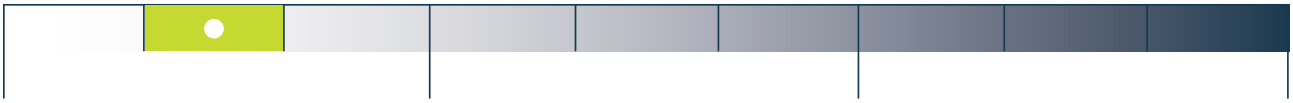
TRAVELLER'S CHEQUES >>>

MONEY LAUNDERING AND TERRORISM FINANCING RISK ASSESSMENT

CONTENTS

KEY ASSESSMENTS

OVERALL RISK RATING



AUSTRAC assesses the overall money laundering/terrorism financing (ML/TF) risk posed by traveller's cheques to be **low**.

There is no recent criminal intelligence relating to traveller's cheques recorded by AUSTRAC's partner agencies. Only 27 suspicious matter reports (SMRs) were submitted to AUSTRAC in relation to traveller's cheques over a two-year period.[1] These SMRs all related to the process of cashing traveller's cheques. The reasons for suspicion in this small SMR dataset were suspected low-level money laundering and traveller's cheque fraud. There were no SMRs in the dataset relating to terrorism financing.

The purchase of traveller's cheques is likely to be vulnerable to ML 'placement' risk, as customers can buy traveller's cheques using cash.[2] The very significant reduction in recent years in the number of outlets in Australia where traveller's cheques can be purchased has limited this risk. There are now only two financial institutions that sell traveller's cheques in Australia.

Entities consulted for this assessment outlined risk management systems and controls that are used to mitigate the vulnerabilities that apply to providing traveller's cheque services.[3] Measures implemented include: only selling to known customers; limiting the total value of traveller's cheques a person can buy in a single day; and adding physical features to traveller's cheques to reduce the risk of counterfeiting.

The risk posed by the use of traveller's cheques is likely to continue to decline, due to the decrease in the availability and use of traveller's cheques in Australia and globally. Consultation with industry indicates that sales of traveller's cheques in Australia have been declining rapidly over recent years, with 2016 sales figures representing a 90 per cent decline on sales from 2012.

The decline in demand for traveller's cheques is likely to be a result of the increased uptake of travel money cards, or stored value cards (SVCs). SVCs have many features that make them a more attractive way of funding travel activity than traveller's cheques. However, they are also highly vulnerable to criminal misuse.

The decline in domestic sales of traveller's cheques is mirrored by a decline in SMRs and threshold transaction reports (TTRs) submitted to AUSTRAC over a similar period. The number of traveller's cheque-related SMRs submitted to AUSTRAC per year has fallen from 61 to just 13 between 2012-13 and 2016-17. Over the same period, TTR submission has fallen from 1,213 to 177 per year.

---

1 1 July 2015 to 30 June 2017.
2 'Placement' is the initial stage of money laundering, where illegitimately obtained funds are introduced into the legitimate financial system.
3 Nine entities involved in the provision of traveller's cheques services were consulted for this risk assessment.

PURPOSE

Recommendation 4.2 in the Report on the Statutory Review of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and Associated Rules and Regulations requires AUSTRAC to assess the ML/TF risks posed by traveller's cheques in Australia. This ML/TF risk assessment responds to that recommendation.

This report considered 26 factors across three categories of risk: criminal threat environment, vulnerability and consequences. An average risk rating was determined for each category, and these averages were used to determine an overall risk rating.

Assessments are based on reports and intelligence from: a variety of partner agencies; feedback and professional insights by industry stakeholders; and analysis of transaction reports submitted to AUSTRAC, including SMRs and TTRs.

See the Appendix for further information on the methodology.

This report forms part of AUSTRAC's ML/TF risk assessments program. Publications to date are available on the AUSTRAC website.

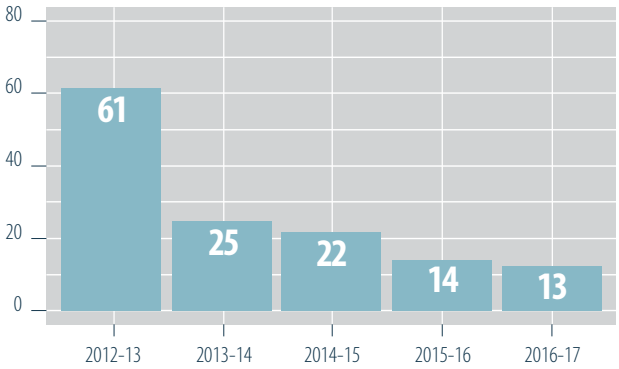
FEEDBACK

AUSTRAC is committed to continual improvement and values your feedback on its products. We would appreciate notification of any outcomes associated with this report by contacting AUSTRAC via riskassessments@austrac.gov.au.

CRIMINAL THREAT ENVIRONMENT

AUSTRAC assesses that there is a low level of criminality associated with the use of traveller's cheques in Australia. There is no recent criminal intelligence relating to traveller's cheques recorded by AUSTRAC's partner agencies, and very few SMRs have been submitted to AUSTRAC indicating suspected criminality. As the chart below shows, the number of SMRs submitted to AUSTRAC in relation to traveller's cheques has been declining year-on-year since 2012.

SMRS RELATING TO TRAVELLER'S CHEQUES BY FINANCIAL YEAR



Twenty-seven SMRs relating to traveller's cheques were submitted to AUSTRAC from 1 July 2015 to 30 June 2017 and were studied in detail for this assessment.

SMR SUMMARY

- 20 SMRs related to suspected money laundering and seven to suspected fraud
- None of the SMRs submitted during the sample period related to suspected terrorism financing
- Eight reporting entities submitted at least one SMR
- The total value of the SMRs was $685,016 [4]
- The average value of the SMRs was $27,401
- Two SMRs related to amounts of less than $1,000
- All SMRs related to the process of cashing traveller's cheques

MONEY LAUNDERING

Twenty of the SMRs submitted during the sample period related to suspected money laundering. These SMRs fell into two categories:

1. Entities that identified potential money laundering while processing cash-out requests (eight SMRs), with indicators including:
   - customers cashing multiple traveller's cheques for individual amounts of less than $10,000 in an apparent attempt to avoid TTR obligations (and then depositing the cash into personal bank accounts)
   - customers using traveller's cheques in a manner inconsistent with the purpose of traveller's cheques—for example for property investment, cashing traveller's cheques and then immediately transferring the value offshore or into an account, or transacting in unexpectedly large amounts
   - customers using traveller's cheques in a manner inconsistent with their claimed income
   - customers cashing numerous traveller's cheques in a single day or in large batches over a short period
   - customers refusing to show identification or disclose their source of funds
2. Entities that had identified potential money laundering when processing the settlement of traveller's cheques that had been cashed by a foreign correspondent bank (12 SMRs)—these SMRs fell into two categories:
   - a large number of traveller's cheques being cashed offshore in a single day or in large batches over a short period (inconsistent with the purpose of traveller's cheques)
   - all or most of the traveller's cheques being sequentially numbered, indicating they were cashed in a single transaction in order to move large amounts of money across borders.

4 Two SMRs did not specify a value.

UNUSUAL USE OF TRAVELLER'S CHEQUES IS NOT ALWAYS ILLEGITIMATE

Entities described a number of lawful, non-tourism related reasons customers may purchase traveller's cheques.
For example, entities consulted for this assessment are aware that some customers use traveller's cheques to:

- speculate in foreign currency movements
- facilitate the currency exchange and movement of funds overseas (particularly for financially excluded individuals migrating to another country)
- purchase large items from an overseas vendor

While AUSTRAC encourages entities to be alert to unusual patterns of use in relation to traveller's cheques, conducting enhanced customer due diligence may help inform the decision as to whether lodgement of an SMR is required

SCAMS INVOLVING TRAVELLER'S CHEQUE FRAUD

One SMR detailed a series of scams involving traveller's cheques, being carried out against several people.

A foreign currency services provider reported that two customers came to the branch in the space of a week to exchange several traveller's cheques (all in USD500 denominations). However, the traveller's cheques were all identified as fraudulent.

The two customers had come in on different days, and both said they had applied for a job online and were told they were being paid in advance with the traveller's cheques, which they had received in the mail. A third customer came to the branch, also trying to cash counterfeit USD traveller's cheques. This customer said they had received the traveller's cheques in the mail from someone who owed them money.

The reporting entity noted that all of the customers appeared to be surprised when they were told the cheques were counterfeit.

FRAUD

Seven of the SMRs submitted during the sample period related to suspected cases of traveller's cheque fraud. Again, suspicion was always raised at the time of cashing the traveller's cheques, and described three main scenarios:

- customers attempting to cash traveller's cheques that were identified by the reporting entity as being counterfeit (for example, because of the unusual appearance of the traveller's cheque or failed authorisation from the issuer)
- customers attempting to cash traveller's cheques that had been tampered with (for example, by chemically removing the original signature from the traveller's cheque and then signing over it)
- customers attempting to cash counterfeit traveller's cheques that they received from someone they met over the internet

While AUSTRAC information indicates that improved security features applying to traveller's cheques have led to a decline in the number of counterfeit traveller's cheques in circulation, partner agency feedback indicates that this threat has not been eliminated entirely.

VULNERABILITIES

AUSTRAC assesses that there is a **low** level of ML/TF vulnerability associated with traveller's cheques. Vulnerability refers to the characteristics of traveller's cheques and their use that make them attractive for ML/TF purposes.

CUSTOMERS

AUSTRAC considers the ML/TF vulnerability presented by the customers of traveller's cheques to be low.

This is because traveller's cheques can only be issued or sold to individual customers—they cannot be made out to agents of customers, or non-individuals such as companies and trusts. In addition, consultation with industry indicates there is very limited use of traveller's cheques by politically exposed persons.[5]

The size of the customer base for traveller's cheques in Australia is very small and declining. The value of traveller's cheque sales in 2016 amounted to approximately 10 per cent of the value of sales in 2012.

Entities consulted for this risk assessment generally attributed the reduction in demand for traveller's cheques to a shift in consumer preference towards travel money cards, due to their superior functionality. The movement away from traveller's cheques towards travel cards is expected to continue.

SOURCE OF FUNDS AND WEALTH

AUSTRAC assesses that difficulty in assessing the source of funds used to purchase traveller's cheques represents a medium vulnerability.

Entities that sell or cash traveller's cheques for customers with whom they do not have a pre-existing relationship, reported difficulties in establishing the source of the funds that were used to buy the traveller's cheques. One entity advised AUSTRAC that they only sold traveller's cheques to customers with whom they had a pre-existing relationship, and no longer held traveller's cheques onsite to service 'walk-in' customers.

Sixteen of the 27 SMRs submitted to AUSTRAC over the sample period noted that the suspect transaction was inconsistent with the customer's profile, or that the source of the customer's funds was unknown.

PRODUCT FEATURES

AUSTRAC assesses that the features of traveller's cheques pose a low level of ML/TF vulnerability. Like cash, traveller's cheques need to be physically moved for the value on them to be transferred.

However, traveller's cheques can often be more easily obtained in larger denominations than cash, making transport and storage comparatively easier. Further, traveller's cheques are cashed without a clearance period and do not expire, increasing their liquidity when compared to many account-based cheques.

Serial numbers provide a degree of security in relation to lost or stolen traveller's cheques. The traveller's cheques that are sold in Australia are also protected from forgery by several physical security features such as magnetic ink, watermarks and metal threads.

A key protection for traveller's cheques is the requirement that customers be identified and sign the traveller's cheques being bought. The effectiveness of this control is limited, however, due to the availability of false identification and the ease with which signatures can be forged.

---

5 Politically exposed persons, or PEPs, are individuals who occupy a prominent public position or function in a government body or international organisation, both within and outside Australia. This definition also extends to their immediate family members and close associates

NEW TECHNOLOGY CONTRIBUTING TO TRAVELLER'S CHEQUES' DECLINE

In 2017 AUSTRAC published its risk assessment on SVCs. While the features of individuals SVC products vary significantly, many SVCs provide customers with functionality far in advance of that which can be offered by paper-based products like traveller's cheques.

Many travel SVCs operate almost exactly like debit cards, the key difference being that the funds are not held in the customer's bank account. These cards will be accepted anywhere around the world where debit cards are accepted, including ATMs, and they also facilitate remote reloads (including in cash). The technology that travellers now have access to through SVCs improves the experience for legitimate travellers, but also increases the ML/TF risk associated with the products.

DELIVERY CHANNEL

AUSTRAC assesses that the delivery channels used to provide traveller's cheque services represent a low level of ML/TF vulnerability. The number of physical retailers in Australia that sell traveller's cheques has been declining in recent years, corresponding with the overall decline in traveller's cheques' popularity. Prominent traveller's cheque retailers have exited the market, reducing the number of active sellers in the Australian market to just two, albeit large organisations.

Traveller's cheques can be purchased both online and face-to-face. The higher ML/TF vulnerability that is commonly associated with online delivery services is partly mitigated for traveller's cheques because face-to-face contact with the customer still occurs when they pick up their traveller's cheques at an outlet.

The value of this face-to-face contact is demonstrated by several SMRs in the dataset that rely at least partly on staff members' observations of unusual customer behaviour.

FOREIGN JURISDICTION

AUSTRAC assesses that traveller's cheques are highly vulnerable to foreign jurisdiction risk. The purpose of traveller's cheques is to move value across borders, so they carry an intrinsic vulnerability to being misused by persons moving the proceeds of crime either into or out of Australia.

The traveller's cheques sold in Australia can be cashed in more than 100 countries and at tens of thousands of outlets worldwide. This gives them a relatively high potential exposure to foreign jurisdictions. However, this vulnerability is somewhat tempered by the dramatic and sustained decrease in the overall value of traveller's cheques purchased in Australia for offshore use.

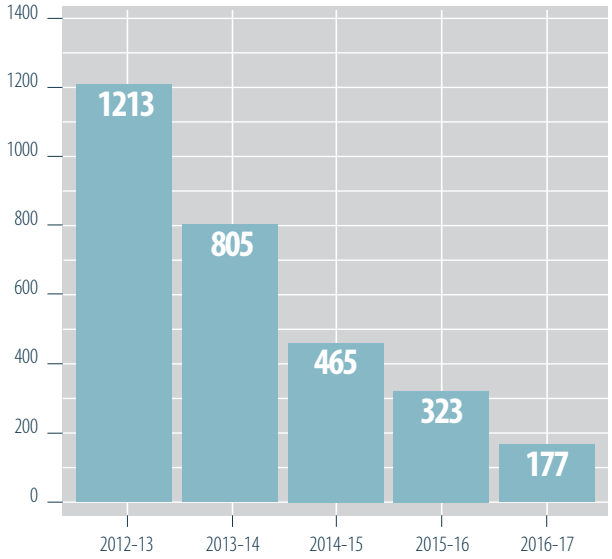
Traveller's cheques are also purchased offshore and cashed in Australia. The value of foreign purchased traveller's cheques that are cashed Australia is not known, but is likely to be small and diminishing, in line with the global decrease in the use of traveller's cheques.

USE OF CASH

AUSTRAC assesses that the use of cash in buying and cashing traveller's cheques represents a low level of ML/TF vulnerability. Like SMRs, the number of TTRs relating to traveller's cheques has been declining significantly year-on-year, in line with the overall decline in the availability and use of traveller's cheques.

The following chart captures TTRs relating to both the selling and cashing of traveller's cheques over the last five financial years.

TTRS RELATING TO TRAVELLER'S CHEQUES BY FINANCIAL YEAR



AUSTRAC analysed the 500 traveller's cheque-related TTRs that were submitted by 14 reporting entities over a two-year sample period.[6] While these TTRs cumulatively amounted to $23.6 million, the component of the transactions that related to traveller's cheques totalled only $4.1 million.[7] This constitutes a relatively low exposure to large cash transactions when compared to other products regulated by AUSTRAC. Further, only six SMRs submitted over the two-year sample period related to transactions that involved cash.

The issuer of the traveller's cheques that are sold in Australia limits the total value of traveller's cheques that can be sold to an individual in one day. This control limits the amount of cash that can be used to purchase traveller's cheques.

AML/CTF SYSTEMS AND CONTROLS

AUSTRAC assesses that the AML/CTF systems and controls implemented by the providers of traveller's cheque services represent a low level of ML/TF vulnerability.

Traveller's cheques are subject to broad coverage across the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and the Financial Transaction Reports Act 1988.

Reporting entities are exempt from carrying out the applicable customer identification procedures for traveller's cheque transactions of less than AUD1,000 (unless their enhanced customer due diligence program requires customer identification to occur). This exemption is considered appropriate due to the demonstrated low ML/TF risk of traveller's cheque transactions.

Entities that were consulted for this risk assessment demonstrated a high level of understanding of the threats and vulnerabilities associated with traveller's cheques. They described a variety of mitigation strategies and controls that they have in place to address these issues, including:

- only selling traveller's cheques to customers who already have an account
- ensuring robust customer identification and verification processes are followed when selling and cashing traveller's cheques
- restricting the cashing of traveller's cheques from certain high-risk jurisdictions
- requiring additional due diligence be undertaken in relation to transactions above a certain value
- limiting the cumulative value of traveller's cheques that can be sold to an individual in one day
- limiting the cumulative value of sequentially numbered traveller's cheques that can be cashed
- providing authorisation mechanisms to protect against fraud.

OPERATIONAL VULNERABILITIES

Given that traveller's cheques are used across jurisdictions, it is rare that the entity that cashes a traveller's cheque is the same as the entity that sold the traveller's cheque.

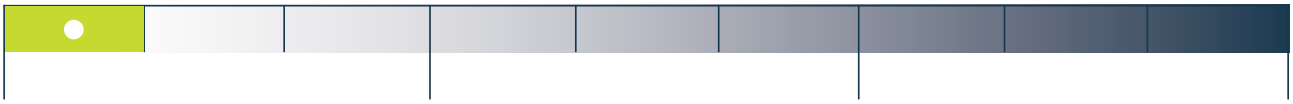
This makes it difficult for a single entity to have end-to-end oversight of how the traveller's cheques they sell are used. Therefore, AUSTRAC considers that the operational characteristics of traveller's cheque service provision represent a medium level of ML/TF vulnerability.

---

6 1 July 2015 to 30 June 2017. All reporting entities must submit a TTR for individual transactions involving physical currency or e-currency valued at AUD10,000 (or foreign equivalent) or higher.

7 Other component transactions included in these TTRs related to AUD and foreign currency cash being provided to/received from the reporting entity by the customer.

CONSEQUENCES



AUSTRAC has assessed the consequences of ML/TF activity facilitated by traveller's cheques to be minor. Consequence refers to the impact or harm that ML/TF activity may cause.

This assessment is largely due to the very limited known criminal misuse of traveller's cheques, and that the overall use of traveller's cheques in Australia is low and declining. There were also no instances of terrorism financing observed that involved traveller's cheques, over a two year period to 30 June 2017.

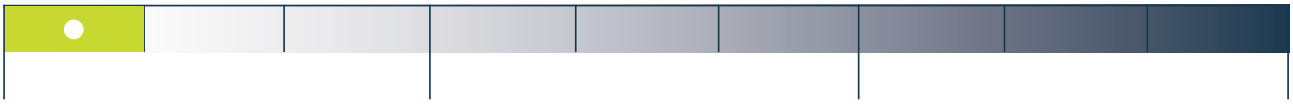
While some individuals and businesses may suffer loss due to traveller's cheque fraud, the criminal misuse of traveller's cheques is unlikely to have consequences for the Australian economy as a whole, or national and international security.

APPENDIX: 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.

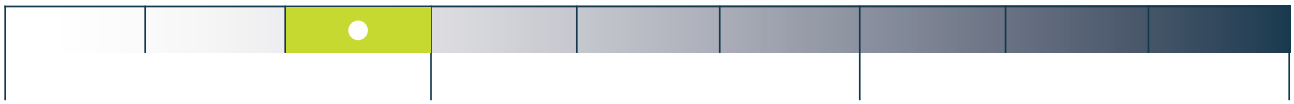
This risk assessment considered 26 risk factors across the above three categories. Each risk factor was assessed as low, medium or high, as per the table below. An average risk rating was determined for each category, and these averages were used to determine an overall risk rating.

CRIMINAL THREAT ENVIRONMENT



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

VULNERABILITIES



LOW MEDIUM HIGH

CUSTOMERS		
Simple customer types, mostly individuals	Mixture of customer types, with some complex companies and trusts	All customer types represented, including large numbers of highly complex companies and trusts
Minimal involvement of agents acting for customers	Moderate involvement of agents acting for customers	Significant involvement of agents acting for customers
Small customer base	Medium-sized customer base	Very large customer base
Very few politically exposed persons	Some politically exposed persons	Many politically exposed persons

SOURCE OF FUNDS AND WEALTH		
Source of funds/wealth can be readily established	Some difficulty in establishing the source of funds/wealth	Source of funds/wealth difficult to establish

PRODUCTS AND SERVICES		
Product/service does not allow a customer to remain anonymous (ownership is transparent)	Product/service allows a customer to retain some anonymity (ownership can be obscured)	Product/service allows a customer to remain anonymous (ownership is opaque)
Small volume of transactions	Moderate volume of transactions	Large volume of transactions
Movement of funds cannot occur easily and/or quickly	Movement of funds can occur relatively easily and/or quickly	Movement of funds is easy and/or quick
Transfer of ownership of product cannot occur easily and/or quickly	Transfer of ownership of product can occur relatively easily and/or quickly	Transfer of ownership of product is easy and/or quick

DELIVERY CHANNEL		
Regular face-to-face contact, with minimal online/telephone services	Mix of face-to-face and online/telephone services	Predominantly online/telephone services, with minimal face-to-face contact

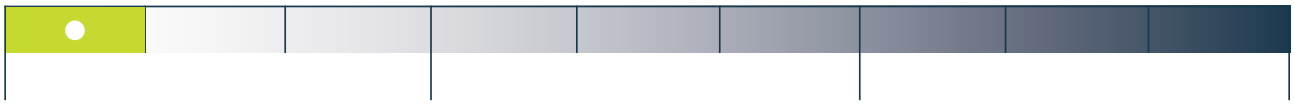
FOREIGN JURISDICTION		
Very few or no overseas-based customers	Some overseas-based customers	Many overseas-based customers
Transactions rarely or never involve foreign jurisdictions	Transactions sometimes involve foreign jurisdictions, or a high-risk jurisdiction	Transactions often involve foreign jurisdictions, or high-risk jurisdictions

USE OF CASH		
Provision of product/service rarely involves cash, or involves cash in small amounts	Provision of product/service often involves cash, or involves cash in moderate amounts	Provision of product/service usually involves cash, or involves cash in very large amounts

OPERATIONAL VULNERABILITIES		
There are very few operational factors that make the sector susceptible to criminal activity	There are some operational factors that make the sector susceptible to criminal activity	There are many operational factors that make the sector susceptible to criminal activity

AML/CTF SYSTEMS AND CONTROLS		
Sector is subject to all or most AML/CTF obligations	Sector is subject to partial AML/CTF obligations	Sector is not subject to AML/CTF obligations
At a sector level, significant systems and controls have been implemented to mitigate against criminal threats	At a sector level, moderate systems and controls have been implemented to mitigate against criminal threats	At a sector level, limited systems and controls have been implemented to mitigate against criminal threats

CONSEQUENCES



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

www.**austrac**.gov.au

JUNE 2018