2008

Risk Mitigation Strategies for the Prepaid Card Issuer in Australia

M A. Khairuddin
RMIT University

P Zhang
RMIT University

A Rao
RMIT University

DOI: 10.4225/75/57b56360b876f
Originally published in the Proceedings of the 6th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 1st to 3rd December 2006.

Risk Mitigation Strategies for the Prepaid Card Issuer in Australia

M. A. Khairuddin, P. Zhang and A. Rao
RMIT University
m_khairuddin@student.rmit.edu.au, p.zhang@student.rmit.edu.au,
asha@rmit.edu.au

Abstract

The prepaid card market in Australia is growing rapidly. Its features not only attract customers from all sorts of backgrounds but also expose it to numerous risks. Using the methodology of the Australian Risk Management Standard AS/NZS4360, this paper looks at the risks inherent in prepaid cards. Concentrating on two major risks, the paper details the regulations governing the industry in the USA as well the technical controls employed by the credit/debit card industry. We suggest risk mitigation strategies from these two view-points, aiming to become an important reference both for industry as it adopts better risk mitigation techniques, and for government as it improves the laws and regulations governing this industry.

Keywords

Prepaid cards, open-loop, closed-loop, money-laundering, fraud

INTRODUCTION

All market research points to continued growth in the prepaid card market. Anonymity and bank-less transactions are the main attractors giving prepaid cards the potential to capture a wide range of customers including the unbanked sector such as students and immigrants. To be able to exploit this growth, prepaid card issuers will need to install appropriate controls to manage and mitigate the inherent risks and to create a secure and trustworthy environment for prepaid cards to flourish. This paper presents two important controls – that of policy requirements and currently available technical means to help mitigate the two important risks of card fraud and money laundering.

According to a press release by Packaged Facts (2008) the sales of gift cards is expected to increase over the next five years by nearly US$14 billion, a part of an overall US$81 billion market for prepaid cards in the USA. Similarly Williams (2007) states that by 2010, there will be around 375 million prepaid cards in Europe, a 1,000% increase on 2005, with prepaid card usage rising 600% to €75 billion. Jackson from Travelex (2007) says that in 2007 the demand for prepaid travel cards (Cash Passports) in Australia increased by 50% with more than 600,000 Australian Cash Passports currently in circulation, while Braue (2007) reports that the Commonwealth Bank has been "pushing 60,000 PayPass prepaid cards into the Australian market every month". Clearly from these statements and figures, the demand and sales of prepaid cards is exploding and consequently, the need for clear and concise risk mitigating controls in terms of policies and technical requirements is becoming paramount.

There are two types of prepaid cards: Closed-loop or retailer specific cards are prepaid cards that can only be used in a specific area and have limited purpose. Examples include gift cards (MYER and COLES Group cards) and prepaid phone cards (Telstra and Optus). Open-loop or network branded cards are prepaid cards that utilize the VISA or MasterCard payment network as the means of business transactions, and normally the logo of either one of the service providers (SP) is embedded on the card as a symbol of acceptance and trust. Open-loop cards allow the customer to engage in numerous financial activities including purchasing from any store as well as withdrawing money through POS and ATM, provided both the stores and the ATM accept the SP.

The focus of this paper will be the usage of gift cards and prepaid credit/debit cards as representatives, respectively, for the closed-loop and the open-loop prepaid card market. The methodology of the Australian Risk Management Standard AS/NZS4360 was the basis of this risk management exercise.

The first step in AS/NZS4360 is establishment of the context and identification of the stakeholders – related parties that determine and influence the direction and workings of the industry. These stakeholders include:

- The Customer – the user of prepaid cards

- The Issuer – companies that issue the prepaid cards. For example CANVAS & Cuscal BOPO (Australia), Bancorp Bank Eufora & RUSHCARD (USA) and Cashplus (Europe)
- The Service Provider (SP) – payment networks that handle the clearance and settlement of transactions such as VISA, MASTERCARD and AMEX
- The Distributor – companies or 3rd party organizations that manage the distribution of the cards such as a retail store or the post office.
- Merchants – basically any store that accepts the SP

Even though this discussion will briefly touch on all of the above parties, the focus will be on the responsibilities of prepaid card issuers, because we believe the task of mitigating the risks associated with prepaid cards lies mainly with the card issuer. However this does not alleviate the responsibility of the other stakeholders, as the security of prepaid cards should be borne by all of them. We hope to address the responsibilities of other stakeholders in a future paper.

The process of establishing the context is followed by the identification of the risks. The known risks in the prepaid card market are basically similar to those that affect other financial payment methods including traditional cash and cheque transactions, as well as credit and debit cards. In order to limit the focus of this paper, the discussion presented will be restricted to two major risks:

- Money Laundering – a process that involves taking illegal money and moving it through a legitimate financial system so as to disguise its criminal nature and origin. Prepaid card issuers are obligated to report to Government under the AML/CTF Act 2006 since they provide a "designated" service and non-compliance could result in civil penalties of up to AU$11 million for a body corporate and AU$2.2 million for individuals.
- Card Fraud – includes using stolen cards or accounts to purchase goods and services, data alteration on cards, skimming and counterfeiting cards and malicious threats involving internal accomplices.

This paper will present existing regulations and currently available technical controls governing the usage and working of prepaid cards especially in the USA market. We will then provide the necessary comparison and suggestions with respect to the Australian prepaid card market. Finally, in the conclusion we will give the risk mitigation controls which we believe will help issuers provide a more secure arena for the expansion of prepaid cards.

REGULATIONS

In this section we look at the laws, regulations and policies governing the prepaid card market. These regulations, while also decreasing the likelihood of fraud, are aimed at providing a just market and fair-trading. We will look first at the regulations existing in the USA as the prepaid card market is more mature there.

Regulations in the USA

The USA has seen a huge growth in gift cards in the last few years. This growth has driven legislatives to propose or revise laws regulating this market. However, these state-based laws vary widely, and, even more interestingly, are often conflicting: some states permit expiration date with reasonable disclosure on the card, while others require minimum period before expiration, and still others strictly prohibit expiration date (Lorentz 2008, Consumers Union 2008).

Very similar to expiration date, fees are permitted with adequate disclosure in some states, and they can be applied after a certain period of time in another 7 states. Still other states either have very strict restrictions on fees or explicitly prohibit all fees. Abandoned Property Laws (aka escheat laws) also need to be adhered to (Lorentz 2008, Consumers Union 2008).

With disclosure as described above, the Office of the Comptroller of the Currency (OCC) Bulletin 2006-34 states that the expiration date, fees, card value etc have to be explicitly disclosed on the card both at purchase as well as at gift card recipient side (OCC 2006 only applies to gift cards as stated in its scope). This bulletin also covers the disclosure issue at promotional activities, where usually only the word "discount" is mentioned, but no mention is made of "commission fee" even if it exists. In all, disclosure is aimed at maximizing transparency on purchaser side. Thus, gift cards in the USA are regulated mainly under collaboration with state laws and disclosure regulations.

Since most open-loop prepaid cards are financial institution (FI) branded, they have a direct relationship with FIs and are subject to policies within FIs. However, laws and regulations for credit cards and debit cards cannot be applied to open-loop prepaid cards. In the USA as there is no unique law for open-loop prepaid cards, they have to comply with Regulation D, Regulation E, FDIA etc. As Rinearson (cited in Furletti 2004) says, "Prepaid cards are at an intersection of multiple kinds of laws."

By the definition of "deposit" in Regulation D open-loop prepaid cards and their issuers are considered as "deposit" and "depository institution" respectively. However, only financial institution issued prepaid cards, mostly open-loop prepaid cards, are considered as "deposit" by the Federal Deposit Insurance Act (FDIA) whilst all merchant issued prepaid cards (gift cards) are excluded. Thus FI issued prepaid cards are insured by FDIC against risk of loss through bank or thrift failures (Furletti 2004) while merchant issued ones are not.

As almost all open-loop prepaid cards possess ATM and on-line transaction functionalities they fall into the Electronic Funds Transfer Act (EFTA) under the definition of "account" and therefore, consumers are provided protections, rights, liability limits and error resolutions from issuers (Furletti 2004). Regulation E says much the same thing as EFTA (Furletti 2004).

It is interesting to look into the relationship between the Patriot Act and prepaid cards. Due to the anonymity of most prepaid cards, (the identity of users cannot be ascertained), the Patriot Act would seem to have nothing to do with prepaid cards. But as the article in BusinessWeek.com suggests - ". . . they're ready tools for thieves, drug rings - even terrorists" (Dawson 2005) and as Semesky (quoted in NTARC 2007) points out "It is a great concern . . . because of the terrorist financing angle," there exist serious concerns about prepaid cards being used as tools for terrorist activities. Clearly, although there is an issue with terrorism, currently there is no law in place to deal with this matter.

Money laundering is another issue related to prepaid cards as the anonymity could make them a preferred tool for criminals (USDOJ 2006). In addition prepaid cards are considered the "best" (Archer 2007) way to transfer money abroad making money laundering activities convenient. But it is still unclear whether prepaid cards are actually involved, as, for example the approximately US$600 million laundered cash seized by the DEA in 2006 turned out to have no suspected connections with prepaid cards (Derman 2007).

Australian Regulations

The Prepaid card market in Australia is relatively in its infancy when compared to the USA market, but regulations here are no less "fragmented" (Bollen 2004).

Officially, prepaid cards in Australia are recognised under the Australian Securities and Investments Commission (ASIC). Prepaid cards are classified as "non-cash payments" (Adams 2004) in much the same way as electronic cash, direct debit, travellers' cheques and so on. According to the Corporations Act (2001), ASIC licenses issuers and distributors of "non-cash payment facilities". The Reserve Bank of Australia (RBA) supervises the whole payment system (Bollen 2004).

Unlike the USA, Australia has no separate laws and regulations for closed-loop and open-loop cards.

The disclosure of fees, expiration date etc. are regulated by the Corporations Act (2001) and is issuer and distributor oriented (Bollen 2004). In Australia the Product Disclosure Statement (PDS) takes the place of the OCC bulletin of the USA but also proposes the disclosure of related risks (Bollen 2004). Additionally, the Social Security and other legislations amendment act 2007 stipulates that for stored value cards issued by the government, the monetary value of the card must remain unchanged until the legitimate recipient starts to use it and that these cards may contribute to personal income regime. However, there is no law regulating fees or the expiration date in Australia. Consumer rights are protected by the ACCC.

For the open-loop prepaid card, the Banking and the Electronic Funds Transfer Codes of Conduct exercise the same authority as the EFTA (Furletti 2004) and Regulation E of the USA. While there is no FDIC in Australia, deposit institutions are supervised by the Australian Prudential Regulation Authority (APRA) in collaboration with the RBA (Bollen 2004).

Proposed Policy Requirements for Gift Card Issuers

As mentioned above, regulations regarding fees and expiration date for close-loop prepaid cards are quite ambiguous in Australia. Therefore, consumers may incur losses from either hidden charges or cards expiring inadvertently. Here is an indication of policy regulations which would aid in transparency to purchasers and bring prepaid card regulations in Australia at par with the USA. These regulations would definitely provide a more trustworthy environment for prepaid cards.

Considering the trade-off between business and customer rights, we suggest that fees be prohibited for all closed -loop prepaid cards. On the other hand the expiration date may remain as a discretionary item. It could be applied for cards of monetary value more than a certain level (maybe AU$20) with expiration date no less than 3 years. Information about fees and the expiration date (if applicable) should be disclosed at promotional activities and at the time of purchase as well as after purchase on available media (gift card package, advertisements, website, help line etc).

The reasoning behind our suggestions is as follows: small-value gift cards are relatively more common than large-value cards; since monetary value is small cards may easily be forgotten and expire inadvertently. Expiration dates could apply to cards of value over AU$20, as on the one hand people are probably more aware of cards of higher value, and on the other hand, expiration date does encourage consumers' purchases in the favour of merchants. Above all, ensuring that the monetary value on a card is the same at the time of first use as at the time of purchase is paramount. Disclosure has to be thorough, accurate and proper throughout the entire lifetime of every single gift card covering issuer information, value, expiration date (if appropriate), fees (if fees are charged), where and how to use the card, error resolution, how to record a complaint etc. All gift card sales and after purchase customer services should be included in the annual audit.

Merchants should take the responsibility of monitoring the purchase of gift cards. Due diligence for issuers should include the setting of purchase limits (10 cards or up to AU$500) for individuals and credit checks for bulk purchase of gift cards (over 10 cards or total value over AU$500).

Money laundering is a very serious issue as discussed above. It usually takes place across borders. An online search on open-loop prepaid cards came up with a large number of reloadable and anonymous prepaid cards with labels of Visa, MasterCard and Maestro around the world that cardholders could use to launder money at any place on the planet where services are provided. Thus, the licensing of issuers is very important. All open-loop prepaid card issuers in Australia should be limited to banking or similar regulated institutions just as in the UK (Bollen 2004). Meanwhile, monetary limit for all open-loop prepaid cards should be AU$500, but can be greater if the cardholder is willing to undergo an identity check. Issuers should monitor all card accounts on initial values, purchases, overseas activities, reloads etc. Issuers may be given the right to temporarily freeze an account if that account is suspected of money laundering until the cardholder can provide evidence of certain financial activities. All prepaid card values and monitoring management need to be recorded in the annual audits.

Our introduction of an "AU$500" limit is inspired by the Travelex "Cash Passport", which sets a limit of AU$500. Whereas Travelex does not support any monetary value above this limit, we believe that such a position could lead to the loss of genuine customers. Thus issuers need to keep the limit flexible, and customers who wish to avail of the higher amounts must be willing to undergo conventional registration in order to prevent the cards being put to malicious use. Further AU$500 and 10 cards limit (remembering that closed-loop cards have less monetary value and are assumed to range from AU$30 to AU$50) is set with the aim of maintaining a balance between investment on security by issuers and mitigation of card fraud. On the one hand security measures are costly to deploy and could outweigh the profits brought by prepaid cards. Small value losses such as a small number of AU$500 losses could feasibly be acceptable to issuers who do not wish to spend on advanced security solutions. On the other hand, since AU$500 bonds with anonymity, the limit could act as a strong fence to deter money laundering and card fraud as these activities typically require both bulk monetary value and anonymity.

TECHNICAL SOLUTIONS

There are many factors that attract customers to prepaid cards, two of which are that a prepaid card provides a sense of anonymity and is able to cater to the needs of the unbanked customer who is either not eligible or does not want to have an account with a financial institution. Javelin Strategy & Research (2008) defines unbanked as those that have neither a checking nor a savings account with a bank or credit union. However, by offering anonymity to its customers and opportunities for unbanked customers to perform financial activities without proper control, the market is exposed to numerous financial and operational risks.

Money laundering and card fraud are two of the most common risks associated with the use of prepaid cards. Anonymity implies that the purchase of prepaid cards does not require any registration and no transaction is monitored or recorded, which could lead to severe consequences. Sienkiewicz (2007) points out that the risk of money laundering is excessive in an environment where the prepaid card system does not necessitate the need to identify and monitor its customers.

Unbanked customers, besides comprising of students and immigrants, may also extend to individuals with bad credit or financial history as well as criminals. According to Smith and Grabosky (1998), about 40% of

worldwide plastic card counterfeiting is being carried out by Asian organized crime. Even though these attacks are more prevalent in credit and debit card markets, clearly with the increase in customer acceptance and diversification of use, the probability of prepaid cards being exploited for fraud will increase.

To deter and minimize the likelihood and consequences of both risks, necessary measures have been adopted and applied in the market. It is interesting to observe that the technical measures currently being adopted by issuers in combating the above risks are basically similar to solutions being used in the more mature credit and debit card markets. These provide issuers with the preliminary tools to assist them in implementing and maintaining a secure, reliable and trusted environment for prepaid cards. We present a brief outline of these measures below.

Use of Existing Payment Card Security Guidelines for Prepaid Cards

At present it is common practice for prepaid card issuers to conform the security controls of their system to requirements laid down in existing PCI DSS (2008) guidelines. This comprehensive guideline, developed by the Payment Card Industry Security Standards Council, was initially intended to secure the environment of the credit and debit card markets. Looking into the current version of PCI DSS, the requirements are more towards strengthening internal controls and providing the necessary protection of customer data within the environment of the issuer itself, thus indirectly making it hard for external parties to carry out malicious attacks and inflict threats. It requires issuers to setup appropriate network perimeter controls, install encryption and data protection and establish proper physical and logical access controls. Periodically, issuers also need to engage a certified assessor to audit their compliance.

Methods currently available for Detecting and Preventing Fraudulent Transactions

System wise, there are many ways for issuers to detect and prevent fraud. The success rate of these methods depends on the ability of the system to determine the nature of the monitored financial activities. This monitoring can be done either based on filtering (the use of black and white list) or rule-based algorithms (Oscar Kilo 2006). Leading fraud management companies such as Retail Decision (2008) and ACI Worldwide (2008) prefer the use of the rule-based techniques in their fraud detection software as they believe it is flexible enough to allow customization depending on the preferences of the issuers. The detection capabilities of these systems, especially the application of neural networks in the card payment industry, have been tested and the results are reportedly equivalent to human experts (Bose 2006).

Finally, with the emergence of new ways of committing card fraud, detection alone is not enough to resolve the threat of fraud. To minimize and discourage counterfeiting and skimming thus preventing any fraudulent transactions, card design typically includes some preventive elements. For example, the prepaid open-loop VISA branded card includes 3D Dove hologram and PIN security code for ATM withdrawal.

Technical Suggestions for Australian Issuers

Current controls adopted by prepaid card issuers especially in the USA, such as PCI DSS guidelines (2008) and fraud detection software, are believed adequate and efficient in detecting and preventing both money laundering and card fraud. However, these solutions are more suitable for the credit and debit card market, where the background of the customers are meticulously checked and verified, and their activities are constantly monitored and recorded.

It is difficult to attempt to resolve the issue of money laundering by creating a system that detects and prevents it from happening, mainly because money laundering activities do not have any damaging effect on the system and have no harmful effect on the user or the usage of prepaid cards. The act of money laundering as discussed before is an act of disguising the origin, the placement and the movement of the criminal transaction such as purchasing and using the prepaid card. However, from the aspect of legality and society, money laundering is a crime and entities are obligated to monitor for it and report it.

Consequently, to mitigate the risk of money laundering and card fraud especially in the Australian prepaid card market, we suggest that:

- The registration of customers be enforced, depending on the usage and monetary value of the prepaid card especially open-loop cards. This registration must at least contain the information related to the background of the customer such as name and occupation.
- Patterns and relevant information pertaining to money laundering and fraud such as information about identified culprits and their usage patterns be shared between Australian issuers. This should be in real

time as it would help in detecting and preventing any attempt of laundering or card fraud immediately and efficiently.

- Preventive elements on prepaid cards should follow the same elements existing on credit/debit cards such as signature and holographic magnetic stripe. Further more, we do believe it is beneficial for Australian prepaid issuers to use smartcards as this would not only make the prepaid card more secure but also enhance its usability and functionality.

We acknowledge that any changes concerning technical solutions on current systems would require careful and extensive work on the part of the issuer. One of the major drawbacks resulting from the implementation of all of the above recommendations is cost. Initial spending on the integration of fraud detection systems between issuers and the inclusion of strong preventive elements or smartcards would be enormous. Nonetheless, as the prepaid card market grows more secure and stronger as a result of these measures, the expenses would in long term be covered.

Another possible downside would be accusations of breach of privacy of the customers due to the enforcement of customer registration and sharing of monitoring information between the issuers. It is important during the preliminary planning stage for issuers to work closely with relevant government bodies. Policies relating to registration and monitoring should be audited and verified by independent experts. Moreover, issuers could also provide appropriate clarifications to the public on their intention and the measurements taken to achieve it.

In summary, the risks affecting prepaid cards are basically similar to the credit/debit card market. Even though the monetary value is low, due to the current features of the cards, the likelihood is quite high. Without proper strategic controls, the consequences of each malicious incident could prove to be severe.

It is not wise to believe that any solution, regulatory and technically, is enough to ultimately restrain and deter the threats related to the prepaid card market, especially the risks of money laundering and card fraud. The effort and research into ways to handle and mitigate risks and overcome threats that are constantly changing need to be continuous and constant.

CONCLUSION:

The prepaid market in Australia is projected to grow at a steady pace. To facilitate this growth it is important that prepaid card issuers consider certain risk mitigation strategies to reduce the two important risks of card fraud and money laundering. Whereas card fraud leads to a direct impact on profits for card issuers, the need to prevent money laundering is dictated more by the laws and regulations set by the Australian Government. Having conducted a risk management exercise on prepaid cards using the methodology suggested in AS/NZS4360, we believe that the best way to mitigate these two risks is via regulations and technical means.

With regards to regulations the most essential aspect is the licensing of issuers. Therefore we propose,

- All closed-loop prepaid card issuers should be licensed by APRA, ASIC or related government departments.
- Only financial institutions should be allowed to issue open-loop prepaid cards.

But these regulations are of course in the realm of government. To enable issuers to be proactive we suggest that they implement relevant policies, such as:

Closed-loop prepaid card issuers should

- Record the sales of all closed-loop cards in the annual audit.
- Prohibit the bulk purchase of closed-loop cards (over 10 cards a time) unless the purchaser is prepared to have the purchase recorded along with identifying details.
- Perform due diligence by training their sales representatives to control the sales limit stated above.

Open-loop prepaid card issuers should

- Monitor all financial activities of cards and document them for audit purposes.
- Freeze suspicious accounts until adequate proof of financial activity is submitted.
- If proof is not presented, issuers should promptly report these accounts or entities to AUSTRAC.

The policy statements above need to be coupled with technical controls as often this is the only means of implementing them. These technical controls would include

- Conforming to the PCI DSS security guidelines.
- Installing fraud detection and monitoring systems.
- Including fraud preventive elements on the card.

These controls are, of course more suitable for traditional card payment schemes (credit/ debit card), since in that case the customer background is thoroughly checked and verified, and the card activities are constantly monitored and recorded. Based on the above premises and for the benefit of Australian card issuers, we do strongly propose that,

- Registration of customers should be mandatory for higher value cards and should include at the very least, name, current address and occupation.
- Card usage should be monitored and any anomalies should be shared among card issuers in real time. This would enable detection of cases when a customer goes to many different geographically-close locations and purchases the minimum number of cards.
- Additional preventive elements such as signature or smart chips should be added to the prepaid card itself making it less prone to fraud and misuse.

Clearly there is still work needed in this area. For example, customers need to be aware of their responsibilities as well. Thus possible future work could include:

- Feasibility studies on the recommendations presented in this paper.
- Prepaid card risk mitigation strategies for customers.

REFERENCES:

ACCC Australian Competition and Consumer Commission. URL. http://www.accc.gov.au/content/index.phtml/itemId/142

AML/CTF Act (2006) Anti-Money Laundering and Counter-Terrorism Financing Act 2006, Commonwealth of Australia Law, URL. http://www.austrac.gov.au/aml_ctf.html

ACI Worldwide, Inc. (2008), ACI Prepaid Solutions Flyer. Product Information, URL. http://www.aciworldwide.com/pdfs/ACIPrepaidSolutionsFLUS3577.pdf

Adams, M. (2004) ASIC and the regulation of non-cash payment products, *Cards Australia Conference*, URL. http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/Cards_Australia_speech_050804.pdf/$file/Cards_Australia_speech_050804.pdf

Archer, F. (2007) Pre-pay may be best way when moving money overseas, *The Daily Telegraph*, 24th March 2007, URL. http://www.telegraph.co.uk/global/main.jhtml?xml=/global/2007/03/24/cmoverseas24.xml

Braue, D. (2007) MasterCard cash replacement makes Aussie debut, *ZDNet Australia*, 26 November 2007, URL. http://www.zdnet.com.au/news/communications/soa/MasterCard-cash-replacement-makes-Aussie-debut/0,130061791,339284060,00.htm

Bollen, R. (2004) Regulation of Payment Facilities, *MurUEJL 28, Murdoch Uni. Elec. J. Law*, Volume 11, Number 3, URL. http://www.austlii.edu.au/au/journals/MurUEJL/2004/28.html

Bose, R (2006) Intelligent Technologies for Managing Fraud and Identity Theft, *ITNG'06: Proceedings of the Third International Conference on Information Technology: New Generations*, IEEE Computer Society, Washington DC, USA. pp 446–451. doi = http://dx.doi.org/10.1109/ITNG.2006.78

Consumers Union (2008) State Gift Card Consumer Protection Laws, URL. http://www.consumersunion.org/pub/core_financial_services/003889.html

Commonwealth Consolidated Acts - Corporations Act 2001, URL. http://www.austlii.edu.au/au/legis/cth/consol_act/ca2001172/

Dawson, C. (2005) Prepaid Cards: Candy for Criminals? 12 December, 2005, *Business Week*, URL. http://www.businessweek.com/magazine/content/05_50/b3963115.htm

Derman, B. (2007) Watching the Anti-Money Laundering Risk in Prepaid Cards, *American Bar Association, Section of Business Law, Spring Meeting* 15 March 2007, URL. http://www.glenbrook.com/2007/03/watching_the_an.html

DEA Drug Enforcement Administration, US Department of Justice, URL. http://www.usdoj.gov/dea/

FDIA, Federal Deposit Insurance Act, Federal Deposit Insurance Corporation, URL. http://www.fdic.gov/regulations/laws/rules/1000-100.html

Furletti, M. (2004) Prepaid Cards: How Do They Function? How Are They Regulated? *Prepaid Card Conference*, 2-3 June, 2004, URL. http://www.philadelphiafed.org/pcc/conferences/2004/PrepaidCards_062004.pdf

Javelin Strategy & Research (2008), Underbanked/Unbanked Opportunity, First Data Corporation, URL. http://www.firstdata.com/about/whitepapers/WP13_Unbank_Underbank.pdf

Jackson, P. (2007) ReD fraud prevention added to Travelex cash passport, 13 September 2007, URL. http://www.itwire.com/content/view/14438/545/

Lorentz, A.J. (2008) Disclosure for Prepaid Cards Program: An overview of rules, The American Conference Institute's Prepaid Card Compliance conference, 17 June 2008, URL. http://www.wilmerhale.com/files/Publication/7af95c8d-2b8c-4804-9c82-2a4204a76c59/Presentation/PublicationAttachment/a609010a-f44a-47a4-a00e-31f844686980/PrepaidCards_Lorentz.pdf

NTARC National Terror Alert Response Center, (2007) New Tool For Terrorists - Prepaid Gift Cards, 5 October 2007, URL. http://www.nationalterroralert.com/updates/2007/10/05/new-tool-for-terrorists-prepaid-gift-cards/

OCC bulletin, (2006) Comptroller of the Currency, Administrator of National Banks, US Department of the Treasury, 2006-34, 14 August 2006, URL. http://www.occ.treas.gov/ftp/bulletin/2006-34.doc

Oscar Kilo Ltd, (2006) Fraud Detection Technical Comparison of Methods, Whitepaper, URL. http://www.oscarkilo.net/whitepapers/DETECT-TechniquesReview.pdf

Packaged Facts, (2008) Gift Card Market Expected to Grow 5%, Exceeding $52 Billion by 2012, 9 January 2008, URL. http://www.packagedfacts.com/about/release.asp?id=1035

PCI Security Standards Council, (2008) URL. http://www.pcisecuritystandards.org/index.shtml

Retail Decisions, Inc. (2008), CNP Fraud Prevention – ebitGuard, Product Information, URL. http://www.redplc.com/documents/ebitGuard.pdf

Regulation D, The Federal Reserve Board, URL. http://www.federalreserve.gov/Regulations/#d

Regulation E, The Federal Reserve Board, URL. http://www.federalreserve.gov/Regulations/#e

Sienkiewicz, S.J. (2007) Prepaid Cards: Vulnerable to Money Laundering? *Federal Reserve Bank of Philadelphia Payment Center Discussion Paper* No. 07-02, URL. http://ssrn.com/abstract=969042

Smith, R.G. and Grabosky, P. (June 1998). Plastic Card Fraud. *Crime Against Business Conference*, Australian Institute of Criminology, URL. http://www.popcenter.org/problems/credit_card_fraud/PDFs/Smith&Grabosky.pdf

Social Security and other Legislation Amendment (Welfare Payment Reform) Act 2007 (No. 130, 2007) - Schedule 1, Commonwealth Numbered Acts, URL. http://www.austlii.edu.au/au/legis/cth/num_act/ssaolapra2007674/sch1.html

USDOJ (2006) United States Department of Justice, Prepaid Store Value Cards: A Potential Alternative to Traditional Money Laundering Methods, URL. http://www.usdoj.gov/ndic/pubs11/20777/20777p.pdf

Williams, K. (2007), The Potential of Prepaid: A World of Benefits, URL. http://www.efunds.com/web/pdf/EFDThePotentialofPrepaid.pdf

COPYRIGHT