Australian Government
AUSTRAC

STORED VALUE CARDS >>>

MONEY LAUNDERING AND TERRORISM FINANCING RISK ASSESSMENT

KEY STATISTICS ON STORED VALUE CARDS (SVCs)

FROM 1 SEPTEMBER 2015 TO 31 AUGUST 2016

The information below was obtained through an industry survey conducted by AUSTRAC. The survey was issued in September 2016 and asked SVC issuers various questions in relation to the number, features and usage of the SVCs they issued as at 31 August 2016.

11
survey respondents

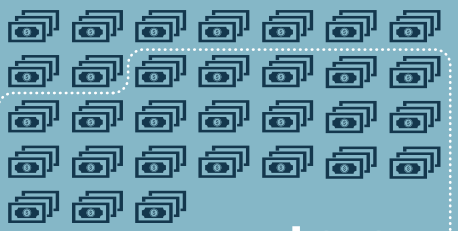
>$5.1 billion
loaded onto these SVCs

>$835.5 million
loaded in cash

10 million
active SVCs

$1.5 billion
stored

>$3.1 billion
redeemed



>$981.5 million
redeemed offshore in cash

>$2.2 billion
redeemed offshore

= $100 million

33 of these SVC products are **above** the threshold SVCs*

They represent:

- **35%** of active cards
- **50%** of funds stored on SVCs
- **90%** of the amount loaded onto SVCs
- **87%** of funds redeemed from SVCs
- **98%** of funds redeemed offshore

of these SVC products are **below** the threshold SVCs* **46**

They represent:

- **65%** of active cards
- **50%** of funds stored on SVCs
- **10%** of the amount loaded onto SVCs
- **13%** of funds redeemed from SVCs
- **2%** of funds redeemed offshore

* For the purpose of regulation under the AML/CTF Act 2006

Note: The statistics do not represent the complete figures for SVCs in Australia and should only be taken as a minimum representation of the size of the market. For more information about survey data please refer to the Methodologies section below.

CONTENTS

KEY TERMS 03

EXECUTIVE SUMMARY 04

PURPOSE 06

METHODOLOGY 06

REPORTING TO AUSTRAC 07

CRIMINAL THREAT ENVIRONMENT 08

- Money laundering 08
- Terrorism financing 10
- Cyber-enabled fraud 12
- Other fraud 12
- Scams 12
- Tax evasion 13
- Other indicators of suspicion 13

VULNERABILITIES 14

- Product features 14
- Customers 16
- Source of funds and wealth 17
- Delivery channel 17
- Foreign jurisdiction 18
- Use of cash 19
- Operational vulnerabilities 19
- AML/CTF systems and controls 21
- Vulnerability mitigation 23

CONSEQUENCES 24

APPENDIX: Risk assessment methodology 26

KEY TERMS

Term	Description
Above the threshold SVC	An SVC that carries AML/CTF obligations. The applicable thresholds are: • if the card can hold $1,000 or more at any one time and cash can be withdrawn from the card, or • if the card can hold $5,000 or more at any one time and cash cannot be withdrawn from the card.
Below the threshold SVC	An SVC that is not regulated under the AML/CTF Act because it does not meet the relevant thresholds, as set out above.
Closed loop SVCs	SVCs that can only be redeemed at specific retailers (for example, gift cards). Cash cannot be withdrawn from closed loop SVCs.
Grounds for suspicion (GFS)	The free text field in the SMR form which allows the reporting entity to provide a description about the suspicious matter.
Open loop SVCs	SVCs that operate on the Visa, MasterCard or EFTPOS networks. Cash can usually be withdrawn from open loop SVCs.
Point of Sale (POS)	Electronic transaction facilitator at physical retailers.
Stored value card (SVC)	For the purposes of section 6 of the AML/CTF Act. Often referred to as 'prepaid card'.
Suspicious matter reports (SMRs)	Reports submitted to AUSTRAC in relation to suspicious transactions under section 41 of the AML/CTF Act.
Threshold transaction reports (TTRs)	Reports submitted to AUSTRAC in relation to transactions conducted with cash amounts of $10,000 or more, under section 43 of the AML/CTF Act.

EXECUTIVE SUMMARY

This risk assessment separately analyses above and below the threshold SVCs. This is due to the difference in the regulatory statuses of these card-types, as well as the absence of transactional report data submitted to AUSTRAC in relation to below the threshold cards. While the absence of reporting data means that AUSTRAC has only applied risk ratings to above the threshold SVCs, there is extensive qualitative analysis of the risks relating to below the threshold SVCs using other sources throughout this assessment.

OVERALL RISK RATING

AUSTRAC assesses the overall money laundering/terrorism financing (ML/TF) risk posed by the use of above the threshold SVCs to be **MEDIUM**. This rating is based on an assessment of the criminal threat environment and vulnerabilities associated with above the threshold SVCs, as well as the associated consequences of their misuse.

CRIMINAL THREAT ENVIRONMENT

Based on analysis of the nature and extent of observed criminal activity relating to above the threshold SVCs, AUSTRAC assesses the criminal threat environment to be **MEDIUM**.

SVCs are used to support a wide variety of criminal activities perpetrated by individuals as well as serious and organised crime groups.

AUSTRAC analysed in detail two years of SMRs submitted in relation to SVCs.[1] The most frequently reported offence indicated in the SMR dataset was money laundering. Various money laundering typologies were observed in relation to above the threshold SVCs, notably loading large volumes of cash and movement of large volumes of funds offshore. Proceeds of crime also appear to have been used to bulk purchase below the threshold SVCs in an attempt to launder funds.

SVCs have been used to support terrorism financing. Criminal intelligence and analysis of SMRs revealed that SVCs have been used by foreign terrorist fighters before and after departure from Australia. Twelve SVC-related terrorism financing SMRs were submitted to AUSTRAC during the sample period; all related to above the threshold SVCs being redeemed in countries that border Syria.

Below the threshold SVCs that can be redeemed offshore are also highly vulnerable to exploitation by terrorism financiers, who may seek to use them as anonymous vehicles for moving the smaller sums of money that are associated with terrorism financing.

AUSTRAC assesses that the use of SVCs to finance terrorism may increase, particularly if displacement from other international remittance channels continues to grow.

Suspected cyber-enabled fraud is also particularly prevalent in relation to SVCs, and represents the second-largest category of SMRs in the sample period. Many SMRs in the dataset describe cybercriminals transferring funds from victims' bank accounts onto above the threshold SVCs, then redeeming the stolen funds from the SVCs (generally in cash). Below the threshold SVCs may be less likely to be used for cyber-enabled fraud due to the lower storage thresholds.

1 1 April 2014-31 March 2016

Other suspicious behaviour associated with above the threshold SVCs included:

- scam activity (primarily suspected romance scams), in which scammers use SVCs to receive and access funds deceptively obtained from victims
- tax evasion, in which customers receive wages or payments onto SVCs in apparent attempts to avoid tax obligations
- offshore redemption of SVCs where an unknown third party is loading or redeeming funds.

VULNERABILITIES

AUSTRAC assesses that SVCs carry a **HIGH** level of vulnerability to ML/TF.

The features of individual SVC products in the Australian market vary significantly, which means that the vulnerabilities associated with different products also varies significantly. As widely observed, the risk of 'open loop' SVCs is generally higher than that of 'closed loop' SVCs. However, in this risk assessment, AUSTRAC has moved beyond the simple open loop/closed loop comparison to assess risk. Instead, this assessment highlights several additional product features that significantly influence an SVC's vulnerability to misuse, all of which require attention when considering a product's risk.

The key features that make an SVC product particularly vulnerable to financial crimes are:

- reloadability
- ability to use cash to load/reload the SVC
- ability to redeem SVC value in cash
- ability to redeem at a wide range of merchants ('acceptability')
- ability to redeem internationally
- high storage limits.

The more of these features that apply to a single SVC, the higher the product's vulnerability to criminal misuse. Many of these vulnerabilities can apply to both above and below the threshold cards.

Other vulnerabilities that apply to above the threshold SVCs include:

- ability to be reloaded/redeemed by unidentified third parties (particularly where secondary cards are available)
- difficulty in establishing the source of funds used to load/reload SVCs
- significant use of online delivery services
- operational vulnerabilities associated with reporting entities outsourcing AML/CTF obligations to multiple third-party entities
- use as an alternative international remittance vehicle
- limited visibility by AUSTRAC over SVCs being moved across the border, due to not being subject to reporting as bearer negotiable instruments.

Vulnerabilities associated specifically with below the threshold SVCs include:

- the anonymity of all customers – no customer identification is required for below the threshold SVCs
- the large size of the customer base
- the absence of AML/CTF obligations, including being frequently issued by entities that are not regulated under the AML/CTF Act.

CONSEQUENCES

AUSTRAC assesses the consequences associated with the misuse of above the threshold SVCs to be **MODERATE**.

The most significant potential consequence is the threat to national and international security if used to facilitate terrorism financing, particularly in sustaining and enabling the activities of Australian foreign terrorist fighters.

Consequences for SVC issuers include reputational damage, financial losses, and potential loss of consumer confidence in SVCs as a safe financial product.

Although the use of SVCs to facilitate criminal activity has the potential to harm the broader Australian economy and community, the overall impact on the Australian economy is unlikely to be very significant given SVCs represent a relatively small proportion of financial products available to customers.

There may also be consequences for individuals, including financial loss and emotional distress.

PURPOSE

The purpose of this risk assessment is to provide information to SVC issuers and their agents on the ML/TF risks of SVCs at the national level. It also responds to Recommendation 4.3 of the statutory review of the AML/CTF Act for AUSTRAC to conduct an assessment of the ML/TF risk posed by SVCs.

The risk ratings in this assessment apply only to above the threshold SVCs, because almost all of the SMRs submitted to AUSTRAC in relation to SVCs relate to above the threshold cards. Other sources of intelligence have been drawn upon to inform the qualitative assessments on below the threshold SVCs throughout this assessment.

AUSTRAC expects that SVC issuers will use this assessment to refine their own risk assessments and compliance controls, including transaction monitoring and oversight of any agents that discharge AML/CTF obligations on an SVC issuer's behalf. It also aims to assist SVC issuers and their agents to identify cases of suspicious use of SVCs, and to submit SMRs to AUSTRAC.

Reporting entities should apply information in this assessment in a way that is consistent with the nature, size and complexity of their businesses, as well as the ML/TF risk posed by their SVCs, customers and delivery channels, and the foreign jurisdictions in which their SVCs can be redeemed.

Future AUSTRAC compliance activities will assess how reporting entities in the sector have responded to the information provided in this assessment.

METHODOLOGY

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

- **Criminal threat environment** refers to the extent and nature of observed ML/TF and other offences associated with the exploitation of above the threshold SVCs.
- **Vulnerability** refers to the characteristics of above the threshold SVCs that make them attractive for ML/TF purposes. This includes features of a particular SVC that can be exploited, as well as the relevant customer types, delivery channels and foreign jurisdictions in which it can be used. Vulnerability is also influenced by the level of AML/CTF systems and controls in place across the sector that provides the product.
- **Consequence** refers to the impact or harm that ML/TF activity may cause.

In relation to above the threshold SVCs, this assessment considered 25 risk factors across the above three categories. An average risk rating was determined for each category, and these averages were used to determine an overall risk rating. Further information on the methodology is in the Appendix.

Four main intelligence inputs informed the risk ratings in this assessment:

- analysis of SVC-related SMRs, as well as other AUSTRAC information and intelligence
- reports and intelligence from a variety of domestic and international partner agencies, including intelligence, regulatory and law enforcement agencies
- feedback and professional insights offered during interviews and consultation with a range of SVC issuers, transaction processors, payment network providers and industry experts
- information on SVC features and usage provided by 11 SVC issuers in response to a national survey conducted by AUSTRAC.

  Some reporting entities were not able to provide complete data for some questions in the survey, and one large reporting entity did not respond to the survey. As the majority of entities that issue gift cards have no anti-money laundering and counter-terrorism financing (AML/CTF) obligations and were not sent the survey, gift card data is not comprehensively captured by survey responses.

REPORTING TO AUSTRAC

Under the AML/CTF Act, entities that issue above the threshold SVCs and/or increase the value stored in connection with above the threshold SVCs have an obligation to submit SMRs and TTRs to AUSTRAC.[2] A reporting entity must submit an SMR if it forms a reasonable suspicion of money laundering, terrorism financing or any other offence such as fraud or tax evasion.

SMRs submitted in relation to SVCs provide valuable intelligence to AUSTRAC. Working with partner agencies, AUSTRAC pieces together intelligence from a range of sources to develop a picture of criminal activities and networks. Many of AUSTRAC's partner agencies – including the Australian Federal Police, Australian Criminal Intelligence Commission, Australian Taxation Office (ATO) and Department of Immigration and Border Protection – have access to AUSTRAC SMRs to conduct further analysis and investigation.

Reporting entities also lodge SMRs in response to enquiries made by AUSTRAC's partner agencies in relation to particular activities or customers.

For this risk assessment, AUSTRAC analysed in detail two years of SMRs submitted in relation to SVCs.

SMRs RELATING TO SVCs

916 Number of SMRs submitted

$72.3M Total value of SMRs

17 Number of reporting entities submitting at least 1 SMR

3 Number of reporting entities accounting for **80%** of all SMRs submitted

1 April 2014 to 31 March 2016

It is highly likely that the above total value figure significantly understates the actual value of suspicious activity reported in the sample period, as 62 SMRs in the sample period did not state a value. Moreover, AUSTRAC observed that the value of the transactions provided in SMRs varied depending on how reporting entities interpreted the 'amount' field on the SMR form. Some reporting entities use the 'amount' field to capture only one of the transactions in a sequence of transactions that were *cumulatively* deemed suspicious. For example, one SMR related to a series of SVC withdrawals from an ATM. The amount reported in the SMR reflected just one of these ATM withdrawals – not the total amount that was withdrawn from the SVC over the whole period discussed in the GFS. The overall amount withdrawn from the SVC was around 40 times higher than the amount reported in the amount field.

2 Other reporting obligations also apply, such as the annual AML/CTF compliance report.

CRIMINAL THREAT ENVIRONMENT

The criminal threat environment refers to the extent and nature of the ML/TF and other crimes that are associated with SVC use. AUSTRAC assesses this as a **MEDIUM** threat for above the threshold SVCs.

Reporting entities reported a wide variety of suspicious activity[3] in their SVC-related SMRs during the two-year sample period. As shown in the chart below, AUSTRAC divided the likely offences described in these SMRs into several categories. The most prevalent likely offences were money laundering and cyber-enabled fraud, followed by other types of fraud, scams and tax evasion.

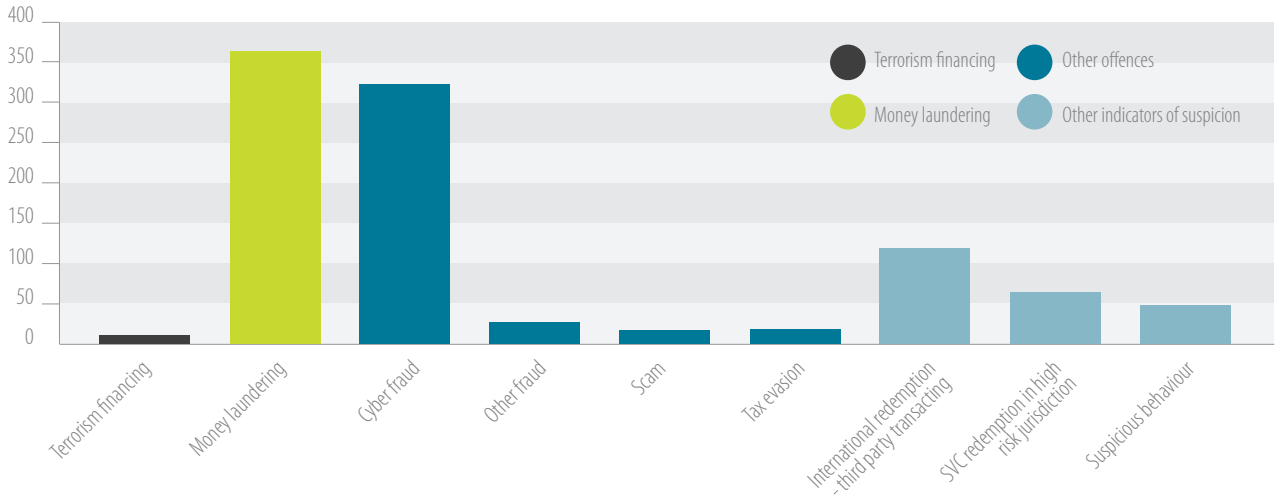
AUSTRAC assessed 12 SMRs in the SVC dataset to be highly likely to relate to terrorism financing.

In 16 per cent of SVC SMRs, the likely offence was not clear. The reasons for suspicion in these SMRs included: third party use of SVCs that were redeemed offshore; redemption of SVC value in high-risk jurisdictions; and/or suspicious behaviour exhibited by SVC customers.

MONEY LAUNDERING

AUSTRAC SMR data indicates that criminals are using above the threshold SVCs to launder and move the proceeds of crime. Reporting entities submitted 366 SMRs indicative of money laundering during the sample period, representing 40 per cent of the total number of reports.

Reporting entities often detected suspected money laundering by observing SVCs being used in a manner inconsistent with the purpose of the product being used.



The figures above total more than 916 because several SMRs contained more than one cause for concern.

3 This analysis is based on suspicions of illicit activity, as analysed by AUSTRAC in SMRs. It does not reflect criminal convictions. However, the activity demonstrates the types of behaviours that entities should be aware of as possibly indicating SVC misuse.

The following indicators of money laundering activity prompted reporting entities to submit SMRs:

- loading, reloading and redeeming SVCs in a manner inconsistent with the purpose of the product; for example, loading substantially more money onto a travel card than could be reasonably required to sustain tourist activity
- loading value onto an SVC then immediately redeeming the value in cash, including:
  - loading funds onto an SVC in Australia, then a likely third party immediately redeeming them offshore in cash
  - loading funds onto an SVC then immediately redeeming them in cash in close proximity to the load location
- systematically using maximum load/redemption amounts, particularly daily maximum ATM withdrawal limits (as determined either by the SVC or the ATM)
- redeeming value on an SVC only in cash, where the purpose of the card is also to purchase goods and services
- loading a specific currency onto a travel card, then converting it into another currency and then back into the original currency, attracting currency conversion fees for no ultimate purpose
- using international travel cards domestically, when the particular travel card attracts high fees when used domestically[4]
- loading and/or reloading unusually large volumes of cash onto SVCs where the origin of the funds was unknown
- loading and reloading large volumes onto SVCs in a manner inconsistent with the customer's profile/claimed source of funds
- making large cash deposits onto SVCs, then transferring the value to a personal account and withdrawing in cash
- making large cash deposits into a personal account, then transferring the value onto an SVC and redeeming in cash
- structuring loads and/or reloads of cash into amounts of less than $10,000, possibly to avoid TTR obligations
- purchasing/transacting on several SVCs at once
- holding large amounts of value on SVCs for long periods with no redemption activity[5]
- receiving large amounts of money onto an SVC, redeeming the value, closing the SVC and then opening a new SVC and repeating the process
- redeeming value stored on SVCs in gambling establishments.

4 Not all travel cards attract fees for domestic use. This is only an indicator if the features of the particular product make domestic use of the SVC uneconomical.

5 SVC credits do not attract interest so there is limited economic rationale for this behaviour.

IMMEDIATE OFFSHORE REDEMPTION OF FUNDS LOADED IN AUSTRALIA

One SMR described an SVC that was used to move over $80,000 from an Australian bank account offshore in less than two months. The reporting entity suspected that funds were likely redeemed by a third party who was unknown to the reporting entity and who, within two days of the reload, used the same offshore ATM several times per day to exhaust the stored funds in cash.

LAUNDERING MONEY THROUGH GIFT CARDS

One SMR outlined a reporting entity's suspicion that a customer was laundering money by bulk purchasing and on-selling gift cards. The reporting entity noted that the customer was receiving structured cash deposits, interbank transfers and electronic credits into their bank account, then making high-value gift card purchases. Given the activity on the account, the reporting entity formed the suspicion that the customer was selling the purchased gift cards online.

FOREIGN RESIDENTS BUYING SVCs IN AUSTRALIA AND REDEEMING THEM OFFSHORE

One SMR described a foreign passport holder (with a foreign residential address) who purchased an SVC in Australia. They loaded the SVC with $24,000 cash over a six-month period and then returned to their country of residence, where they redeemed all the funds.

It was unclear how the temporary visitor obtained access to such large amounts of cash while in Australia, particularly given the working conditions attached to most temporary visas. It was also unclear why all of the funds would be redeemed in the customer's country of residence rather than in Australia.

In light of these considerations, reporting entities encountering this type of behaviour should consider their level of comfort that their customer has a legitimate source for the cash being loaded onto the SVC, or whether such behaviour may indicate that the cash was illicitly obtained. For example, funds may have been received as payment for illicit goods or services after arrival into Australia, in which case an SMR should be lodged.

MONEY LAUNDERING - BELOW THE THRESHOLD SVCs

AUSTRAC has observed that below the threshold SVCs are also being used to launder money. Although below the threshold SVCs can store less value at any one time (and may therefore be less attractive to those seeking to launder/move large amounts of money), below the threshold SVCs afford complete anonymity to customers and can be easily purchased in bulk to mitigate lower storage capacity.

Even though they are not subject to reporting obligations, five SMRs in the dataset related to the use of open loop below the threshold cards. Each of these SMRs related to suspected money laundering. In four SMRs, the grounds for suspicion (GFS) field indicated that the cardholder was transacting on several below the threshold cards at once.

Several additional SMRs related to money laundering through bulk purchases of closed loop below the threshold SVCs.

HOW MANY GIFT CARDS ARE THERE?

The Australian Retailers Association estimated that 32 million closed loop gift cards were issued in 2014, with a spend value of around $2 billion.[6] Most of these SVCs are below the threshold, and many are issued by entities that are not captured by Australia's AML/CTF regime.

TERRORISM FINANCING

AUSTRAC assesses that 12 of the SMRs in the SVC dataset are highly likely to be related to terrorism financing, based on details in the GFS in the SMR. These reports were made by five reporting entities and relate to over $170,000 being redeemed from above the threshold SVCs in high-risk jurisdictions.

The 12 SMRs all related to SVCs being redeemed in countries that border Syria (Turkey, Jordan and Lebanon). The use of SVCs in foreign terrorist fighter transit routes is also considered a high-risk indicator of terrorism financing. However, as SVCs can be used for legitimate activities in these countries, the presence of other terrorism financing risk indicators would increase the level of risk.

Other indicators of terrorism financing in this dataset included:

- unusually rapid exhaustion of stored funds in cash
- redemption by unknown third parties
- funds loads by unknown third parties
- possible jewellery store purchases.

Of the four stages of terrorism financing (raise, move, store and use), AUSTRAC assesses that the SVCs in the 12 identified SMRs were used in three of these stages – ***move***, ***store*** and ***use***. There is no direct evidence in the SVC SMR dataset that SVCs have been used to ***raise*** funds for terrorism in Australia.

REGIONAL USE OF SVCs FOR TERRORISM FINANCING

A joint intelligence publication by the financial intelligence units of Australia, Indonesia, Malaysia, Philippines, Singapore and Thailand noted that:

> *Stored value cards are an increasingly popular method of legitimately moving money offshore. In the context of terrorism financing, foreign terrorist fighters have used them before and after departure to their destination. They can be loaded domestically with cash or via non-reportable electronic methods, easily carried (or posted) offshore and are not subject to reporting requirements. Funds can be redeemed through multiple offshore ATM withdrawals, restricted only by ATM withdrawal limits. Cards can also be regularly reloaded remotely and anonymously by third parties, meaning that the face value of some cards understates the cards' actual risk level.*[7]

6 In Submission to Senate Standing Committee on Economics in March 2016. Source: http://retail.org.au/wp-content/uploads/2016/06/ARA-Submission-to-Sen-Inq-on-Gift-Cards-Mar-16.pdf

7 *Regional risk assessment on terrorism financing 2016*, p.36, http://www.austrac.gov.au/sites/default/files/regional-risk-assessment-SMALL_0.pdf.

TIPS FOR INDUSTRY – REPORTING TERRORISM FINANCING OFFENCES IN SMRs

Offence type

Reporting entities only selected 'Financing of terrorism' in the 'Offence Type' field of five SMRs in the sample period. However, in several other SMRs, the GFS field described activities indicating the reporting entity held concerns that the customer's behaviour could affect national security. When completing the SMR form, reporting entities should select 'Financing of terrorism' in the suspected offence type field if they suspect any link to terrorism financing. This is to ensure the SMR is detected early and escalated for priority action.

Location of redemption

AUSTRAC encourages reporting entities to provide as much information as possible about the location of overseas transactions. There is often significant variation in the extent of the terrorism financing threat posed by transactions conducted in different regions *within* higher risk jurisdictions. If possible, it would assist AUSTRAC and its partners to analyse SMRs if reporting entities included the specific region or city that suspect transactions are conducted in, rather than just the country.

POTENTIAL FOR DISPLACEMENT OF TERRORISM FINANCING ONTO SVCs

The *Regional risk assessment on terrorism financing 2016* states that the 'use of stored value cards and online payment platforms for terrorism financing is more likely to increase if detection or disruption of commonly used methods forces a shift in activity'.

AUSTRAC assesses that the hardening of the banking and remittance sectors against criminal misuse is likely to cause displacement of international remittances from traditional service providers onto SVCs. This may increase the risk that SVCs will be used for terrorism financing.

TERRORISM FINANCING - BELOW THE THRESHOLD SVCs

Terrorism financiers generally deal in relatively small sums of money. As such, below the threshold SVCs (particularly those that can be redeemed offshore) can provide a convenient vehicle for the anonymous financing of terrorism, despite their lower storage capacity.

In 2005 the United States Treasury Department observed:

> *The 9/11 hijackers opened US bank accounts, had face-to-face dealings with bank employees, signed signature cards and received wire transfers, all of which left footprints. Law enforcement was able to follow the trail, identify the hijackers and trace them back to their terror cells abroad. Had the 9/11 terrorists used prepaid [stored value] cards to cover their expenses, none of these financial footprints would have been available.*[8]

Additionally, as was widely reported in the media, below the threshold SVCs were used in the funding of the Paris terrorist attacks in November 2015. A July 2016 European Commission report observed that:

> *The investigation into the November 2015 attacks in Paris has revealed that a prepaid reloadable card issued in the EU was used for the rental of flats in Alfortville as well as the rental of cars for the commando. That card had been reloaded many times with individual reloads in excess of 750 EUR. Whilst electronic means are traceable after-the-event (unlike cash) and thus it was possible to know that a given card was reloaded many times, if the card is CDD [customer due diligence]-exempt (as in this case) it is not possible to attach a name to the holder of the card. The Belgian press recently reported that Salah Abdelsam, one of the protagonists of the Paris attacks, had used an anonymous prepaid card to move around Europe over a period of time before his arrest.*[9]

While the European Commission recognised the social utility of legitimate use of SVCs, it noted that '[a]dditional efforts are expected to further reduce anonymity in the sector, considering that the social convenience offered by prepaid cards does not have to necessarily equate with anonymity'.

8 Treasury Cash Equivalent Working Group, Prepaid Card Primer and Threat Assessment, 2005 , as cited here: https://archive.org/stream/242344-moving-illegal-proceeds-challenges-exist-in-the/242344-moving-illegal-proceeds-challenges-exist-in-the_djvu.txt

9 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016SC0223, p18

CYBER-ENABLED FRAUD

Thirty-five per cent (324) of the SMRs in the sample period indicated cyber-enabled fraud, representing the second largest category of SMRs after money laundering. Most of these SMRs described criminals purchasing above the threshold SVCs (often several at a time), obtaining unauthorised access to a victim's bank account, transferring funds from the bank account onto the SVC(s), and then immediately redeeming the stolen funds via cash or by making high-value purchases.

This methodology was often observed as being associated with:

- attempts to transfer more value onto the SVC than was in the compromised account (because the criminal did not know the exact account balance)
- attempts to withdraw more than the daily limit from an ATM
- purchasing SVCs with a very small/the minimum amount loaded and then rapidly reloading with very large amounts.

Although most activity of this kind appeared to be domestic-based, SMRs indicate that there has been some involvement by foreign criminal entities in this type of activity.

CYBER-ENABLED FRAUD - BELOW THE THRESHOLD SVCs

Criminals engaged in cyber-enabled fraud may be less likely to use below the threshold SVCs, as lower storage thresholds mean it would take longer to remove large amounts of value from the compromised accounts, thereby increasing the likelihood of the reporting entity, bank or account holder noticing the irregularity.

OTHER FRAUD

AUSTRAC assesses that a further 26 SMRs in the dataset related to other types of suspected fraud. In these SMRs:

- attempts were made to load SVCs from lost, stolen or fake credit cards
- fraudulent refunds were processed onto SVCs (without a corresponding debit) from merchant terminals.

SCAMS

A small number of SMRs (16) indicated that above the threshold SVCs were being used to facilitate scam activity. Most of these were in relation to romance scams.

Some examples of SMRs in this category include:

- a customer admitting to the reporting entity that he had sent his SVC to his 'girlfriend' who he had never met
- a customer believing his SVC was being used in one jurisdiction, when the funds were in fact being redeemed in another jurisdiction
- a reporting entity observing rapid offshore cash withdrawal activity where funds were being loaded onto the SVC from a variety of different bank accounts, and the only non-cash redemption was to online dating sites.

SVCs have also been known to facilitate tax-related scams. The United States Internal Revenue Service Commissioner called SVCs the 'currency of criminals' when a tax refund scam emerged, in which scammers used stolen identity information to claim erroneous tax rebates that were then loaded onto SVCs.[10]

SCAMS - BELOW THE THRESHOLD SVCS

There is evidence that below the threshold SVCs are being used by scammers to extract funds from victims under false pretences. For example, the ATO has warned the Australian public about scams in which the scammer tricks victims into thinking that they owe money to the ATO. The scammer instructs the victim to purchase SVCs and provide the scammer with the card numbers. The scammer then redeems the value or on-sells the SVCs.[11]

Tech giant Apple has also warned that its cards are being used in scams:

> *In a typical scheme, a con artist calls a victim and claims to be a tax officer, bill collector or lawyer representing a relative who's just been arrested. Victims are told to purchase several hundred dollars' worth of gift cards and then provide the 16 digit code from each card, usually over the phone. Fraudsters use the codes to redeem the value on the cards or even re-sell the numbers online.*[12]

10 The Tax Refund Scam, 60 Minutes (USA), aired on September 21 2014, transcript available: http://www.cbsnews.com/news/irs-scam-identity-tax-refund-fraud-60-minutes/

11 https://www.ato.gov.au/Media-centre/Media-releases/Don-t-get-played-by-iTunes-scammers/

12 https://www.yahoo.com/tech/apple-warns-against-scams-involving-itunes-cards-213204611--finance.html, September 10 2016

TAX EVASION

Less than two per cent of SMRs in the sample period indicated the use of above the threshold SVCs for tax evasion. All of these SMRs related to individual customers who appeared to be using SVCs as a de facto bank account in which to receive wages or payments for services rendered, in suspected attempts to avoid declaring the funds to the ATO as income for taxation purposes.

TAX EVASION - BELOW THE THRESHOLD SVCs

Given the amounts of money that can be loaded, redeemed and reloaded on some below the threshold SVCs over time, they have high potential to facilitate the anonymous receipt of undeclared wages, and/or illegitimately obtained wage. The risk of below the threshold SVCs being used for scams or tax evasion is also likely to be relatively high, because these crimes are less likely to be detected by reporting entities in a timely manner. This increases the potential for long-term exploitation of a single product, meaning that the SVC can be made lucrative despite low storage limits.

OTHER INDICATORS OF SUSPICION

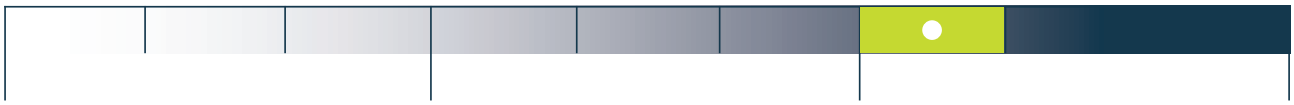
The remaining SMRs in the dataset were in relation to a range of matters, but due to the limited information in the SMR, it was not possible to assess a likely offence type.

The indicators of suspicion in these SMRs included:

- likely unknown third parties transacting on SVCs that were being redeemed offshore without an obvious associated crime (eight per cent of SMRs)
- redemption of SVCs in high-risk jurisdictions for terrorism financing, but without any other details to indicate likely terrorism financing (five per cent of SMRs)
- generally suspicious behaviour by a customer (five per cent of SMRs).

All of these indicators are explored further in the following 'Vulnerabilities' section.

VULNERABILITIES



Vulnerability refers to the characteristics of SVCs that make them susceptible to criminal exploitation. Many of these risk factors can apply to both above and below the threshold SVCs, depending on the specific features of individual SVC products.

AUSTRAC assesses that SVCs carry a **HIGH** level of vulnerability to ML/TF.

PRODUCT FEATURES

The features of individual SVC products in the Australian market vary significantly. This means that the vulnerability associated with different products also varies significantly. As widely observed, the risk of 'open loop' SVCs is generally higher than that of 'closed loop' SVCs. However, in this risk assessment AUSTRAC has moved beyond the simple open loop/closed loop comparison to assess risk. Instead, this section canvasses several additional product features that significantly influence an SVC's vulnerability to misuse, all of which require attention when considering a product's risk. This analytical framework allows for a more in-depth assessment of vulnerability.

AUSTRAC assesses that the key factors affecting the vulnerability of an SVC are:

- reloadability
- ability to use cash to load/reload the SVC
- ability to redeem SVC value in cash
- ability to redeem at a wide range of merchants ('acceptability')
- ability to redeem internationally
- high storage limits.

Individual features of an SVC should not be considered in isolation – the overall risk of each SVC should be seen as a combination of all of its features, and importantly, how its combined features interact to determine its potential functionality in the hands of the customer.

RELOADABILITY

Reloadable SVCs present a higher risk in terms of ML/TF and other offences, compared to non-reloadable SVCs. This is because illicit funds can be moved between locations and/or people outside traditional banking/remittance channels. For example, reloadability can be used to support:

- systematic movement of proceeds of crime from Australia to an unknown third party offshore
- remittance of terrorism financing into high-risk countries
- movement of funds from compromised accounts for easy and immediate redemption from ATMs.

LOAD/RELOAD METHODS

SVCs that allow loading/reloading in cash are more vulnerable to criminal exploitation than cards that have restrictions on cash loads. This is because cards that accept cash deposits are likely to be preferred by criminals seeking to launder proceeds of crime.

Non-cash reloads also present vulnerabilities. For example, certain electronic means of reloading SVCs increase vulnerability to exploitation for cyber-enabled fraud.

For this reason, it is important for reporting entities to consider the range of different crime types facilitated by SVCs when deciding on allowable load/reload methods.

CASH REDEMPTION

SMR data demonstrates SVCs that allow cash redemption are highly vulnerable to criminal misuse. It is clear that cash redemption is a key feature exploited by criminals to access the proceeds of cyber-enabled fraud. SMRs indicating the movement of proceeds of crime offshore consistently describe systematic cash withdrawals. Cash redemption in Syrian border countries was also a key feature of the terrorism financing dataset described earlier.

While cash redemption is often associated with open loop cards, there are open loop cards that do not allow cash redemption.

ACCEPTABILITY

Where SVCs can be redeemed is another very important product feature that influences vulnerability to criminal misuse. SVCs that are accepted throughout the Visa/MasterCard global network carry higher levels of vulnerability compared to SVCs that are only accepted at a single business.

However, AUSTRAC notes that there is significant variability in acceptability among closed loop SVCs, which makes some of these SVCs more vulnerable to exploitation than others. For example, a $1,000 gift card for an independent clothing boutique has very limited redemption flexibility or resale potential. On the other hand, a $1,000 closed loop gift card for a large group of different but related household retailers such as supermarkets, department stores and hardware stores, could be usefully redeemed both by criminals and legitimate consumers buying gift cards on secondary markets.

OFFSHORE REDEMPTION

The ability to redeem funds internationally can expose SVCs to very significant jurisdiction risks –including in relation to terrorism financing – especially when combined with other features such as the ability to withdraw cash, reloadability and/or high storage limits.

The AUSTRAC survey revealed that customers of SVCs redeemed $2.2 billion in foreign countries between 1 September 2015 and 31 August 2016.

HIGH STORAGE LIMITS

SVCs carry a range of storage limits. The more value that can be stored on an SVC at any one time, the higher its vulnerability to criminal exploitation, especially for money laundering and cyber-enabled fraud. AUSTRAC's survey revealed there are at least three above the threshold SVC products that can store up to $100,000. One industry expert engaged by AUSTRAC questioned why SVCs that are travel cards would have such high storage limits, because the storage capacity was excessive for the requirements of tourists.

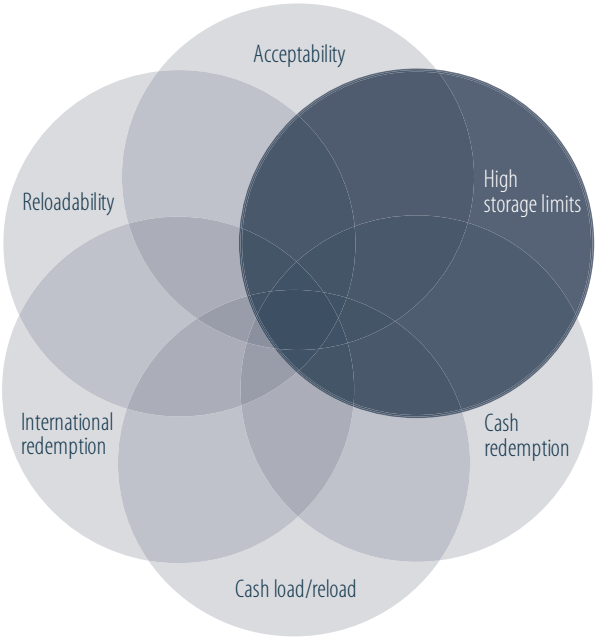
AUSTRAC encourages reporting entities to manage this vulnerability by ensuring the storage limits applied to individual products are appropriate and proportionate to the purpose of the SVC.

OVERALL RISK AS A COMBINATION OF FEATURES

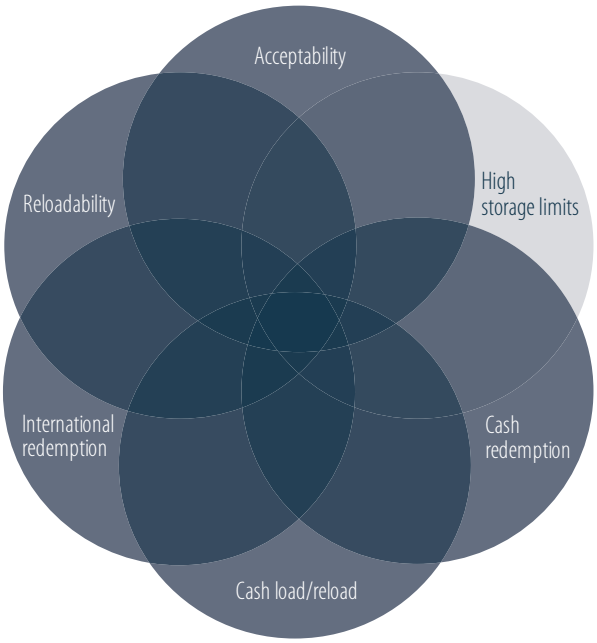
An SVC that has none, or only one, of the above features is likely to be relatively lower risk than an SVC that has several of them. For example, a single load $6,000 e-gift card that can only be redeemed at an Australian clothing retailer ('SVC 1') would be relatively low risk. However, a reloadable SVC accepted globally on the Visa or MasterCard network, which can be redeemed in cash and hold up to $999 at any one time ('SVC 2'), carries a higher risk. Yet, under current regulatory frameworks, SVC 1 will be above the threshold and SVC 2 will be below.

This is illustrated in the diagrams below.

SVC 1 (above the threshold, but with only one high-risk feature)



SVC 2 (below the threshold, but with five of six high-risk features)



CUSTOMERS

Based on responses to AUSTRAC's survey, there were at least 3.4 million active above the threshold SVCs as at 31 August 2016. Although some customers may hold more than one SVC, this figure provides a useful indication of the size of the customer base for above the threshold SVCs in Australia.

The vast majority of SMRs lodged by reporting entities in the sample period were in relation to individual customers – most frequently as the perpetrator of suspected criminal activity, but in some cases as the victim of a crime (in relation to scams, for example).

Only nine SMRs (one per cent) in the dataset related to corporate customers – always as the perpetrator of suspected crime. In five of these SMRs, funds on SVCs were redeemed in high-risk jurisdictions where the party loading the funds was likely to be different to the party redeeming the funds. The remaining four SMRs related to suspected money laundering – largely relating to bulk purchases of SVCs.

THIRD PARTY USE

The ability for above the threshold SVCs to be reloaded/redeemed by unidentified third parties creates additional vulnerabilities, particularly where secondary cards are available.

118 SMRs in the dataset (13 per cent) indicated that value loaded onto Australian SVCs was redeemed offshore by a person who was either not the 'customer', or not the person who loaded value onto the SVC. This was generally indicated by the fact that the offshore redemptions took place too quickly after funds were loaded in Australia (for example, in branch/at physical retailer) for the loading individual to travel to the offshore redemption location.

Reporting entities may also be able to identify when online SVC transactions are facilitated simultaneously from IP addresses in different jurisdictions, suggesting use by a third party.

Some reporting entities noted that unknown third-party use was contrary to the intention, as well as the terms and conditions, of the relevant product. While AUSTRAC recognises that customers using SVCs in this way may not be involved in illicit activity, reporting entities should consider whether they should allow their customers to use their cards in a manner contrary to the terms and conditions.

WHO IS THE CUSTOMER OF AN SVC DESIGNATED SERVICE?

Reporting entities need to undertake their 'applicable customer identification procedure' in relation to customers of their designated services. When an above the threshold SVC is purchased, the person who needs to be identified is the person to whom the SVC is being issued. When an above the threshold SVC is reloaded and storing an amount above the threshold, the customer of the SVC is the person 'holding' the card – which could be someone other than the person to whom the card was issued. As such, there may be more than one customer in relation to one SVC.

It appears that reporting entities may not be aware of this, as many SMRs refer to redemption of reloadable cards by an 'unknown third party', who the reporting entity does not appear to have identified. This makes SVCs much more vulnerable to criminal misuse.

CUSTOMERS – BELOW THE THRESHOLD SVCs

There is no requirement for entities to identify customers of below the threshold SVCs, meaning these SVCs are essentially anonymous products.

As with above the threshold SVCs, it is likely that the vast majority of customers of below the threshold SVCs are individuals. However, traveller activity is likely to be much lower on below the threshold cards, because travellers often require more funds than can be stored on below the threshold cards at any one time.

The customer base for below the threshold SVCs in Australia is likely to be substantially larger than the above the threshold card market, due to the number of below the threshold SVCs (including gift cards) in circulation.

SOURCE OF FUNDS AND WEALTH

The inability to ascertain the source of funds being used to purchase and/or load SVCs was indicated across the SMR dataset and is a key ML/TF vulnerability. When a reporting entity provides to a customer general banking services as well as SVCs, they are often able to identify salary credits or welfare payments entering an account held by the SVC customer. This means that some reporting entities have been able to form a suspicion when, for example, a customer receiving Centrelink benefits also has unusually large amounts of cash loaded onto their SVC, contrary to their apparent income level.

Ascertaining source of funds is made more difficult when SVCs are loaded or reloaded by third parties. Third parties are often not identified, limiting the ability for reporting entities to assess the legitimacy of the funds they load. Some SMRs indicated that reporting entities attempted to analyse the transaction description for the funds load, to determine the source of funds for value electronically credited. However, these descriptors are not reliable indicators of actual source of funds.

SOURCE OF FUNDS AND WEALTH – BELOW THE THRESHOLD SVCs

There is no legal requirement for reporting entities to establish the source of funds and wealth for below the threshold SVCs. This increases the vulnerability of below the threshold cards. Reporting entities enrolled with AUSTRAC may seek to voluntarily determine source of funds and wealth relating to below the threshold SVCs. However, it is highly unlikely that SVC issuers who are not enrolled with AUSTRAC (for example, bookshops that issue gift cards) seek this kind of information from their customer.

DELIVERY CHANNEL

Many above the threshold SVCs can be purchased and reloaded entirely online, so the customer has only online contact with the reporting entity (or the reporting entity's agent). Where contact is completely online, the reporting entity or their agent has much more limited opportunity to observe customer behaviour and form reasonable suspicions on that basis.

In cases where SVCs are purchased or reloaded in person by customers, reporting entities have been able to generate useful insights into customers' behaviour. Five per cent (49) of SMRs in the dataset related to a customer behaving in a suspicious manner, generally at a physical retailer, including:

- providing false identity details or documentation
- providing contradictory information
- aborting transactions before they were finalised.

Some SMRs also indicated that customers were attempting to avoid being noticed, by visiting several different physical retailers to conduct large numbers of face-to-face SVC transactions. Reporting entities that maintain centralised oversight of transactions processed at all of their sites may be better placed to identify suspicious patterns of behaviour than entities whose transaction monitoring is isolated by site.

These examples demonstrate the usefulness of having face-to-face contact with customers, as well as having engaged, well-trained staff who understand the risks associated with use of SVCs.

MITIGATING DELIVERY CHANNEL RISK

Several reporting entities have sought to mitigate the risks associated with the online delivery of SVC services by increasing their ability to maintain remote oversight of their customers' transactions. SMRs indicated that some reporting entities are able to determine the location where online reloads of SVCs were being conducted, and compare this with the location in which that value was redeemed.[13] Where these locations were not the same, this enabled the reporting entity to form a suspicion that at least one of the transacting parties was not their customer.

Reporting entities were also able to remotely compare the time of the funds load with the time of redemption. This could raise suspicion as to why a customer would load funds onto an SVC and then immediately redeem them.

13 While sophisticated criminals can obscure the location of their internet activity, limiting the utility of monitoring IP addresses, it is AUSTRAC's view that when funds loads appear to be occurring onshore and redemption offshore, this may be sufficient to form a reasonable suspicion that the loading party is not the redeeming party.

DELIVERY CHANNEL – BELOW THE THRESHOLD SVCs

There is a substantial online secondary market for buying and selling below the threshold SVCs. These secondary markets are vulnerable to criminal exploitation. Money launderers may convert proceeds of crime (that may be in cash) into apparently legitimate electronic value, by buying below the threshold SVCs and then selling them online.

For example, customers with unwanted e-gift cards can sell them to an online intermediary for below face value. The intermediary can then on-sell the e-gift card at a discount to another customer, and keep the difference between these prices for themselves. There are also online secondary marketplaces in which SVCs can be sold directly from a holder to a buyer, without an intermediary.

There is also an online market for buying below the threshold SVCs with bitcoin. One website facilitates the use of bitcoin to purchase various broadly-accepted below the threshold cards (including a card from which cash can be withdrawn), using bitcoin.

FOREIGN JURISDICTION

SVCs that allow value to be redeemed offshore and allow for the storage of foreign currency (commonly known as a 'travel cards') constitute a substantial portion of the above the threshold SVC market in Australia. There are also SVCs that are marketed as 'general purpose', which have several of the same features as travel cards, including the ability to redeem value overseas.

	Above the threshold SVCs
Amount redeemed from point of sale transactions offshore	$1,251,133,462
Amount redeemed in cash offshore	$980,255,213
Total	$2,231,388,674

The figures in the table above were drawn from the AUSTRAC survey data and show that some $2.2 billion was redeemed from above the threshold SVCs offshore in one year. This makes foreign jurisdiction risk a significant vulnerability for SVCs.

Several entities and industry experts engaged for this assessment believed that the travel card market will continue to grow, largely due to the enhanced functionality and security of travel cards when compared to travellers cheques, cash, debit and credit cards. However, the remittance-like function of several travel and general purpose SVCs could also be used by criminals to move illicit funds offshore, or to pay for illicit goods and services that are produced offshore.

Twenty-three per cent (212) of the SMRs in the sample period referred to SVCs that were redeemed outside Australia. Although overseas redemption of SVCs is not on its own an indication of a suspicious activity, concern was raised by reporting entities when offshore redemption was combined with:

- cash-intensive transactions (both loads and reloads) indicative of money laundering
- redemption/loads by unknown third parties
- transactional activity considered excessive for the purposes of tourism
- redemption in high-risk jurisdictions.

Approximately one-third (66) of the 212 SMRs referenced above related to SVCs being redeemed in jurisdictions considered high risk for terrorism financing or high risk as a transit hub for terrorism financing. Many of these included indications that funds were either provided or redeemed by a person who was not the customer identified by the reporting entity. These SMRs did not contain sufficient details to be assessed as terrorism financing related and were therefore not included in the terrorism financing section of this assessment.

Responses to the AUSTRAC survey indicate that various SVCs cannot be used in selected high-risk jurisdictions. However, some reporting entities indicated that these limitations were outside their control, as they are usually set by the scheme that provided the payment network (that is, Visa or MasterCard). One reporting entity noted that they would like to expand the list of countries in which value could not be redeemed, but that they could not affect this themselves, which created vulnerability for their business.

FOREIGN JURISDICTION – BELOW THE THRESHOLD SVCs

The extent to which below the threshold SVCs are used in foreign jurisdictions is an intelligence gap for AUSTRAC. However, some below the threshold SVCs may be more exposed to foreign jurisdiction risk in relation to crimes – such as terrorism financing– that rely on comparatively small volumes of funds being moved offshore anonymously.

USE OF CASH

There is extensive use of cash in the SVC market, because it can be used to load as well as redeem value from several SVCs (subject to individual product specifications). Responses to the AUSTRAC survey of SVC issuers revealed that:

- In the twelve months to 31 August 2016, customers loaded $835,472,932 in cash onto SVCs.
- Over the same time period, customers redeemed $981,501,987 from SVCs in cash overseas

The extent of cash activity using SVCs is also shown below, based on TTRs submitted to AUSTRAC.[14] As the majority of SVC customers are individuals, it is unclear why SVCs are being used to transact in such large cash amounts.

TTRs SUBMITTED BY REPORTING ENTITIES

9,022 Number of TTRs submitted

$121.8M Total value of TTRs

$13,496 Average value of TTRs

19 Number of reporting entities submitting at least 1 TTR

1 April 2014 to 31 March 2016

There was substantial evidence in SMRs that the above the threshold SVC market is subject to 'structured' loading activity. This is where large amounts of cash are systematically loaded onto SVCs in a way that avoids the requirement to lodge a TTR. This can be a strong indicator of money laundering 'placement'.

SMRs also detailed large amounts of cash being systematically redeemed from SVCs. This can indicate:

- the final stage of a successful cyber-enabled fraud
- the movement of proceeds of crime between locations (outside traditional banking/remittance channels)
- the movement of funds from Australia to support terrorist activity in high-risk jurisdictions (outside traditional banking/remittance channels).

USE OF CASH – BELOW THE THRESHOLD SVCs

One large reporting entity consulted for this risk assessment observed that, despite lower storage limits, below the threshold cards can be highly attractive vehicles for the disposal and/or redemption of cash. Below the threshold SVCs can be purchased in bulk with cash proceeds of crime. Reloadable SVCs that are redeemable in cash can be made very lucrative over several transactions and/or SVCs.

OPERATIONAL VULNERABILITIES

Industry feedback to AUSTRAC demonstrates that there is extensive outsourcing in relation to the issue, management, and processing of SVCs to external entities, often with a chain of multiple entities involved. This can affect the capacity of the SVC issuer, who is ultimately responsible for all AML/CTF compliance, to effectively discharge their AML/CTF obligations.

For example, AUSTRAC understands it is common practice for SVC issuers to outsource AML/CTF obligations to a program manager, who may in turn outsource transaction monitoring functions, SMR reporting and/or 'know your customer' collection and verification to another third party (for example, a processing platform). In this situation there is no direct relationship between the SVC issuer and the processing platform (see figure 1 below). If not carefully implemented and monitored, this type of separation between the party that holds the AML/CTF obligations and the parties discharging the obligations, could compromise the integrity and effectiveness of the reporting entity's AML/CTF regime in relation to SVCs.

One reporting entity engaged by AUSTRAC described a model that applied to some of its SVCs in which all parties engaged in discharging AML/CTF obligations were contractually related to each other (see figure 2). This type of arrangement provides AUSTRAC with more comfort that the reporting entity has the mechanisms and relationships in place to be able to access data, exercise oversight and where necessary, influence practices to help reduce risk.

14 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.

Figure 1

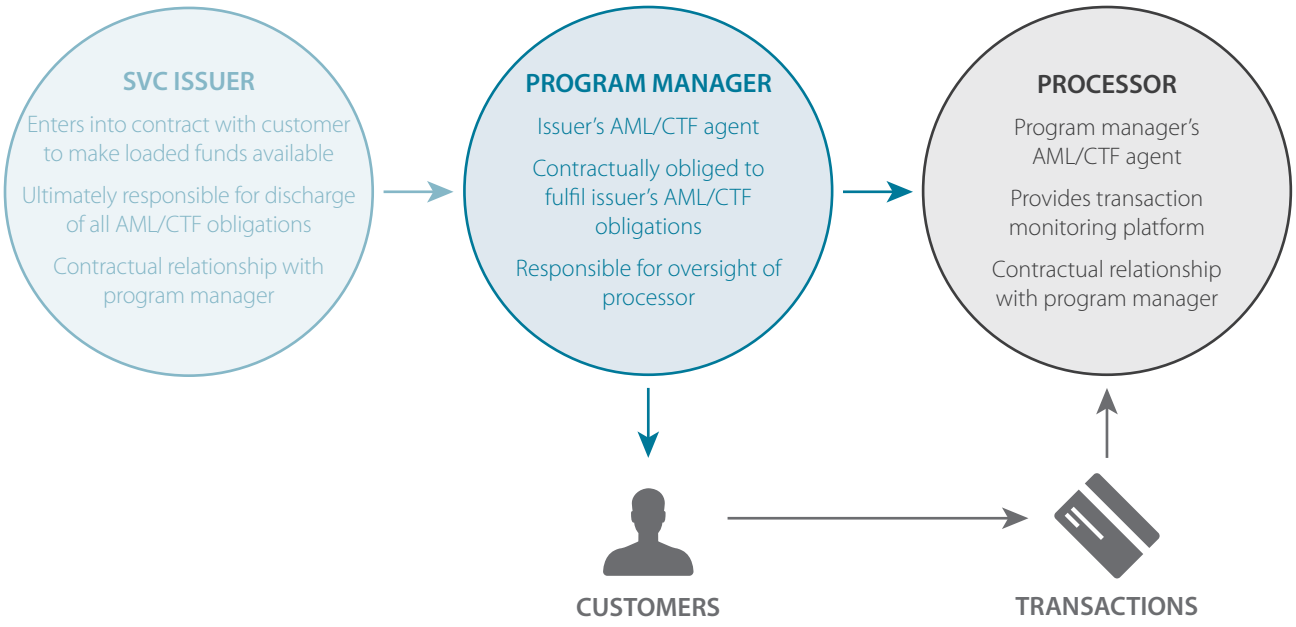
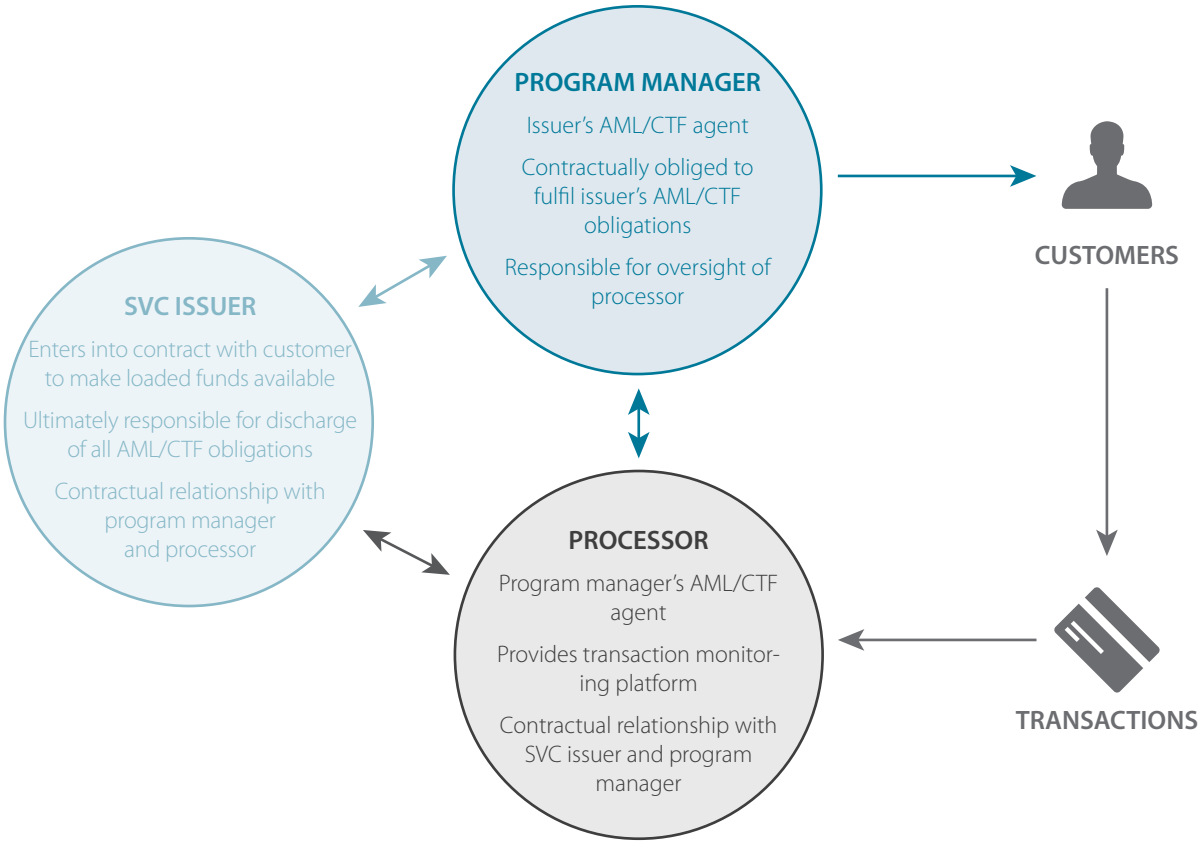


Figure 2



WHO HAS TO REPORT THE SMR?

One reporting entity revealed to AUSTRAC that overlapping responsibilities in terms of SVC service provision had created confusion as to who was required to report SMRs. While SMR lodgement may be outsourced, it is the responsibility of the 'designated service' provider to ensure that SMRs are lodged when required, and that complementary AML/CTF systems and controls are in place, such as staff training and enhanced customer due diligence. To do this, the reporting entity should have robust oversight of, and clarity in, its contracts with service providers.

RISK MITIGATION

AUSTRAC observed in some SMRs that effective communication and cooperation between entities had assisted in identifying and mitigating some threats. For example, cooperation between entities in relation to cyber-enabled fraud restricted the amount of money that some cybercriminals were able to fraudulently obtain from bank accounts. Additionally, during AUSTRAC's engagement with reporting entities, some entities demonstrated they had taken proactive measures to identify exploitation of their SVCs, and respond by changing product features to successfully reduce misuse. For example, one reporting entity advised that they had revised the reload methods applicable to one of their products, which had reduced the amount of fraud they saw on those cards.

AML/CTF SYSTEMS AND CONTROLS

A significant vulnerability in the AML/CTF controls in place for SVCs is the lack of identification and verification of customers who redeem value on reloadable SVCs, when that customer was not the person to whom the SVC was issued. During consultation with AUSTRAC, some reporting entities indicated they had not considered that the customer for the designated service for reloading may be a different person to the customer of the designated service for issuing. As such, the reporting entities had not been identifying the former.

One SMR described a case in which a customer possessed two sets of primary and secondary SVCs. The primary cards were loaded in Australia with cash. Shortly afterwards, all the funds were redeemed from ATMs overseas using the secondary cards. The SMR noted that this conduct was against the policy of the SVC issuer. However, there was no indication that the reporting entity responded to this breach of their conditions by suspending the card, or seeking clarification from the customer as to the purpose of their transactions, or the identity (or identities) of the person(s) redeeming the funds. Where a customer is using an SVC in a manner contrary to the SVC's terms and conditions, AUSTRAC encourages reporting entities to investigate the matter; for example, seeking further information from the customer, and in some cases by suspending or cancelling the SVC.

USE OF SVCs AS REMITTANCE VEHICLES

SVCs that can be reloaded and from which cash can be withdrawn offshore, are particularly vulnerable to being used as a de facto remittance vehicle. Thirteen per cent of SMRs related to above the threshold SVCs that were being redeemed offshore, in circumstances where the person loading the funds onto the SVC was likely to be different to the person redeeming the funds offshore.

Many of these SMRs noted that substantial volumes of funds were rapidly exhausted via offshore ATMs in a manner deemed by the reporting entity to be 'inconsistent with tourist use'. In some cases this activity may relate to romance scams or the provision of financial assistance to friends and family overseas, but such activity can also indicate attempts to move proceeds of crime offshore.

All reporting entities consulted for this assessment strongly indicated that SVCs should not be used to remit funds offshore, and that this was not the purpose of these products. However, there was also broad acknowledgement that in practice many customers used SVCs in this way.

This is an area of significant concern as it carries extensive ML/TF risks. SVCs operating in this way effectively circumvent many of the existing AML/CTF regulations that apply to remittance activities because:

- the person loading the funds onto the SVC does not have to be identified unless they are holding the card and/or are the person to whom the card was issued
- it is not common practice for the cardholder redeeming funds to be identified, when this person is not the person to whom the SVC was issued.

Additionally, use of SVCs as de facto remittance vehicles is highly vulnerable to 'mule' activity. A person who is reluctant to identify themselves may request a third party to purchase the SVC in the third party's name, then pass the SVC to the first person who may use the SVC to anonymously remit money offshore.

During consultation with AUSTRAC, several SVC issuers revealed they were approached by remitters who wished to set up SVC-based systems of money remittance. SVC issuers indicated that taking on a remitter as a corporate client was outside their risk appetite, so all the requests were declined. Some reporting entities attributed the increase in these enquiries to the ongoing process of banks exiting customers who are remitters, who are in turn seeking alternative means to remit funds offshore.

AML/CTF SYSTEMS AND CONTROLS: BELOW THE THRESHOLD SVCs

AML/CTF systems and controls are not mandated in relation to below the threshold SVCs.

One large reporting entity emphasised the vulnerability caused by the absence of reporting obligations in relation to below the threshold open loop SVCs. They also reiterated that below the threshold closed loop SVCs are being used to support scam and fraud activity. They observed that criminals could obtain bulk below the threshold SVCs to move larger amounts of money, and voiced their concern that if reporting entities only strengthened their systems and controls in relation to above the threshold SVCs, then criminality would be displaced onto below the threshold SVCs where systems and controls remained weak.

VULNERABILITY MITIGATION

AUSTRAC's engagement with reporting entities demonstrated that many have implemented risk mitigation techniques that have made their products and/or processes less vulnerable to criminal misuse. Depending on the purpose and features of the SVC product, there are various techniques reporting entities could and have used to limit and mitigate their vulnerabilities. Some of these have been detailed throughout this assessment and are listed below.

PRODUCT FEATURES

- Lowering reload limits, particularly for cash reloads
- Lowering redemption limits, particularly for cash redemption
- Lowering maximum storage limits (for example from $100,000 to $25,000)

CUSTOMERS

- Restricting the ability for SVCs to be used by unknown third parties

SOURCE OF FUNDS

- Identifying all people who reload an SVC in cash
- Allowing electronic reloads to be sourced only from the customer's bank account

DELIVERY CHANNEL

- Implementing transaction monitoring measures to identify when an unknown third party is loading or redeeming funds
- Centralising transaction monitoring so that transactions conducted by the same customer over various sites and/or products are identifiable
- Conducting enhanced customer due diligence on customers that conduct bulk online purchases of SVCs

FOREIGN JURISDICTION

- Implementing transaction monitoring measures that trigger alerts when transactions are initiated in high-risk regions or in various regions simultaneously

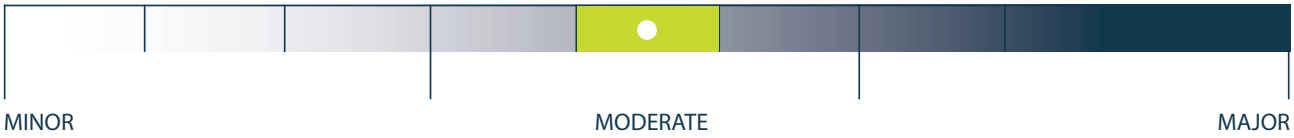
USE OF CASH

- Lowering cash load, reload and redemption limits
- Requiring senior manager approval to process cash transactions above a certain amount

OPERATIONAL VULNERABILITIES

- Where outsourcing occurs, implementing contractual arrangements as outlined in the Operational vulnerabilities section
- Where outsourcing occurs, ensuring contracts explicitly identify which party will discharge each obligation and how they will discharge it
- Maintaining regular oversight of outsourced service providers, including understanding their processes and systems
- Ensuring that information management systems capture metadata in relation to card use, in particular load and redemption amounts by load/redemption method.

CONSEQUENCES



Consequence refers to the potential impact or harm that ML/TF and other crimes may cause. AUSTRAC has assessed the consequences of ML/TF activity facilitated by above the threshold SVCs as **MODERATE**.

Criminal activity associated with above the threshold SVCs has consequences for individuals, SVC issuers and their agents, other financial institutions, and the Australian economy and community. There are also national security and international consequences. While the absence of reporting data in relation to below the threshold SVCs makes it difficult to assess the consequences of their misuse, AUSTRAC believes that the consequences would be similar in nature.

INDIVIDUALS

There are financial and indirect consequences for customers of SVCs. These could include financial loss and emotional distress for customers, for example when they are the victims of scams.

SVC ISSUERS AND THEIR AGENTS, AND OTHER FINANCIAL INSTITUTIONS

Consequences could include:

- increased costs associated with combating criminal attacks, particularly IT security costs to build cyber resilience
- increased administrative costs in reviewing accounts upon the discovery of a fraudulent/criminal activity
- undermining the relationship between SVC issuers and their agents, including potential costs associated with addressing contractual disagreements or establishing new business relationships
- reputational damage and loss of consumer confidence in the product, and potentially the company brand and other products associated with the brand (this may also lead to loss of customers)
- requirement to reduce flexibility in product offering, if more onerous requirements are needed to mitigate threats
- regulatory action
- financial institutions that provide account services for victims of identity theft are likely to bear the burden of reimbursing victims for stolen funds – for example, through a cyber-enabled fraud incident – and may also face increased fraud insurance premiums.

AUSTRALIAN ECONOMY AND COMMUNITY

The use of SVCs to facilitate criminal activity has the potential to impact the broader Australian economy and community, including:

- undetected criminal activity (particularly through below the threshold SVCs), thereby providing a safe haven for the proceeds of crime
- diminishing Australia's tax revenue base when used to facilitate tax evasion
- undermining the integrity and effectiveness of Australia's remittance regulation framework when used as de facto remittance vehicles
- harms to the community associated with criminal activity.

Despite these issues, the overall impact of associated ML/TF through SVCs on the Australian economy is unlikely to be very significant.

NATIONAL SECURITY AND INTERNATIONAL CONSEQUENCES

The most significant potential consequence of the criminal use of SVCs is the threat to national and international security if used to facilitate terrorism financing, particularly enabling and sustaining the activities of foreign terrorist fighters. Indeed, the Paris terrorist attacks of November 2015 demonstrate the significant harm that can be caused using funds stored on SVCs. Such an incident harms both international stability as well as Australia's global image.

FEEDBACK

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

APPENDIX

RISK ASSESSMENT METHODOLOGY

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

For **criminal threat environment**, six risk factors were considered – each was given equal weight. The average of these six ratings gave an overall rating for threat.

For **vulnerabilities**, there were 15 risk factors. These were grouped into eight subsections – customers, source of funds and wealth, products and services, delivery channel, foreign jurisdiction, use of cash, operational vulnerabilities, and AML/CTF systems and controls. The average of these eight subsections gave an overall rating for vulnerabilities.

For **consequences**, four risk factors were considered – each was given equal weight. The average of these ratings gave an overall rating for consequences.

CRIMINAL THREAT ENVIRONMENT

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

VULNERABILITIES

LOW MEDIUM HIGH

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

CONSEQUENCES

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

www.austrac.gov.au

APRIL 2017