U.S. Department of Justice
National Drug Intelligence Center

Assessment

Product No. 2006-R0803-001

Prepaid Stored Value Cards:

A Potential Alternative to Traditional Money Laundering Methods

31 October 2006

Key Judgments

Prepaid stored value cards—a product experiencing explosive growth—provide an ideal money laundering instrument to anonymously move monies associated with all types of illicit activity, without fear of documentation, identification, law enforcement suspicion, or seizure. Therefore, it is very likely that drug traffickers and criminals alike are exploiting and will increasingly exploit the convenience and anonymity of prepaid stored value cards to launder and move funds associated with their illicit enterprises.

- Prepaid stored value cards cannot be seized for Report of International Transportation of Currency or Monetary Instrument (CMIR) violations; are loosely regulated; function as remittance cards; frequently provide cardholder anonymity when individuals are obtaining cards or adding value to cards; often have liberal daily limits on total card value, reloading, withdrawal, and spending of funds; and feature fees that are generally consistent with or lower than the normal "cost" of laundering money.
- Prepaid stored value cards are, in many ways, superior to established methods of money laundering and money movement—specifically, the use of money transmitters and bulk cash smuggling—and may replace these methods under certain conditions.
- Drug traffickers and other criminals will most likely use prepaid stored value cards in lieu of electronic money transfers because the fund-transfer processes are similar and use of the cards provides additional benefits.
- Prepaid stored value cards are an advantageous alternative to bulk cash smuggling via package delivery services or couriers on board commercial conveyances (airplanes, buses, trains)—methods that carry a significant risk of detection by law enforcement.
- It is much less likely that prepaid stored value cards will replace traditional bulk cash smuggling by private or commercial vehicle—methods that currently appear to be adequate to fulfill traffickers' needs.
- U.S. regulatory action alone will not be sufficient to suppress the money laundering threat posed by prepaid cards, since cards issued by non-U.S. banks or other institutions can be used domestically to transfer funds, make purchases, or access cash at automated teller machines (ATMs).

Introduction

Prepaid stored value cards provide drug traffickers with a unique and simplistic money laundering method, which can be used to smuggle profits from the United States to other countries or to send instant cross-border remittances. The techniques made possible by prepaid stored value cards are, in many ways, superior to the use of money transmitters and bulk cash smuggling, methods commonly used to move a portion of the estimated $13.6 billion to $47.7 billion of wholesale illicit drug proceeds transferred to foreign destinations annually.[1] Under the proper conditions, prepaid stored value cards may emerge as a substitute for these methods.

Background

Several types of stored value cards—open system, semi-open system, closed system, and semi-closed system—are widely available in the United States. Open system cards operate on major credit card networks and can be used anywhere that the network brand is accepted, frequently including worldwide ATMs. These cards are similar in appearance to traditional debit cards and are embossed with the cardholder's name. Semi-open system cards generally have the same features and limitations as open system cards but cannot be used to access cash at ATMs. Closed system cards, such as store gift cards, operate on merchants' internal networks and can be used only to conduct transactions within the specific payment system(s) for which they were intended. Semi-closed system cards may operate on major credit card networks and carry a major credit card network brand. Closed and semi-closed system cards are generally anonymous, are issued in preset dollar amounts, and are not reloadable. All prepaid stored value cards draw value from funds provided to the program manager or a designee prior to use.

Typical Infrastructure of Network-Branded, Prepaid Stored Value Card Programs

- A **program manager** is the owner of a prepaid stored value card program. Typically, program managers are responsible for establishing relationships with processors, banks, payments networks, and distributors and for establishing pooled account(s) at banks.
- A **processor** facilitates payment transactions for prepaid stored value card programs and tracks and distributes funds in pooled accounts. Although this function is generally outsourced, program managers may choose to function as their own processors.
- A **bank** maintains pooled accounts, settles payments, and issues Visa- and MasterCard-branded prepaid stored value cards. Banks may also function as program managers and/or distributors.
- A **payments network** provides the connection between processor and retailer, ATM, etc., for authorization of payment transactions and issues American Express- and Discover-branded prepaid stored value cards.
- A **distributor** sells prepaid stored value cards.

Source: Federal Reserve Board; Network Branded Prepaid Card Association.

1. National Drug Intelligence Center (NDIC) estimates indicate that drug trafficking organizations (DTOs) generate, remove, and launder from $13.6 billion to $47.7 billion in wholesale distribution proceeds annually. These figures were derived by multiplying the total quantity of foreign-produced drugs available at the wholesale level in the United States by wholesale prices for those drugs.

Money laundering activity can be facilitated by each type of prepaid stored value card; however, open system cards have the greatest utility for money laundering related to wholesale-level drug trafficking. Open system cards function as a secure, compact, and inconspicuous vehicle for the physical transportation of funds. These cards also can be used to electronically transmit funds by the addition of funds to the card in one location and withdrawal of funds via ATM in another. Front companies can exploit payroll cards—a type of open system card used to pay employees who prefer not to use traditional bank accounts—by loading unlimited amounts of funds onto the cards of fictitious employees. Additionally, funds loaded on open, semi-open, and semi-closed system cards can be removed from cards via "purchases" made at front companies. Further, Black Market Peso Exchange (BMPE)[2] activity could be facilitated by all types of prepaid stored value cards because the cards can be used to purchase goods within the BMPE system. However, closed and semi-closed system cards are poor methods of moving large amounts of money, because they generally cannot be converted to cash without the resale of the card, often at a loss. Nonetheless, these cards can be sold in an increasing number of Internet venues, including web sites devoted exclusively to trading these cards and Internet auction sites that allow limited sales of the cards. These examples represent only a limited number of ways that prepaid stored value cards can be exploited by money launderers.

Substantiation

Prepaid stored value cards have several characteristics that contribute to the considerable utility, efficiency, and accessibility of this money laundering method.

Prepaid stored value cards cannot be seized for failure to file a CMIR and may therefore be openly carried or shipped across U.S. borders without fear of seizure. According to the U.S. Department of the Treasury and the U.S. Department of Justice Asset Forfeiture and Money Laundering Section (AFMLS), CMIRs are not applicable to the cards, because they are not considered to be monetary instruments under 31 USC 5316. Thus, the cards are easier to transport across U.S. borders than illicit bulk cash—which, in amounts greater than $10,000, must be concealed to prevent discovery and seizure—and the cards occupy less physical space as well. Additionally, it is often difficult to distinguish open system cards from traditional debit cards.

Prepaid stored value cards are loosely regulated in comparison to many other types of financial products, because it is unclear whether existing federal laws designed to regulate other financial products also apply to prepaid stored value cards and because the cards are specifically exempt from some Bank Secrecy Act (BSA)[3] requirements. The only applicable federal reporting requirement to providers of stored value is the Currency Transaction Report (CTR)[4] rule. While banks that maintain pooled accounts for program managers are clearly

2. The Black Market Peso Exchange (BMPE) is a system in which Colombian traffickers receive Colombian pesos in Colombia in exchange for U.S. dollars located in the United States. Peso brokers facilitate this process by selling Colombian trafficker-owned U.S. dollars located in the United States at a discount to Colombian merchants who use the funds to purchase U.S. goods.
3. The Bank Secrecy Act of 1970 was designed to do the following: deter money laundering and the use of secret foreign bank accounts; create an investigative paper trail for large currency transactions by establishing regulatory reporting standards and requirements; impose civil and criminal penalties for noncompliance with its reporting requirements; and impose detection and investigation of criminal, tax, and regulatory violations.
4. Currency Transaction Reports (CTRs) must be filed for all cash transactions greater than $10,000.

responsible for conducting program manager due diligence, it is unclear whether either party—the bank or the program manager—is required to verify the identities of individual cardholders; the USA PATRIOT Act requires financial institutions to verify the identities of customers for whom they have opened accounts.[5] Although the BSA definition of money services businesses (MSBs) includes issuers, sellers, and redeemers of stored value, these businesses—unlike other MSBs—are not required to register with Financial Crimes Enforcement Network (FinCEN), retain customer identification information or transaction records, or file Suspicious Activity Reports by MSBs (SAR-MSBs).[6] The only MSB BSA requirement applicable to providers of stored value is an obligation to maintain anti-money laundering (AML) programs. Conversely, money transmitters—also included in the BSA definition of an MSB—are required to maintain AML programs; to verify, record, and retain customer identification information on all transactions greater than \$3,000; and to file SAR-MSBs on all suspicious transactions in excess of \$2,000.

Open system cards that offer global ATM access without a bank account function as remittance cards, allowing traffickers to move funds electronically in a manner that approximates money transfers. By allowing cross-border remittances without the services of a bank or money transmitter, traffickers (through the use of the cards) can send remittances that are exempt from BSA requirements, including reporting requirements and verification of the cardholder's (and recipient's) identity. The cards are the ideal instrument for large-scale drug trafficking and money laundering operations because some of these programs have no limit on the amount of cash that can be accessed outside the host country. Moreover, many cards that are marketed as remittance cards are specifically designed to transport funds to Mexico because of legitimate demand; however, Mexico is the destination for a significant amount of wholesale drug proceeds. Cards that are not marketed as remittance cards can function as such if the provider offers multiple cards per account. Further, transactions are sometimes conducted without the cardholder's presentation of the card (by using the account number only). This situation enables cardholders in numerous locations to add or withdraw funds or make purchases.

Because prepaid stored value cards can be obtained without securing a traditional banking relationship, they often can be obtained and reloaded anonymously or without photo verification of cardholder identity. Cardholder anonymity is a marketed characteristic of some prepaid stored value products; while other cards require identity verification, several factors make it easy to falsify identification. Many cards that are purchased at agent locations, online, or by fax do not require photo identification; in these cases, identification is often accomplished by verifying that the cardholder's reported name, address, and social security number correspond according to a credit reporting service. This situation enables cardholders to secure multiple anonymous accounts by using stolen identities. The anonymity associated with obtaining prepaid stored value cards is maintained throughout the process of adding value to the cards, which also can be done without face-to-face interaction or identification. Most brands of such cards allow cash to be loaded anonymously at ATMs and at program managers' or agents' locations, making it difficult to determine the origins of funds and the identity of the funding individual or entity. Cards can also be loaded with varying degrees of anonymity via mail,

5. The USA PATRIOT Act defines "account" as "a formal banking or business relationship established to provide regular services."
6. Issuers, sellers, and redeemers of stored value cards may file Suspicious Activity Reports by MSBs (SAR-MSBs) voluntarily.

Internet, or ATMs using various payment methods, including checks, bank credit, account-to-account transfers, Internet fund transfers, and electronic transfers of wages. Law enforcement agents participating in the El Dorado Task Force in New York found that they could use false identification to obtain prepaid cards and could have the cards sent to a post office box, further insulating illicit activity. U.S. Secret Service (USSS) investigations revealed that some prepaid card applicants not only use false identification but also fund their initial deposits with stolen credit cards. In addition, vending machines designed to add value to prepaid stored value cards are being used in Japan; the use of these machines will quite likely spread to the United States as the domestic popularity of these cards increases.

Many program managers offer liberal limits on daily total card value and on daily reloading, withdrawal, and spending of funds; some domestic program managers permit cardholders to load cards with an unlimited total value. Offshore banks also offer prepaid stored value cards with unlimited reloading; these cards are marketed specifically to allow cardholders to move money anonymously. Cards with liberal limits on total value are ideal for large-scale drug trafficking and money laundering operations; such cards make it easier for traffickers to manipulate larger amounts of money using fewer transactions. The network brands of most domestically issued prepaid stored value cards have suggested caps on card reloading, but the limits are not binding on issuers.

Internal Anti-Money Laundering Guidelines for Network-Branded Prepaid Stored Value Cards

MasterCard International and Visa USA have established internal AML guidelines for network-branded, prepaid stored value cards in response to growing concerns about their potential utility for money laundering. Both branders suggest that companies carrying their brands administer programs regarding account limits and identity verification; however, neither organization is actively policing program managers to ensure compliance with these programs. MasterCard has proposed a card balance limit of $2,500; however, the limit is not binding on issuers.

Source: U.S. Department of the Treasury.

Although consumer advocacy groups allege that fees charged for use of prepaid stored value cards are high in relation to legitimate consumer activity, the fees are generally consistent with or lower than the normal "cost" of laundering money. Depending on the manner in which the cardholder conducts activity and on the fees charged by the company, the total fees for the use of prepaid stored value cards can be similar to those charged by money transmitters and are significantly lower than the costs associated with bulk cash smuggling (i.e., the cost of maintaining vehicles, building traps in vehicles, purchasing gasoline, paying couriers, etc.). Card fees vary by provider and may or may not be charged for a variety of activities, including, but not limited to, account setup; loading, spending, and cash withdrawal of funds; monthly maintenance; balance inquiries; and overdrafts.

Scope of the Industry

The rapid growth of the prepaid stored value market—which is quickly replacing a variety of paper payment products such as checks, traveler's checks, and gift certificates—and the resulting legitimate competition between institutions that offer such services will

provide drug traffickers and other criminals with more service options; the increasing number of transactions will make illicit transactions more difficult to detect. The Mercator Advisory Group, a research and advisory firm focused on the payments industry, reports that from 2003 to 2004, spending on all types of prepaid cards, including store gift cards, payroll cards, and government benefits cards, grew by almost 21 percent ($110.7 billion to $133.9 billion). During that time the open system prepaid card market itself grew by 91.6 percent. The Aite Group, a research and advisory firm focused on issues related to the financial services industry, estimates that prepaid debit card spending will increase from $12.8 billion in 2004 to $150 billion by 2009. As of January 2005 roughly 7 million Visa and MasterCard brand prepaid debit cards were in circulation, issued by more than 2,000 programs. According to a report issued by the Aite Group in 2005, the number of U.S.-issued Visa- and MasterCard-branded money remittance cards will increase from 400,000 in 2005 to more than one million in 2006. Currently, network-branded prepaid stored value cards carry the logos of American Express, MasterCard International, and Visa USA. Discover Financial Services, in partnership with Morgan Beaumont, is working to develop prepaid stored value cards.

Outlook

Drug traffickers, narcoterrorists, and other criminals will increasingly rely upon prepaid stored value cards as a method to launder and move funds, in part because the cards provide the means for a unique and simplistic money laundering method that can be used to send instant cross-border remittances or to smuggle profits from the United States to other countries. The cards are superior to established methods of money laundering and money movement—specifically, the use of money transmitters and some bulk cash smuggling techniques—because the cards can be utilized without fear of documentation, identification, law enforcement suspicion, or seizure.

Open system prepaid stored value cards may emerge as a substitute for use of money transmitters because the process of obtaining the cards is very similar to the process of making money transfers, including the use of "smurfs"[7] to place illicit funds. As such, the use of prepaid stored value cards in lieu of money transfers will require very little change in those traffickers' operational activities, and any changes made will ultimately benefit the traffickers.

Under certain conditions, open system prepaid stored value cards may be used in lieu of bulk cash smuggling; however, this use depends on the particular bulk smuggling method. Use of these cards as a substitute for any such method will require significant operational changes, including the use of smurfs to structure and place funds. It is likely that the cards will emerge in lieu of bulk cash smuggling via package delivery services or couriers onboard commercial conveyances (airplanes, buses, trains) because it is more likely that bulk cash smuggled by these methods could be detected by law enforcement. It is less likely that bulk cash smuggling

7. "Smurfs" are teams of persons who, acting in conjunction with or on behalf of other persons, structure financial transactions by conducting or attempting to conduct one or more transaction in currency, in any amount, at one or more financial institutions, on one or more days, in any manner, for the purpose of evading the reporting requirements under Title 31. "In any manner" includes but is not limited to the breaking down of a single sum of currency exceeding $10,000 into smaller sums, including sums at or below $10,000. The transaction or transactions need not exceed the $10,000 reporting threshold at any single financial institution on any single day in order to constitute structuring within the meaning of this definition.

operations conducted via private and commercial vehicles—one of the primary money movement methods used by Mexican drug trafficking organizations (DTOs)—will be replaced by the use of prepaid stored value cards. A considerable amount of the estimated $8.3 billion to $24.2 billion in Mexican and Colombian wholesale drug proceeds generated annually in the United States quite likely is moved into Mexico via bulk cash smuggling by vehicles. The use of bulk cash smuggling via vehicles is likely adequate to fulfill the traffickers' current needs; in addition, there would be no need to transport the cards long distances by vehicles, since the cards can be sent to a final destination expeditiously via package delivery services or commercial conveyances. However, if the movement of bulk cash were severely hindered by dramatically increased law enforcement interdictions in the Southwest Border area, the chances that these cards would be used in lieu of smuggling via vehicles would increase.

The U.S. Department of the Treasury has acknowledged the need to modify and clarify existing regulations related to the prepaid stored value card industry; in fact, FinCEN recently announced that it will issue new regulations designed to clarify the roles and obligations of issuers of prepaid cards. Although it is not yet clear what actions will be taken, there is an obvious need to implement several changes to existing regulations. In order to enable seizure of prepaid stored value cards with a monetary value of more than $10,000, stored value should be included in the definition of monetary instruments for CMIR purposes. Because it is often difficult to distinguish between traditional debit cards and network-branded prepaid stored value cards, a requirement designed to distinguish the appearance of open and semi-open system prepaid stored value cards would enable law enforcement agencies to better identify suspicious cards. Due diligence procedures required of financial institutions under the USA PATRIOT Act—such as identity verification and comparison of customers' identities against names of known terrorists—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. Additionally, the imposition of compliance programs such as those that apply to money transmitters—including customer identification, recordkeeping, and SAR-MSB reporting requirements—would empower law enforcement investigations by allowing agencies to access information such as cardholders' identities, to track transactions, and to identify patterns of suspicious activity. Procedures such as identity verification, recordkeeping, and SAR-MSB reporting requirements will most likely become the responsibility of the program manager in conjunction with the processor, rather than the responsibility of the bank, because the bank's role in the prepaid card process prevents it from having access to information necessary to completing those processes. Various risks are associated with different types of cards; therefore, it is also likely that those cards will be regulated in different ways. For example, there may not be a need to treat closed or semi-closed cards—which are issued in small preset amounts and cannot be reloaded or used at ATMs—with the same AML procedures as open system cards. Because prepaid stored value cards have demonstrated unique and substantial economic benefits, any regulations applied to these products should be balanced in order to protect consumers and combat money laundering without inhibiting the growth of the industry.

U.S. regulatory action alone will not be sufficient to suppress the money laundering threat posed by prepaid cards. Even if clear and consistent regulatory measures are imposed, cards issued by non-U.S. banks or other institutions—which are not subject to the BSA—can be used in the United States to make purchases or access cash at ATMs. Limited international oversight of these cards is possible through a recommendation of the Financial Action Task Force on Money

Laundering (FATF), which has publicly stated the need to monitor the growth of and implement AML controls for this industry; however, FATF recommendations will have little effect on non-member countries and noncooperative countries or territories (NCCTs). Legislation of regulatory controls that would allow the U.S. government to prevent foreign cards from being used in the United States will be difficult. In order to limit illicit use of foreign-issued cards in the United States, cooperation from card branders will be necessary.

Card readers should be made available to law enforcement agencies throughout the United States, particularly those located at or near ports of entry (POEs), in order to determine the value of cards—seizures of funds on cards might be possible if it could be proven that the card was funded with the proceeds of a specified unlawful activity (SUA).[8] If law enforcement officers who encounter suspicious cards, i.e., one (or more) high-value card or numerous low-value cards that have no credible purpose, there may be a separate basis on which to seize the cards under 18 USC 1956, *Laundering of Monetary Instruments*, or 18 USC 1960, *Prohibition of Unlicensed Money Transmitting Businesses*. Law enforcement officers may be able to assemble evidence regarding the cards—specifically, information regarding how much money is loaded on the cards; how the funds were generated; where the cards are being taken and for what purpose; and, if the cards are being carried by a courier, what that person is being paid and the number of previous trips he or she has made. During this process it is important that law enforcement officers avoid alerting the suspect to their suspicions regarding the source of the funds in order to ensure that the funds are not removed from the cards by the suspect or a coconspirator.

8. Specified Unlawful Activity (SUA) is defined under 18 USC 1956 (c) (7).

Sources

National

U.S. Department of Justice
- Criminal Division
  - Asset Forfeiture and Money Laundering Section
- Drug Enforcement Administration
- Federal Bureau of Investigation

U.S. Department of the Treasury
- Financial Crimes Enforcement Network

Open Sources

American Banker

Financial Action Task Force

Mercator Advisory Group

Money Laundering Alert

Rand Corporation

This page intentionally left blank.

This page intentionally left blank.

319 Washington Street 5th Floor, Johnstown, PA 15901-1622 • (814) 532-4601

NDIC publications are available on the following web sites:

ADNET	http://ndicosa	LEO	home.leo.gov/lesig/ndic
RISS	ndic.riss.net	INTERNET	www.usdoj.gov/ndic

103106