Prepaid Cards: Vulnerable to Money Laundering?

Stanley Sienkiewicz*

February 2007

Summary: *This paper discusses the potential money laundering threat that prepaid cards face as they enter the mainstream of consumer payments. Over the past year, several government agencies have issued reports describing the threat to the U.S. financial system, including the use of prepaid cards by money launderers. Also, this paper incorporates the presentations made at a workshop hosted by the Payment Cards Center at which Patrice Motz, executive vice president, Premier Compliance Solutions, and Paul Silverstein, executive vice president, Epoch Data Inc., led discussions. These two leading anti-money laundering strategists explained how money laundering occurs in financial payments and how firms can mitigate and detect money laundering activities. This paper provides an overview of money laundering, describes how prepaid cards could be abused, and outlines how both the government and the payment sectors have responded to mitigate risks.*

* Payment Cards Center, Federal Reserve Bank of Philadelphia, Ten Independence Mall, Philadelphia, PA 19106. E-mail: stan.sienkiewicz@phil.frb.org. The views expressed here are not necessarily those of this Reserve Bank or of the Federal Reserve System.

FEDERAL RESERVE BANK OF PHILADELPHIA

Ten Independence Mall, Philadelphia, PA 19106-1574 • (215) 574-7220 • www.philadelphiafed.org/pcc

I. Background and Introduction

Prepaid cards are one of the newer developments in the world of consumer electronic payments. Beginning as an electronic replacement for paper gift certificates, so-called gift cards have become especially popular with consumers and marketed aggressively by retail merchants. Recent innovations to prepaid cards have incorporated the same pre-funding characteristic but are integrated into the Visa, MasterCard, and other payment card networks, significantly expanding the range of applications beyond the simple gift card concept. These network-branded prepaid card programs are now gaining traction as attractive alternatives for traditional paper-based solutions such as payroll payments, cross-border remittances, government assistance programs, and many other emerging applications.

A number of observers have also emphasized the potential that prepaid card applications have for more efficiently and effectively delivering financial services to the unbanked and underserved segments of society. Unfortunately, many of the same features that make prepaid cards such a positive payment innovation have also attracted criminals interested in exploiting this new payment form to facilitate money laundering.[1]

The United States government officially documented its concern in a report published in late 2005, entitled the *Money Laundering Threat Assessment (MLTA)*.[2] The report was the product of an interagency working group that consisted of subject matter experts from the Department of the Treasury, Department of Justice, Department of Homeland Security, Board of Governors of the Federal Reserve System, and the United States Postal Service.[3] The material

---

[1] Ethan Zindler, "Prepaid Cards Give Rise to Laundering Concerns," *American Banker*, November 7, 2005; and Richard Mitchell, "Under Scrutiny: Regulators Are Keeping a Watchful Eye on the Possible Misuse of Prepaid Cards," *Intele-CardNEWS*, April 2006.

[2] http://www.ustreas.gov/offices/enforcement/pdf/mlta.pdf

[3] Contributors to the report include from Treasury: the Office of Terrorist Financing and Financial Crime, the Financial Crimes Enforcement Network, the Office of Intelligence and Analysis, the Office of Foreign Assets Control, Office for Asset Forfeiture, IRS Criminal Investigation Division, and the IRS Small Business/Self Employed Division; from Justice: the Federal Bureau of Investigation, the Drug Enforcement Administration, the Asset Forfeiture Money Laundering Section of the Criminal Division, the National Drug Intelligence Center, and the Organized Crime Drug Enforcement Task Force; from Homeland

presented in this 72-page document addresses 13 channels through which money launderers may take advantage of the U.S. financial system. Significantly, one section of the *MLTA* is devoted to the threats presented by prepaid cards. That section, titled "Stored Value Cards," identifies a number of vulnerabilities particular to prepaid cards, including the cross-border features of some prepaid cards that allow a person to use a foreign-issued card in the United States and a U.S.-issued card outside the United States. The *MLTA* emphasizes that the money laundering risk associated with prepaid cards lies in their easy transportability and the relative ease of moving and potentially accessing monetary value anonymously. The report further notes that prepaid card programs that do not require customer identification or that do not include rigorous monitoring of suspicious activity are most at risk for money laundering abuse.

In October 2006, the U.S. Department of Justice's (DOJ) National Drug Intelligence Center (NDIC) released a separate report on its view of the potential vulnerability of prepaid cards to money laundering. The DOJ report took a more aggressive position than the *MLTA*, stating that prepaid cards "provide an ideal money laundering instrument to anonymously move monies associated with all types of illicit activity." It concluded, "Due diligence procedures required of financial institutions…should be applied to prepaid stored value cards because open and semi-open system prepaid stored value cards are used in a manner that approximates a traditional checking account." [4]

In addition, in late 2006, the Financial Action Task Force (FATF)[5] released its "Report on New Payment Methods," which reviews prepaid cards and other new payment methods that

---

Security: Immigration and Customs Enforcement and Customs and Border Protection; and from the Postal Service: the United States Postal Inspection Service.

[4] The Network Branded Prepaid Card Association wrote a letter to the NDIC director outlining what the association believed were misconceptions and omissions in the report. The letter can be viewed at http://www.nbpca.com/docs/NBPCA-NDIC.pdf.

[5] The Financial Action Task Force on money laundering was organized by the G-7 countries in 1989 and now comprises 33 member countries plus the European Commission and the Gulf Co-operation Council. Its purpose is to develop national and international policies to combat money laundering and terrorist financing. See http://www.fatf-gafi.org.

allow for electronic cross-border fund transfers that might also facilitate money laundering. [6] Examining the structure of prepaid card processing, the FATF highlighted programs that incorporate offshore card issuers and access to cash at ATMs as environments with the greatest risk for money laundering abuses. Concurrently, the private-sector side of the payments industry is also actively examining these same issues in an attempt to better understand prepaid cards' vulnerability to abuse by money launderers and to develop appropriate risk mitigation strategies. [7]

To help us understand the issues, the Payment Cards Center hosted a workshop discussion led by Patrice Motz, executive vice president at Premier Compliance Solutions, [8] and Paul Silverstein, executive vice president at Epoch Data Inc. [9] Both are leading experts in anti-money laundering compliance and related matters. Motz and her firm help clients to identify and evaluate money laundering and terrorist financing vulnerabilities and to implement appropriate risk mitigation strategies. Silverstein and his firm specialize in providing technology solutions to control money laundering, fraud, and risk. Motivated by the workshop discussion, this paper describes how money laundering takes place, explores prepaid cards' vulnerability to criminal use, and differentiates these criminal acts from more traditional payment card fraud. [10] Finally,

---

[6] http://www.fatf-gafi.org/dataoecd/30/47/37627240.pdf

[7] As examples of industry-sponsored conferences where this issue was discussed, see: "TSYS Prepaid and Other Top Industry Experts Discuss Prepaid Cards and Money laundering," *Business Wire*, March 9, 2006; and the 2006 Prepaid Card Expo http://www.prepaidcardexpo.com/Final-2006-PrepaidCardExpo-Brochure.pdf.

[8] At the time of the workshop on March 28, 2006, Patrice Motz was Of Counsel at Bryan Cave LLP. Her new company information can be reviewed at www.premiercompliancesolutions.com

[9] Information about Paul Silverstein's company can be found at www.epochdata.com.

[10] While this paper focuses on prepaid cards' vulnerability to money laundering, some have suggested that prepaid cards could also be used to facilitate terrorist financing. In the workshop discussion, Motz explained that while money laundering is the attempt to disguise the nature and source of dirty money, terrorist financing is concerned with moving funds (legitimately or illicitly derived) undetected through the financial system so that terrorists can use these funds to support their activities. As in the case of the 9-11 attacks, seemingly innocuous fund transfers were made to terrorists in the United States, who then used the funds to pay for such mundane goods and services as hotel rooms and airplane tickets. Unlike with money laundering, little public information is available that describes the details of terrorist financing. The *9-11 Commission Report* states that terrorists "moved, stored, and spent their money in ordinary ways, easily defeating the detection mechanisms in place at the time." It appears that the terrorist network used bank accounts, wire transfers, credit cards, and ATMs in such a way as to not raise suspicion and alert authorities. In her remarks, Motz suggested that prepaid cards might provide new and attractive alternatives to traditional payment methods for terrorist financing.

the paper describes how the government's and the payment industry's responses to the challenge have helped mitigate risks while still supporting payment innovations.

II. Defining the Issue

Motz and Silverstein began the workshop with a discussion of several factors that present real cause for concern. Silverstein reflected on some of the similarities between the early days of prepaid phone cards and the similar high growth in today's prepaid card products. Back in the mid-1990s, the industry had few standards for the way phone cards were being marketed and sold to consumers, and no government regulations focused on the potential for abuse. With such a large market available, a number of unscrupulous vendors took money from consumers without giving them a valid telecommunications card. As several large frauds became public, the business of prepaid phone cards collapsed, and the reputations of all in the industry were damaged.[11] It took years of hard work for the legitimate players to regain public confidence in prepaid phone cards and re-establish the market.

Silverstein noted that the new prepaid card market might be susceptible to similar or even greater threats. While many prepaid card applications offer clear value to consumers and improve payment system efficiencies, this is still a relatively new product, and hence more vulnerable to fraud or operational risk than more mature payment alternatives. Unless these issues are appropriately addressed, Silverstein warned that these vulnerabilities could lead to the same level of market-crippling scandals that almost ended the business of prepaid phone cards.

In the case of prepaid cards, Motz and Silverstein see another and potentially greater threat beyond vulnerability to traditional fraud and operational risks. Echoing observations made in the *MLTA* and previewing comments made later in the DOJ and FATF reports discussed above, Motz and Silverstein focused on the features of prepaid payment cards that could make them vulnerable to money laundering. They also described the operational challenges in detecting

[11] "MCI Worker Charged in U.S. Investigation of Phone-card Fraud," *Wall Street Journal*, October 4, 1994.

money laundering activities and why it is much more difficult than combating traditional payment fraud. In summing up the overall challenges, they also noted that criminal demand for new ways to launder money is high and likely growing. Any new payment vehicle, such as prepaid cards, that has the potential to facilitate these activities is going to become a target for abuse.

An important focus of the workshop and this paper is to better understand how industry and government are responding to these threats and what tools and strategies are being employed to help mitigate risk while supporting welfare-enhancing payment innovations. However, before exploring how the specific issue of prepaid cards and money laundering is being addressed, it is important to understand the underlying issues in more detail: What exactly is money laundering? What makes this illegal activity different from traditional payment fraud? How big of a problem is this? Why the particular concern about prepaid cards?

III. What Is Money Laundering?

Money laundering is a process that involves taking money acquired through some criminal action, so-called dirty money, and moving it through the financial system so that its origin, ownership, and criminal nature remain disguised. It is a necessary element of any organized criminal activity undertaken for profit. For the perpetrators to realize the financial benefit of the criminal activity, the proceeds (funds or other assets) generated must be laundered.

The FATF defines money laundering as "an illegal activity carried out by criminals which occur outside of the normal range of economic and financial statistics." According to the FATF website,[12] the best measure of the extent of money laundering comes from the International Monetary Fund (IMF). In 1996, the IMF estimated that this criminal activity was equivalent to 2 to 5 percent of the world's gross domestic product. This would place the annual value of money laundering between $590 billion and $1.5 trillion.

[12] Go to http://www.fatf-gafi.org and click on the link to Money Laundering FAQ in the left-hand column.

At the workshop, Motz explained that money laundering is most easily understood as a process that consists of multiple steps or stages. First is the "placement" stage, during which illicit funds, usually in the form of cash, are placed into the financial system. One common method used in money laundering schemes is undertaken by low-level criminals called smurfs, who break down large sums of dirty money into smaller sums for placement in the financial system. For example, illicit funds may be placed into the financial system by purchasing money orders, bank drafts, or other payment instruments or by depositing money into one or more bank accounts. For the purposes of this paper, the process could also involve the purchase of multiple prepaid cards without necessarily interacting with bank personnel. This is the most vulnerable step in the money laundering process from the criminal's perspective. However, those engaged in organized money laundering activity typically understand the legal and regulatory rules very well. They work to keep the dollar amounts under the thresholds of the Bank Secrecy Act's (BSA) reporting and recordkeeping requirements and engage in transactions in such a way as to avoid patterns of behavior that could easily be detected by conventional means. If they successfully place the money, they can move on to the second, or "layering," stage.

The goal of the layering stage is to further hide the origin of the dirty money by conducting a series of transactions that will distance the funds from their criminal source and otherwise complicate the paper or audit trail so much as to make detection difficult if not impossible. For example, the money launderer initially may have "placed" the funds by purchasing multiple money orders, which are then mailed to an accomplice in another state who deposits them in the bank account of a front company that operates an apparently legitimate business. The accomplice wire-transfers the funds to a second business bank account, from which the funds are transferred to a business bank account of an alleged "supplier" outside the United States. In the case of prepaid cards, as we will see later in a documented case, the scenario could involve purchasing prepaid cards with illicit funds, using these cards to purchase additional

prepaid cards, and then using these cards to remove cash at an off-shore ATM. Once the money launderer believes the money is layered enough, the third and final stage, "integration," occurs.

In the integration stage, the funds are placed back into the economy as apparently legitimate funds. If the placement and layering stages went smoothly and as intended, the dirty money now appears clean, and there is little or no basis for questioning its origins. The criminal may invest this clean money or use it to buy products for consumption or to fund further criminal activity. For example, the last step could be to place the laundered funds onto prepaid cards, which are then used either to purchase retail goods or to pay another criminal.

In summary, money laundering has the objective of obscuring any audit trail that might lead back to the illegal source or funding agent and hiding or disguising the illicit nature of the true owner or controller of the funds. In the next section, we will discuss how this is different from traditional payment fraud.

IV. How Does Money Laundering Differ from Traditional Payment Fraud?

The payment card industry has developed a number of generally successful risk mitigation strategies and tools to address traditional payment fraud.[13] However, as Motz and Silverstein pointed out in their presentation, the risk mitigation strategies required to address money laundering are quite different from those used to combat traditional payment fraud. The reason for this lies in the fact that money laundering has very different consequences for the card issuer. Traditional payment card fraud results in an observable financial loss, but by design, money laundering transactions look like legitimate transfers with no observable loss.[14] For example, in the case of credit card fraud, a criminal steals a person's credit card or credit card

[13] In the credit card industry, fraud rates of card issuers have held steady at about seven basis points in recent years, reflecting a gradual downward trend over the past decade.
[14] However, the effects of money laundering and other illegal uses of payment systems result in a less identifiable, but no less significant, loss to society at large.

account information and then uses the stolen card or account information to buy goods or services for his own consumption.

In a lengthier scenario, the criminal could use the stolen credit card to purchase a money transfer or a prepaid card and then use the proceeds from the prepaid card or money transfer to make purchases. The legitimate owner of the credit card will see the unauthorized transactions on his monthly statement and notify the card-issuing bank. Generally speaking, in such scenarios, the unauthorized transaction is reversed on the consumer's account, and the card-issuing bank or, in some cases, the merchant absorbs the final cost of the loss.[15] When this type of payment fraud occurs, individuals and companies directly suffer financial damages and loss of time. The fact that there is an observable fraudulent event and a measurable financial loss creates natural incentives to mitigate the risk of traditional payment card fraud. In the case of money laundering, there is no observable loss. This not only complicates detection but also reduces incentives to invest in risk mitigation strategies.

When money laundering activity occurs, no person or institution is *directly* harmed.[16] The criminal is using the system as it was designed, but for nefarious purposes. For example, if a large sum of dirty money is broken down into smaller sums and deposited into one or more bank accounts and subsequently withdrawn, no bank or person incurs a financial loss. Specifically in the case of prepaid cards, if dirty money is loaded onto a prepaid card that is given to another individual for use, it could look very much like any normal transaction with no observable loss to the card issuer. As Motz emphasized, understanding the distinction between traditional payment card fraud and money laundering is a critical first step in developing risk mitigation strategies.

---

[15] For more details on the ways in which fraudulent payment card transactions may be processed, see the PCC discussion paper "The Laws, Regulations, and Industry Practices That Protect Consumers Who Use Electronic Payment Systems: Credit and Debit Cards." (www.philadelphiafed.org/pcc/ConsumerProtectionPaper_CreditandDebitCard.pdf)

[16] In a nonregulated open market economy, the crime of money laundering does not result in harm to the consumer or the financial institution. However, in an economy with laws and banking regulations, financial institutions can suffer penalties, damage to reputation, and possible prosecution if they do not follow the law.

The normal market forces that encourage financial institutions to invest in risk mitigation strategies to prevent payment card fraud and reduce losses are less clear in the effort to prevent money laundering. In these cases, the financial institution involved does not directly benefit from the investment it may make to prevent, detect, or report money laundering activity. However, money laundering undermines the integrity of the U.S. and international financial systems and imposes real costs to society at large. Money laundering provides the means by which criminals can continue their illegal activities. Therefore, broader government efforts are required to give the private sector incentives to make the process of cleaning dirty money difficult and facilitate prosecution of such criminal activity.

As Motz and Silverstein described in discussing strategies to mitigate the risk associated with the inappropriate use of prepaid cards, the only way financial institutions can detect such activities is to employ monitoring procedures specifically designed to detect the illicit movement of funds. The well-developed and traditional strategies for detecting payment card fraud are not sufficient to identify patterns of money laundering.

V. Are Prepaid Cards Especially Vulnerable to Money Laundering?

As noted earlier, government and law enforcement agencies have identified money laundering as a significant criminal problem. By its very nature, money laundering takes advantage of payment system vulnerabilities that allow criminals to disguise the nature of their transactions. Traditional payment mechanisms, such as cash, checks, money orders, and credit cards, have long been used by criminals to make illegal payments. Over time, a variety of regulatory, law enforcement, and business practice techniques have been developed to better identify and limit such abuses. Financial institutions are required to report suspicious transactions and authenticate the identity of their customers. Law enforcement agencies have developed ways to trace the illegal use of cash and other traditional payment instruments. However, as Motz and Silverstein noted, criminals are ingenious in exploiting vulnerabilities in payment systems,

especially when it comes to new and less familiar payment methods. As the *MLTA* and the DOJ and FATF reports note, prepaid cards are an example of a new payment method that provides a potentially attractive vehicle for enabling money laundering transactions.

What is it about prepaid cards that make them vulnerable to use in money laundering? Prepaid cards, also known as stored-value cards in the BSA and other related legislation,[17] are a relatively new payment vehicle. Like credit and debit cards, they are plastic cards that have a value associated with them. In some circles, the term stored-value card is used even though the value is not stored on the card itself. Technically, the monetary value is tied in with an account associated with the prepaid card. Conceptually, they can be thought of as "pay early" cards. This is different from credit cards, which are "pay later" cards, or debit cards, which are "pay now" cards. For more detailed information on how these prepaid cards function, please refer to the Payment Cards Center's discussion papers.[18] For the purposes of this paper, a brief discussion of the types of prepaid cards should suffice.

Two basic types of prepaid cards are available to consumers. The differences between the two types relate to how and where the prepaid card can be used. The first type is known as a closed-loop or closed-system prepaid card. The most common examples, and the one this paper will explore, are retail gift cards purchased either at the issuing merchant's location or from a distributor that may sell a variety of retail gift cards.[19] Typically, retail gift cards are sold with a pre-established dollar amount. Generally, the value associated with the card is redeemable only at the issuing retailer and only for goods and services of that retailer. Such retail cards may not be

[17] The Bank Secrecy Act's implementing regulations define stored value as "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." See 31 Code of Federal Regulations, Section 103.11(vv).

[18] See the PCC discussion paper "Prepaid Card Models: A Study in Diversity," http://www.philadelphiafed.org/pcc/PrepaidCardModels_Palmer_FINAL.pdf; and the conference summary "Prepaid Cards: How Do They Function? How Are They Regulated?," http://www.philadelphiafed.org/pcc/conferences/PrepaidCards_062004.pdf.

[19] Other types of closed-system prepaid cards are federal benefit cards associated with the food stamp program, which can be used only to purchase goods allowed by the program and at approved merchant locations.

redeemed for cash. Most retail gift cards do not have a reload feature, that is, additional value cannot be added to the card once the initial value is used. Retail gift cards with a reload feature, such as the Starbucks gift card, generally can be reloaded only up to a limited amount and, again, can be used only at the designated retailer locations.

The second type of prepaid card is known as an open-loop or open-system prepaid card. Open-system cards are network-branded prepaid cards that display the logo of a payment network on the front.[20] Network-branded prepaid cards can be used at any merchant that accepts the payment network's cards and some have the added feature of allowing the cardholder to withdraw cash at an ATM. Cards with an ATM feature generally display the logo of the relevant ATM network on the back of the card.[21] Many network-branded prepaid cards can be reloaded with additional value either through a regular deposit arrangement, such as in the case of payroll cards, or on an ad hoc basis by direct deposit, via the Internet, or directly at participating retail locations.[22] For the remainder of this paper, network-branded prepaid cards will refer only to gift cards associated with one of the payment networks or reloadable cards associated with a network brand and not the other types of network-branded cards, such as payroll, incentive, and health savings accounts.[23]

It is important to understand the differences between retail gift cards (closed-loop) and network-branded prepaid cards (open-loop) when thinking of how criminals can abuse them. For

[20] The four leading U.S. payment networks are Visa, MasterCard, American Express, and Discover. Two of the networks, Visa and MasterCard, started as credit card associations. These payment networks serve as an intermediary between the cardholder and where the card is used.

[21] The leading U.S. ATM networks are Star, NYCE, Co-Op, Pulse, and Jeanie as listed by *ATM & Debit News* for March 2006. The ATM networks serve as an intermediary between the cardholder and the owner of the ATM where the card is used.

[22] Some of the features of network-branded prepaid cards can provide bank-like payment services for those without traditional banking relationships. From a policy perspective, many observers see the functionalities associated with network-branded prepaid cards as positive steps toward providing more efficient payment services for the unbanked and underserved sections of society. For a review of how prepaid cards can benefit consumers without traditional bank accounts, see Julia S. Cheney and Sherrie L. Rhine, "Prepaid Cards: An Important Innovation in Financial Services," July 2006. (www.philadelphiafed.org/pcc/D2006JulyPrepaidCardsACCIcover.pdf)

[23] These other network-branded prepaid cards operate in a controlled environment where the source of funds and the cardholder are known; thus, they are less susceptible to money laundering.

some time it was thought that the limited purchase options and lack of access to cash precluded the use of retail gift cards for money laundering. However, Motz and Silverstein described several examples where retail gift cards have been used as a payment vehicle in money laundering activities. In one example, criminals purchased multiple gift cards from a U.S. retail chain with stores outside the U.S., typically at the highest dollar levels allowed, and sent the cards to an accomplice in another country where the cards were sold for local currency. In their discussions with law enforcement agencies, Motz and Silverstein have learned that drug dealers have used cash proceeds from drug sales to buy retail gift cards to pay drug suppliers. In this scenario, the retail gift cards are a medium of exchange, converting the illegal cash proceeds into a form of stored value.

While vulnerable to abuse, retail gift cards have obvious limitations for large-scale money laundering. As a result, in their efforts to deter the use of prepaid cards in money laundering, law enforcement agencies and industry providers have focused more on network-branded prepaid cards. What follows are several examples of how the more functionally sophisticated network-branded prepaid cards have been used to facilitate money laundering.

As recently as June 2006, an anonymous card with ATM capability, no load limits, and a $5,000 a day withdrawal limit was available on the Internet for $35. The web page[24] advertised the main features of these cards: “Anonymity, No name and No ID required!” Several similar card programs were listed on personal websites and blogs of individuals who refer to themselves as “privacy freaks” and do not want anyone to track their purchases or transaction history. [25]

As will be discussed later, payment networks and others in the prepaid card industry have reacted by putting restrictions on load limits and requiring cardholder identification to help eliminate the potential for using these prepaid cards in money laundering. Limited research done

[24] The information was found on www.evergreen-cards.com. However, the website is no longer active.
[25] Some people have stated that these websites offering to sell purely anonymous prepaid cards are scams operated by criminals to obtain funds with no intent to deliver a prepaid card. While this may be true, there have been criminal cases where criminals have abused the prepaid card system.

for this paper suggests that over the past year, U.S. banks and other participants in prepaid card programs have modified their requirements to include personal identification information for activating the reloadability feature of network-branded prepaid cards. While the availability of anonymous prepaid cards appears to have been largely eliminated in the U.S., they can still be obtained from offshore locations. For example, one company with a Cyprus address offers an anonymous prepaid card with a load value of €1000 (approximately U.S. $1,297 as of January 19, 2007).[26] These prepaid cards are issued anonymously and require no personal identification. In fact, multiple cards with values of €1000 can be ordered and shipped to the same mailing address. The company's website suggests that a person can fund the cards using most bank wire transfers but recommends that Swiss francs be used, since they "are subject to less nosing around by governments than other major currencies."

Another example that highlights the danger that rogue third parties can introduce into the prepaid market is the criminal prosecution of a money transfer firm called Western Express, which was indicted by the Manhattan district attorney for operating an illegal check cashing and money transmittal business.[27] During the four years that Western Express conducted business, a total of $25 million was moved through the company's bank accounts. This company converted funds from sources in Eastern Europe to prepaid cards for which Western Express served as a load location and distributor. The cards were then distributed to various individuals in the U.S. as well as mailed abroad. This allowed millions of dollars to be moved into and out of the United States.[28] When the authorities executed search warrants at the defendants' residence, they recovered more than $100,000 in cash and thousands of prepaid cards.

---

[26] One website has the following statement in its FAQ section: "We do not even require your real name, ID and phone number." In addition, you can purchase several cards that have no load limit.

[27] See the news release dated February 22, 2006, on the What's New web page of New York County's district attorney: www.manhattanda.org/whatsnew/index.htm.

[28] The Bank Secrecy Act (BSA) requires people who physically move money across the U.S. border to file a form called the Report of International Transportation of Currency and Monetary Instruments. The BSA also requires bank and nonbank financial institutions to create and retain records of fund transfers.

A final example comes from the records of a federal indictment in the United States District Court for the Eastern District of Texas alleging that a company called Moola Zoola[29] was a distributor of stored-value ATM cards. The defendant in the case moved money, originally obtained by defrauding consumers using PayPal money transfer accounts, onto multiple Moola Zoola cards; these cards were then used to transfer value onto other Moola Zoola cards, which were used to withdraw cash from ATMs located in Texas and Russia. The Moola Zoola card accounts were opened using information from victims of identity theft. According to a report in the *Dallas Morning News*, the Drug Enforcement Agency was notified about the suspicious activity. Assistant U.S. Attorney Ernest Gonzalez was quoted as saying that the prepaid cards were "used to launder money all over the world."

In these examples, note that behind all of these third-party sponsors or distributors there is always a bank card issuer who is ultimately liable. However, if the bank has lax underwriting standards or does not carefully monitor activity, they may be vulnerable to rogue third-party players. What makes prepaid programs different from traditional credit and debit card programs are the third parties, such as program managers and distributors (including money services businesses), that are a common part of the program design. A program manager is a third-party firm that designs the product, markets and services it, and maintains the account records of card loads. The distributor is the firm that sells the card directly to the consumer or provides the location or other channel (e.g., Internet, voice centers) through which the card can be reloaded. While these third-party firms may play a critical role in the business model for network-branded prepaid cards, their participation may also pose risks to the card-issuing banks.

As these examples demonstrate, banks need to recognize the inherent risks involved when the card-issuing bank does not actively manage the particular prepaid program. As prepaid card operations (sale, distribution, loads and re-loads) become further removed from the direct control of the card-issuing bank, the risk of criminal activity may increase. Just as banks employ

[29] From an article in the *Dallas Morning News*, November 22, 2006.

"know your customer" procedures as warranted by regulators, they must also perform due diligence when agreeing to serve as the issuing bank of a network-branded prepaid card that will be managed and distributed by another party. As will be discussed later, even if the program manager, distributor, and other participants are legitimate, there is always the risk that network-branded prepaid cards could be used by criminals if the bank or program manager does not monitor transactions in order to identify suspicious behavior.

In the presentation, Motz identified key areas where prepaid programs may be vulnerable to money laundering; she used the following table to describe how the risks may escalate as the prepaid program moves more toward anonymous use and weaker controls.

Lower Risk	**Medium Risk**	**Higher Risk**
Fixed Load Amount per Load Transaction	Some Limits	Unlimited Load Amount per Load Transaction
Limit on Total Load Amount	Some Limits	Unlimited Total Load Amount
One-Time Load		Reloadable
Purchaser Is an Existing Customer of Issuing Bank		Purchaser Has No "Account" Relationship to Issuing Bank
Full Identification and Verification of Purchaser		No Identification or Verification of Purchaser
Known Card Holder		Anonymous Card Holder
Source of Funds: Demand Deposit Account of Purchaser at Issuing Bank	Source of Funds: Credit Card	Source of Funds: Cash, Other Prepaid Card

Source: Bryan Cave LLP

In discussing the table, Motz explained that a prepaid program with relatively low risk would incorporate controls that would make it less attractive for money laundering.

Consequently, cards with low-dollar fixed-load limits and no ability to reload would have limited usefulness to money launderers. At the other extreme, cards with an unlimited load limit and reloadability would pose a much greater risk for money laundering. As noted earlier, the "know your customer" maxim is important not only in terms of how a bank manages its partnerships with sponsors of prepaid card programs but also with respect to the actual cardholder. When the bank and sponsor have existing relationships with the ultimate cardholders and can verify their identity, there is relatively low risk of money laundering. On the other hand, card programs that do not require verification of identity clearly offer a more attractive option for money launderers.

Last, Motz pointed out that the source from which prepaid cards are purchased or loaded is important as well. Cards loaded directly from a known customer's bank account provide the greatest security, whereas cards loaded using cash or even another prepaid card present a much higher level of risk. Can anything be done to prevent criminal abuse of prepaid cards? The next two sections will provide an overview of what is being done by the government and the payment industry to detect and prevent money laundering.

VI. Government Responses

As noted earlier, many of the natural market incentives that work to limit payment card fraud are largely absent in efforts to combat the use of payment systems in money laundering. This has led to the need for more direct government involvement in creating legal and regulatory incentives. The BSA was the initial piece of federal legislation focused on these activities. With the passage of the BSA in 1970, the U.S. Treasury was authorized to issue regulations that required financial institutions to file reports and maintain records on financial transactions that were viewed as possibly related to criminal schemes, attempts at tax evasion, or money laundering.

At the heart of the BSA is an attempt to create an identifiable footprint in the movement of funds derived from or to be used for illicit purposes. The impetus for many BSA provisions is

an attempt to identify the source, volume, and transit points of funds moving into and out of the institution that may be related to money laundering and identify the persons associated with such movement. The overall objective is for institutions subject to BSA provisions to take reasonable steps to prevent and detect money laundering. Banks and other financial institutions in the United States are required to file currency transaction reports (CTRs) and suspicious activity reports (SARs). Collecting information, maintaining records, and filing reports enable law enforcement to conduct criminal investigations and provide regulatory agencies with the ability to monitor noncompliance.

The USA PATRIOT Act, which was passed in 2001, amended the BSA to mandate that all statutory financial institutions establish anti-money laundering (AML) programs. This mandate obligates each institution subject to it to develop, implement, and maintain an effective AML program. Through recent BSA enforcement actions, the AML program requirement has been extended to nonbank issuers, sellers and redeemers of stored-value cards (including money services businesses), and operators of credit and debit card systems. As Motz and Silverstein emphasized, an effective program is one reasonably designed (1) to ensure compliance with specific BSA provisions applicable to the institution and (2) to prevent the institution from being used to facilitate money laundering.

Banking regulators have issued the Federal Financial Institutions Examination Council's (FFIEC) BSA/AML Examination Manual,[30] which outlines steps a bank examiner should follow when performing a money laundering review. Prepaid cards are one of the first items mentioned in the section titled "Identification of Specific Risk Categories." In addition to listing specific bank products that may pose a higher risk of money laundering, the FFIEC manual lists types of business partners that warrant closer review during the BSA/AML examination. Second on this list of bank business partners that examiners are instructed to pay attention to are nonbank

[30] The FFIEC's website contains both an online and PDF version of the manual, which can be viewed at: http://www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_print.htm.

financial institutions. As noted earlier, such third-party firms are common participants in many network-branded prepaid card programs.

Federal government responses to the threat of money laundering continue to evolve. Not surprisingly, particular attention is being paid to newer payment mechanisms, including prepaid cards. As Motz noted, efforts are ongoing: The requirement to implement customer identification programs (CIP), for example, has not yet been explicitly extended to operators of card systems or issuers, sellers, or redeemers of prepaid cards. In her view, it is not clear whether and to what extent the CIP requirement that applies to banks also applies to prepaid card programs for which a bank is the card issuer but does not have a direct deposit account relationship with each cardholder.[31] Presumably, these and other issues posed by this new payment mechanism will be addressed by the appropriate government agencies in the future.

As described in the next section, the payment industry has also developed its own strategies to detect and prevent money laundering as described in the next section.

VII. Payment Industry Responses

In addition to developing processes to comply with federally mandated AML programs and other regulatory requirements, banks and participants in prepaid card programs have been developing other strategies and tools to help mitigate the risks of prepaid cards being used to facilitate money laundering. Given their central role in network-branded prepaid cards, Visa, MasterCard, and other network providers have established rules for issuing banks to implement in order to lessen the risk that prepaid cards will be used for money laundering. Many of these rules

[31] The Office of the Comptroller of the Currency (OCC) issued an advisory letter (2004-6) specifically for payment cards on May 6, 2004, suggesting that banks offering payroll cards verify cardholder identity and implement AML controls while waiting for further regulatory guidance. No guidance has been offered to date for network-branded gift cards with or without reloadability.

reflect the risks outlined in the table shown earlier in this paper.[32] For example, recognizing the relatively low risk associated with a nonreloadable prepaid card, network rules do not require a cardholder's personal identifying information, but they do stipulate limits to the amount that can be loaded onto the card. However, recognizing the greater risk of money laundering when a card can be reloaded, the payment networks have imposed additional rules for prepaid cards that have this feature. For example, only a limited dollar amount can be loaded at the time of purchase. To activate the loadability feature, the prepaid cardholder must provide personal identifying information either by phone or through an online automated system.

At the card-issuing and program management level, companies are developing strategies to monitor card usage to detect patterns that identify high-risk situations. Firms such as Epoch Data Inc. have developed real-time transaction-monitoring technology to identify suspicious or high-risk transactions that might suggest money laundering activity. These new transaction monitoring systems differ from traditional card fraud software applications. As Silverstein explained, traditional payment fraud solutions are not likely to identify money laundering activity because detecting money laundering requires a very different set of filtering patterns. As he stated, "If you do not specifically look for money laundering, then you probably will not find it."

For example, in the Moola Zoola case, where funds were loaded onto one prepaid card, transferred to another, and then removed soon after at an ATM, the standard software using parameters designed to detect payment fraud would not have identified these suspicious activities. Only active, real-time transaction monitoring systems designed to spot such patterns would be likely to find money laundering activity.

As the earlier examples showed, the existence of third-party distributors and nonbank reload locations opens up the possibility of collusion with money launderers. However, if a bank or program manager uses transaction monitoring technology to examine purchases, reloads, and

[32] It would be likely that the payment networks have established other rules to detect and prevent criminal activity that are not publicly available for obvious reasons.

withdrawal activities at all distribution locations, anomalous patterns can be detected. For example, such a system of transaction monitoring could identify and highlight unusually high levels of card purchases or reloads at a particular location, prompting further investigation. The key to the success of these automated systems is a robust set of pattern-detecting rules designed to identify specific money laundering behavior. Silverstein also argued that such transaction monitoring has inherent business value for prepaid card issuers and sponsors. The card utilization data and distributor-specific activities captured can help firms to see which products or locations are more profitable, enabling them to adjust to specific market conditions.

VIII. Observations and Conclusion

Efforts to combat money laundering remain a high priority for federal law enforcement and regulatory agencies and the financial services industry. Despite these efforts, criminal elements continue to find ways to exploit financial payment systems to move and hide illicit funds. While all methods of payments from cash, to ACH, to credit cards are subject to illicit use, history suggests that, over time, government agencies and private payment providers are generally able to develop mitigation strategies to limit abuse.

New payment methods, however, are particularly vulnerable to abuse when both regulators and payment providers are just beginning to observe how criminals may carry out such abuse. Criminals are often one step ahead of those trying to prevent the crimes. The task for regulators and the payment industry is to make the abuse of payment products as difficult as possible without stifling legitimate use and continued innovation.

Regulators' and law enforcement's concerns about prepaid cards are justified. Prepaid cards have a number of characteristics that offer opportunities for money laundering if use of such cards is not closely monitored. The high degree of anonymity associated with many prepaid cards, the participation of additional nonbank and unregulated parties in the process, and prepaid

cards' ease of acquisition and reloadability make them more vulnerable to potential abuse than other, more established payment methods, including traditional debit and credit cards. However, the industry and government agencies have come to better understand these risks, and various safeguards are being developed to limit potential abuse.

During the workshop, Motz and Silverstein made several suggestions for how banks and other participants of prepaid card programs should develop their *own* strategies for detecting money laundering beyond the BSA's guidelines. They suggested that firms employ programs that focus on "know your customer" procedures and that limit the velocity of loads and reloads, the acquisition of multiple cards for the same account, and control the number of ATM withdrawals. They further suggest that firms develop and employ monitoring systems specifically designed to examine such activities across their networks to detect suspicious use, much the same way they use other software specifically designed to detect payment fraud.

In conclusion, there is no "silver bullet" to completely stop money launderers' use of prepaid cards. Federal regulations combined with payment network rules and business risk mitigation practices are helping to reduce criminal activity and promote a healthy and robust market for legitimate prepaid card programs. Only time will tell if program participants' actions are enough to prevent prepaid cards from becoming a favored method for criminals to illicitly move money.