TRENDS & ISSUES
in crime and criminal justice

Australian Government
Australian Institute of Criminology

No. 363 September 2008

Money laundering risks of prepaid stored value cards

Kim-Kwang Raymond Choo

In the past decade, there has been an increasing reliance on electronic means of transferring funds for personal and business purposes. One recent development has been the emergence of plastic cards with the capacity to store value electronically, which can be used for a range of retail transactions. With the advent of comprehensive anti-money laundering laws throughout the developed world, criminals are turning to alternative ways of moving funds across borders to circumvent reporting and detection systems. One identified risk is the misuse of prepaid stored value cards to keep the proceeds of crime and move them across borders without alerting law enforcement and financial intelligence units. This paper describes the nature of these risks and considers whether existing regulatory measures are adequate to address them.

Judy Putt
General Manager, Research

The use of electronic transactions has increased considerably in recent years. In Australia, the volume and value of cheque transactions in paper-based clearing systems fell from an average of 2.7 million per day in 2001 to 2.1 million in 2005, and from an average of $8.3b per day in 2001 to $6.3b in 2005 (APCA 2005). A correspondingly large increase in electronic banking has also been observed. This is hardly surprising, as the financial incentive to do business electronically in today's highly competitive market is significant, with the cost of an online transaction often being a fraction of a non-electronic transaction (De Young 2001). Similarly, online retail spending has increased considerably with total sales in the United States in 2007 exceeding US$100b (Ames 2007). One of the more popular electronic payment systems is prepaid stored value cards (SVCs), such as gift cards issued by retail stores.

> The overall market for gift cards is projected to grow to nearly $88 billion in 2008, with the fastest growth occurring in corporate purchases of gift cards for employees and customers, and in "open" gift cards – like the American Express Gift Card that can be redeemed at multiple merchants…. Corporate purchases will rise 72% from 2005 to 2008, growing from [US]$9 billion to [US]$15.5 billion. Open gift card sales are expected to almost quadruple from 2005 to 2008, growing from [US]$1.3 billion to [US]$5 billion, according to Mercator (American Express 2006).

This extensive use of SVCs, coupled with the convergence of financial services and electronic payment technologies, has created new opportunities for money laundering. This paper examines the nature of the risks and how they can best be addressed.

Prepaid stored value cards

Stored value cards are cards with data encoded in either a magnetic strip or a computer chip that are preloaded with a fixed amount of electronic currency or value. This can be redeemed or transferred to individuals and/or merchants in a manner that is similar to spending physical currency.

ISSN 0817-8542

ISBN 978 1 921185 92 2

GPO Box 2944
Canberra ACT 2601
Australia
Tel: 02 6260 9200
Fax: 02 6260 9299

For a complete list and the full text of the papers in the *Trends & issues in crime and criminal justice* series, visit the AIC website at: http://www.aic.gov.au

Project no. 0140

The players in a typical SVC program include:

- program managers – owners of prepaid SVC programs who establish relationships with payment processing facilities (e.g. banks and payment networks) and distributors, and establish pooled account(s) at banks
- payment processing facilities – are responsible for payment transactions for prepaid SVC programs, and they track and distribute funds in pooled accounts. Program managers may also choose to function as their own payment processors
- banks – may also function as program managers and/or distributors, and are responsible for maintaining pooled accounts, settling payments and issuing branded prepaid SVCs (open-system cards)
- the payments network – the 'link' between payment processing facilities, and the retailer and automated teller machine (ATM), for authorisation of payment transactions
- a distributor (e.g. banks and non-financial institutions) – responsible for selling prepaid SVCs.

The market for SVCs has increased considerably over the years, particularly in terms of its availability and size. A recent study by Mercator Advisory Group estimated that '[US]$171.18 Billion was loaded on Closed Loop Prepaid Solutions in 2006, an increase of 13.9% over the 2005 spend of [US]$160.29 [billion]' (Sloane 2007). Another study on prepaid general-purpose spending cards (open system cards) predicted that more than 300 million individuals in Latin America (Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Peru, Venezuela, Central America and Dominican Republic) could have prepaid cards that do not require bank accounts by 2015. The spending power is estimated to be more than US$214b (NovoPayment 2008).

This is, perhaps, not surprising, considering the many benefits associated with SVCs:

- easy to get and use (cardholder/buyer anonymity) – credit checks are not required when purchasing SVCs and for some cards, evidence of identification is also not needed
- convenient – SVCs can be purchased, reloaded (for open and semi-open card systems), and redeemed and refunded at conveniently located participating merchant locations (e.g. supermarkets and convenience stores). The UK-based pay-as-you-go MasterCard® card, for example, allows cardholders to obtain their balance, top up their card or lock/unlock their card for added security, from anywhere, 24 hours a day, by sending text messages from a registered mobile phone (Payments News 2008)
- affordable – funds are immediately available, often at a lower cost than when using traditional banking services
- reduced overdraft risk – reduces the risk of overdrafts while providing nearly immediate liquidity for consumers.

The PaymentsDynamicsSM 2007 study also found that ease of use, universal acceptance, the ability to use one's own money, safety and security, and the ability to have control over one's finances are the key drivers for the growth of prepaid cards in the unbanked population (Abal 2007).

SVCs can be categorised broadly into open systems (or open-loop systems), semi-open systems, closed systems (or closed-loop systems) and semi-closed systems (Table 1).

Table 1: Categories of stored value cards

Types	Description	Anonymous?	Reloadable?	Examples
Open system cards	Typically branded (e.g. by American Express) and connected to global debit and ATM networks, which allow the cards to be used for multiple purposes and at multiple points of sale with different participating merchants	Typically no (similar in appearance to traditional debit cards, which are embossed with the cardholder's name and the expiry date)	Typically yes (e.g. via regular deposit arrangement, internet and at participating merchant outlets)	Visa cash passport card [a], a reloadable pin-protected Visa-branded SVC, which allows cardholders to withdraw cash from Visa ATMs worldwide and use the cards at places where Visa debit cards are accepted
Semi-open system cards	Generally have the same features as open system cards, but cannot be used to access cash at ATMs (also known as purchasing-only cards)	Typically no (similar in appearance to traditional debit cards, which are embossed with the cardholder's name and the expiry date)	Typically yes	NETS CashCard [b]
Closed system cards	Limited to only buying goods or services from the merchant issuing the card	Typically yes	Typically no, and sold at preset denominations, but some retail gift cards are reloadable	David Jones Gift Card [c]
Semi-closed system cards	Can be used at a selected group of merchants or service providers	Typically yes	Typically no, and sold at preset denominations	FlyBuys gift cards [d], which can only be used at participating merchants

a: http://www.cashpassportcard.com/

b: http://www.nets.com.sg/consumers/netscashcard/index.php

c: http://www.davidjones.com.au/gift_card.jsp

d: https://www.flybuys.com.au

Open system cards typically allow high values to be loaded and kept on cards. Open system cards that are designed to facilitate cross-border remittance payments are also offered by offshore banks. Such systems often allow multiple cards to be issued per account, so that friends and family in receiving countries can use the cards to access cash and make purchases, without additional information being provided or existing information confirmed.

The Travelex Cash Passport card in Australia, for example, has a maximum card balance value (at any one time) of A$10,000; a maximum amount that can be loaded onto the card during any 12-month period of A$45,000; a 24-hour ATM withdrawal limit of A$6,000; and up to two cards able to be issued per Cash Passport fund.

Closed and semi-closed systems, conversely, are typically used for micropayments in view of their limited storage capacity. Such cards can be purchased without the need for any evidence of identification or prior account history.

In the same way that legitimate businesses will look at market forces and new opportunities for SVCs, criminals will also explore new areas that can be exploited to maximise their profits, and to evade the scrutiny of law enforcement agencies and regulators.

The widespread availability of SVCs (particularly at non-financial outlets), the high loading and card balance value limits of open system cards, and the anonymity offered by closed and semi-closed system cards could be abused by organised criminals for illicit financial transactions, money laundering and bulk cash smuggling, particularly as value limits increase. Stored value cards have been identified in several reports as a potential tool for organised crime groups to launder their illicit crime proceeds (APG 2005; US NDIC 2006). A study on cross-border electronic funds transfer systems raises similar concerns:

> In virtually every investigation of these groups, the movement of the proceeds of the criminal acts from the U.S. back to Canada, whether by movement of bulk cash, funds transfers, or stored value cards, has been significant (FinCEN 2007a: 100).

Money laundering concerns

Although the actual amount of money being laundered will never be known with accuracy, money laundering transactions in Australia are estimated to involve between $2b (Institute of Chartered Accountants 2006) and $4.5b per year (Walker et al. 2007). The International Monetary Fund has further suggested that money laundering transactions are approximately two to five percent of the global gross domestic product. Money laundering could, potentially, lead to a shift of economic power to organised crime groups, thus eroding Australia's political and social systems.

To disguise the origins of illicit proceeds, criminals can perform a series of business transactions such as transferring electronic currency through a series of offshore companies and purchasing goods for resale, prior to integrating the 'cleaned' proceeds into the legitimate financial system. The money laundering process is typically segmented into three stages:

- placement – in which illegal funds or assets are introduced into the financial system, or converted into monetary instruments (e.g. SVCs)
- layering – in which the illegal origins of placed funds are disguised
- integration – in which disguised funds are made available for investment in legitimate or illegitimate businesses.

Placement

In general, it is relatively easy to purchase SVCs, because customers do not generally require a bank account to acquire them. Applications for stored value cards can usually be accepted online, via fax or through non-financial outlets (e.g. local cheque-cashing outlets and convenience stores), which may not require any face-to-face verification of cardholder identity. Small to medium-sized non-financial distributors are also unlikely to have an adequate, or any, risk-based program based on the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (AML/CTF Act) in place, and may not carry out customer due diligence and have trained staff in the areas of money laundering detection.

In cases where face-to-face verification of cardholder identity is required, evidence of identity may be difficult to verify, particularly at non-financial

Events that may raise suspicions

- An excessively obstructive or secretive client.
- Customer asks questions or makes comments that raise suspicions (e.g. questions such as 'Will these purchases be reported to the authorities?').
- Large payments made in actual cash (especially if the cash is wrapped in currency straps).
- Customer purchases a large quantity of stored value cards, particularly reloadable open system or semi-open system cards, in an apparent effort to avoid triggering identification or reporting requirements – an activity also known as structuring.
- Customer purchases a large quantity of stored value cards of large denomination that is not commensurate with normal business activities.
- For open system card purchases at banks, customer makes a large number of stored value card transactions using the banks' services or third-party online payment systems, which appear inconsistent with the stated business activities.

distribution outlets (e.g. verification of a foreign passport at a convenience store). A criminal can, therefore, easily purchase large quantities of stored value cards (perhaps with different issuers) using cash generated from criminal proceeds, and it may then be possible to take these overseas without detection. Even if cards are located at entry ports, customs officials may be unable to ascertain how much value is loaded on each card.

Individuals can also be recruited by organised crime groups to purchase SVCs using stolen credit cards. These individuals ('card mules') may be recruited through email messages, websites or newspaper advertisements that purport to be legitimate businesses seeking new staff. One US case involved the arrest of a six-member syndicate in March 2007. Arrests were made by the Gainesville Police Department for allegedly using stolen credit cards to purchase large quantities of Wal-Mart and Sam's Club gift cards (US FDLE 2007).

Layering

Depending on the types of cards purchased during the placement stage, value can either be redeemed for merchandise or sent overseas.

Closed or semi-closed cards – These can be redeemed for merchandise. For example, in the arrests made by the Gainesville Police Department, the purchased cards were redeemed for merchandise such as computers, gaming devices and large-screen televisions (US FDLE 2007). The redeemed merchandise can either be sent overseas or resold and the proceeds remitted to third-party accounts (minus a commission).

Another recent US example involved the arrest of four Russians who, it was noted:

> [then transferred] the fraudulently-obtained money and goods back to Russia. ... Using stolen identity and credit information, defendant CHUGAEV made on-line purchases of PayPal cards, gift cards, computers, and other merchandise, and requested that the items be shipped to United States addresses under the control of his associates. Those associates quickly withdrew cash from the credit cards, then deposited the cash into bank accounts, and allowed CHUGAEV to withdraw the stolen money in Russia using ATM cards associated with the bank accounts. The computers and other merchandise were repackaged … in the United States and mailed on to Russia, where the stolen goods were resold (US DoJ 2007).

SVCs can also be 'purchased for currency and transferred from one person to another and resold [because beneficiaries' names are not required]. Often, a firm independent of a bank processes all card transactions through a "pooled" bank account held in the name of the firm managing the card program' (US FFIEC 2007: 206). The use of pooled accounts also increases the difficulty in monitoring any specific cardholder's activity.

Open or semi-open cards – Due to the worldwide acceptance of these cards (as most of the open system cards have access to the Plus and Cirrus/Maestro networks), card mules can be instructed to mail the purchased stored value cards to countries with lax anti-money laundering legislation where funds can then be withdrawn from local ATMs (including 'white label' ATMs – machines that offer only cash dispensing services). FINTRAC (2007: 24) pointed out that white label ATMs 'can be "self-loaded" with illicit funds, increasing the potential for money laundering. The involvement of organized crime was a key characteristic of disclosure cases involving white label ATMs this year'.

SVCs can also be easily taken through border controls because of their size – they are often in wallets, which may not be subject to scrutiny.

In another US case, the alleged mastermind of an international theft ring deposited money into several SVCs and sent six of the cards to Russia where his co-conspirators retrieved the money from ATMs (FinCEN 2007b: 25).

Events that may raise suspicions

- Customer makes payments using multiple payment methods or a large number of stored value cards.
- Customer purchasing pattern does not make economic sense (e.g. an individual customer pays for numerous laptops using several cards).
- The merchandise, particularly high-value and low-volume goods such as consumer electronics being shipped, appears inconsistent with the exporter's stated business activities or the merchandise is shipped to a jurisdiction designated as 'high risk' for money laundering activities.
- Stored value cards, particularly open or semi-open system cards (particularly with a large denomination), being sent through the post or found on travellers that appear inconsistent with the stated business activities (similar to bulk cash smuggling).

Integration

SVCs, particularly those used in open systems, can also be used as a means of payment by criminals. For example, precursor chemicals used in the production of illegal drugs, real estate investment, or life insurance policies could be paid for with SVCs.

SVCs can also be used as a means of payment for services rendered. In one case, a former employee of the Ohio Bureau of Motor Vehicles was prosecuted in connection with selling fraudulent Ohio drivers' licences in 2005. It was reported that she was paid using US$10 phone cards (US ICE 2005).

Legislative framework

The AML/CTF Act was enacted to enhance Australia's capacity to detect, prevent and combat money laundering, and to bring Australia in line with international best practice in detecting and deterring money laundering.

Designated services

The AML/CTF Act presently covers industry sectors with obligations under existing legislation, including the banking and finance sector, and other persons or businesses providing designated services. Industry sectors are considered 'reporting entities' under the AML/CTF Act when they provide 'designated services' defined in Section 6 of the AML/CTF Act. Although SVCs were not regulated under the *Financial Transaction Reports Act 1988* (Cth), issuing and reloading SVCs are now listed as designated services under the AML/CTF Act.

Entities providing designated services are subject to the full range of AML/CTF regulatory controls such as statutory reporting of suspicious activity, recordkeeping, and developing and implementing a risk-based AML/CTF program. As the main regulatory obligations under the AML/CTF Act are civil penalty provisions, non-compliance may attract a civil penalty (a fine up to A$2.2 million and A$11 million for individuals and corporations).

Section 81 of the AML/CTF Act requires all reporting entities to have an anti-money laundering and counter-terrorism financing (AML/CTF) program in place by 12 December 2007. The AML/CTF program includes general provisions concerning risk management and specific requirements concerning customer identification.

Banks and major financial institutions recognise the importance of sound ongoing customer due diligence policies and procedures (e.g. Know Your Customer) to reduce their *reputational risk* (e.g. maintain their brand and reputation in a competitive world market sensitive to the threats of international organised crime), *legal risk* and *financial risk*; and have monitoring systems in place to prevent exploitation of SVCs (e.g. monitoring of reloading above a threshold value).

In terms of customer identification at point of purchase or where value is reloaded onto SVCs, major banks and financial institutions employ technologies to detect forged identification documents and carry out enhanced customer due diligence for cardholders who reload SVCs frequently, have cash access and/or use their cards outside Australia.

In relation to monitoring SVC usage and detecting suspicious patterns or high-risk situations, real-time transaction monitoring using monitoring technologies is used. These technologies can be broadly categorised into:

- rules-based systems – assess individual transactions against a set of predefined rules based on value thresholds and other criteria
- pattern recognition systems – use sophisticated techniques such as neural networks, link analysis, peer group analysis, time sequence matching and name recognition technologies to monitor for a library of known patterns and scenarios
- hybrid systems – allow a combination of rules writing by monitoring against a library of known patterns.

Events that may raise suspicions

- Living standards of employees (or public officials) exceed their known lawful income or if they control or possess pecuniary resources or property, that are disproportionate to their present or past known sources of income, and when they are unable or unwilling to account for the discrepancy.
- Transactions incompatible with the customer's normal activity or are beyond the customer's apparent financial means are causes for concern (e.g. a lump sum payment for real estate or life insurance in cash).

Conclusion

To reduce the money laundering risk, SVC providers need to be aware of and comply with local regulatory requirements such as AML/CTF regulation, and prudential and financial regulations.

Compliance with these measures can, however, be challenging and expensive for SVC providers, although the potential legal liability and reputational risk for non-compliance can be significantly costly.

Tsingou (2005: 15) pointed out that '[t]he burden of compliance is more significant for smaller, local institutions, where "know your customer" and reporting requirements are less automated'. Prohibitive AML compliance costs, unlikely to be affordable by small to medium-sized non-financial distributors, might have the unintended consequence of driving the small players underground or driving providers (and users) of SVCs to less restrictive and less costly jurisdictions (regulatory arbitrage).

The process of disintermediation currently experienced in SVC programs (whereby physical contact between organisations and their clients is replaced by virtual contact) also compounds the challenge of customer identity verification at distribution outlets, particularly small to medium-sized non-financial distributors. Individuals in the unbanked sector may be unable to meet AML regulatory demands in terms of providing identification documentation such as passports or driving licences.

Reporting obligations

Anyone travelling into or out of Australia, or mailing/shipping currency, may have reporting obligations under Part 4 of the AML/CTF Act, with regard to cross-border movements of physical currency (carrying, mailing or shipping) and cross-border movements of bearer-

negotiable instruments (carrying). However, there are no reporting obligations in relation to the mailing or shipping of SVCs out of Australia. Illicit proceeds could, therefore, be smuggled out of Australia without regulators being aware (FinCEN 2007b: 25). Reporting obligations should, arguably, be extended to anyone mailing or shipping SVCs out of Australia to minimise risks of abuse by criminals.

The US government has recognised the potential for money launderers to exploit SVCs. On 24 July 2007, the Violent Crime Control Act of 2007 was introduced to the House by US representative, Lamar Smith, (http://www.govtrack.us/congress/billtext.xpd?bill=h110-3156) and the Senate by Senator John Cornyn (http://www.govtrack.us/congress/bill.xpd?bill=s110-1860). The Act includes a provision relating to SVCs. The text of the proposed provision, Section 338: Stored value cards (Section 5312(a)(3) of title 31, United States Code), states:

> ... the Secretary of the Treasury shall provide by regulation for purposes of sections 5316 and 5331, stored value cards or other similar devices including funds or monetary value represented in digital electronics format (whether or not specially encrypted) and stored or capable of storage on electronic media in such a way as to be retrievable and transferable electronically.

Linn (2008) pointed out that if the Bill is enacted, cross-border reporting obligations will be extended to anyone mailing or shipping SVCs out of the United States. A report would be filed each time an individual transports, mails or ships SVCs (having an aggregate value exceeding US$10,000) at one time into or out of the country.

Need for further research

To date, there are few reliable data on risks of this kind. This has resulted in a lack of well-developed research about money laundering using electronic payment systems such as SVCs, especially in comparison with other traditional banking systems. There is, therefore, a need to further analyse the SVC industry to determine possible ways in which the industry could be better regulated.

References

All URLs were correct at 20 June 2008

Abal R 2007. Rich opportunity in the unbanked segment. *Insight* 25: 1–6

American Express 2006. American Express enhances corporate gifting services to tap fastest-growing segment of burgeoning gift card market. *Media release* 24 October

Ames B 2007. *Online spending tops US$100 billion*. Computerworld.com.au 5 January

Asia-Pacific Group on Money Laundering (APG) 2005. *APG yearly typologies report 2004–05*. n.p.: APG. http://www.apgml.org/frameworks/default.aspx?FrameworkID=4

Australian Payments Clearing Association (APCA) 2005. *Annual report 2005*. http://www.apca.com.au/Public/apca01_live.nsf/WebPageDisplay/PUB_AnnualReport

De Young R 2001. The internet's place in the banking industry. *Chicago Fed letter* no. 163. http://www.chicagofed.org/publications/fedletter/2001/cflmar2001_163.pdf

Financial Crimes Enforcement Network (FinCEN) 2007a. *Feasibility of a cross-border electronic funds transfer reporting system under the Bank Secrecy Act*. http://www.fincen.gov/news_room/rp/files/cross_border.html

Financial Crimes Enforcement Network (FinCEN) 2007b. *The SAR activity review: trends, tips & issues*. 12 (October)

Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) 2007. *FINTRAC annual report 2007*. Ottawa: FINTRAC. http://www.fintrac.gc.ca/publications/ar/2007/menu-eng.asp

Institute of Chartered Accountants 2006. Money laundering worth up to 5% of global GDP. *Media release* 26 May

Linn CJ 2008. Regulating the cross-border movement of prepaid cards. *Journal of money laundering control* 11(2): 146–171

NovoPayment 2008. NovoPayment forecasts general purpose spending cards for Latin America's unbanked. *Media release* 10 June. http://www.businesswire.com/portal/site/home/permalink/?ndmViewId=news_view&newsId=20080610005833&newsLang=en

Payments News 2008. FSTC launches mobile technology initiative. *Media release* 3 June

Sloane T 2007. *4th Annual prepaid closed loop market assessment*. Boston, MA: Mercator Advisory Group

Tsingou E 2005. *Global governance and transnational financial crime: opportunities and tensions in the global anti-money laundering regime*. Coventry, UK: Centre for the Study of Globalisation and Regionalisation. http://www2.warwick.ac.uk/fac/soc/csgr/research/workingpapers/2005/wp16105.pdf

United States Department of Justice (US DoJ) 2007. Four Russians indicted in identity theft and fraud ring. *Media release* 1 March

United States Federal Financial Institutions Examination Council (US FFIEC) 2007. *Bank Secrecy Act/Anti-Money Laundering examination manual*. n.p.: US FFIEC. http://www.occ.treas.gov/handbook/1-BSA-AMLwhole.pdf

United States Florida Department of Law Enforcement (US FDLE) 2007. Arrests made in gift card fraud case totalling more than $8 million in losses. *News release* 19 March

United States Immigration and Customs Enforcement (US ICE) 2005. Prepaid cards an emerging threat. *The cornerstone report* 3(2): 4

United States National Drug Intelligence Center (US NDIC) 2006. *Prepaid stored value cards: a potential alternative to traditional money laundering methods*. 31 October

Walker J et al. 2007. *The extent of money laundering in and through Australia in 2004*. Canberra: Criminology Research Council. http://www.criminologyresearchcouncil.gov.au//reports/200304-33.html

Dr Kim-Kwang Raymond Choo is a research analyst in the Global, Economic and Electronic Crime Program at the Australian Institute of Criminology.

General editor, *Trends & issues in crime and criminal justice* series: Dr Judy Putt, General Manager, Research, Australian Institute of Criminology, GPO Box 2944 Canberra ACT 2601
Note: *Trends & issues in crime and criminal justice* papers are peer reviewed.

The AIC is a statutory body with a Board of Management comprising Australian, state and territory government representatives, administered under the *Criminology Research Act 1971*.