Have Anti-Money Laundering Measures Kept Pace with the Rapid Growth of GPR Prepaid Cards?

Douglas King

Retail Payments Risk Forum Working Paper
Federal Reserve Bank of Atlanta
January 2013

Abstract: Since their introduction in the early 1990s, general purpose reloadable (GPR) prepaid cards have evolved to become one of the fastest-growing consumer payment instruments in the United States. Although these cards were at one time lightly regulated and lacking in risk controls and measures, which made them conducive for money laundering, regulatory measures and industry-wide risk management practices have evolved to mitigate the money laundering risks associated with these cards. This paper will examine both the regulatory response and the adoption of risk measures by the industry to minimize the attractiveness of GPR prepaid cards as a money laundering instrument. However, these risks still exist within this industry, and the concerns of law enforcement officials are warranted. Namely, the regulatory and industry responses seen in the United States have not necessarily been adopted in other jurisdictions. The risks of money laundering with GPR prepaid cards issued outside of the United States are thus higher, and they should be of concern to law enforcement agencies and officials.

I. Introduction

According to the 2010 Federal Reserve Payments Study, prepaid card transactions (includes private label, general purpose, and EBT cards) were the fastest growing noncash payments segment between 2006 and 2009 with a compounded annual growth rate of over 20 percent during that period.[1] The primary driver of growth for prepaid cards during this period was usage of general purpose prepaid cards, or network branded prepaid cards. General purpose reloadable (GPR) prepaid card[A] transactions increased at an average annual rate of over 63 percent, from 0.3 billion transactions in 2006 to 1.3 billion in 2009.[2] Consumers loaded over $28 billion onto GPR prepaid cards in 2009 and Mercator Advisory Group estimates this figure to reach nearly $202 billion by 2013.[3]

These cards also referred to as "open loop," carry one of the major payment card network brands and can be used to make purchases at any merchant that accepts the card network brand. Many of these cards can also be used to withdraw cash from an ATM. There are two types of general purpose prepaid cards – 1) reloadable and 2) non-reloadable. GPR prepaid cards allow additional value to be loaded onto the cards via ACH, check, card, or cash transactions. General purpose non-reloadable cards, also labeled as gift cards, do not allow the card user to add additional value to the card beyond its original purchase value.

Introduced with a focus on POS payment applications in the early 1990s, GPR prepaid cards have grown in popularity as an alternative to traditional deposit accounts and other paper-based solutions such as payroll payments, domestic and cross-border remittances, and government assistance programs. According to research, consumers are attracted to GPR prepaid cards because they offer convenience, accessibility, immediate liquidity, simplicity, value, and built-in discipline.[4] However, some of these attributes – convenience, accessibility, and immediate liquidity, as well as others – anonymity, transferability, and transportability, also serve as attractive attributes to criminals for money laundering.

These money laundering concerns have not gone unnoticed by a number of federal law enforcement agencies. As highlighted in a 2007 paper authored by Stanley

[A] General purpose reloadable prepaid cards have evolved since their introduction and can now be segmented by a variety of different product types, including government benefit programs, travel, payroll, and T&E cards. For the purpose of this paper, GPR cards refer to cards that are purchased by consumers, loaded with consumers' own funds, and primarily used for everyday purchases or ATM cash withdrawals.

Sienkiewicz, an interagency workgroup that included the Departments of Treasury, Justice (DOJ), Homeland Security, the Board of Governors of the Federal Reserve System (Board), and the United States Postal Service (USPS) published a report in late 2005 emphasizing the money laundering risks associated with prepaid cards.[5] Since then, this workgroup and other agencies, including the Financial Action Task Force (FATF) and the United States Government Accountability Office (GAO), have continued to release reports highlighting the money laundering risks associated with prepaid cards, including actual case studies.

Given concerns from law enforcement agencies as well as real life examples of money laundering activities using GPR prepaid cards, the government, regulatory agencies, and the industry at-large have taken measures to combat money laundering via GPR prepaid cards. This paper will examine the evolution of government and self-regulation to minimize the risky attributes of GPR prepaid cards that make (or made) them conducive for money laundering. In light of the GPR prepaid card industry's evolving regulatory environment, the paper will also identify any additional risk management measures that could further minimize GPR prepaid cards' money laundering risks.

I. The General Purpose Reloadable Prepaid Card Business Model

While GPR prepaid cards share many of the same value chain participants and characteristics of credit and debit cards, there are some key differences among them. To begin, the models of funding a transaction are different for all three products. GPR prepaid cards use a "pay before" model, meaning that they draw from value that is pre-funded from a variety of sources into the card's account. Debit cards utilize a "pay now" model where funds are debited from a demand deposit account (DDA) at the time of the transaction. And credit cards use a "pay later" model where funds used to complete the transaction are drawn from a credit line and repaid to the card issuer at a later date.

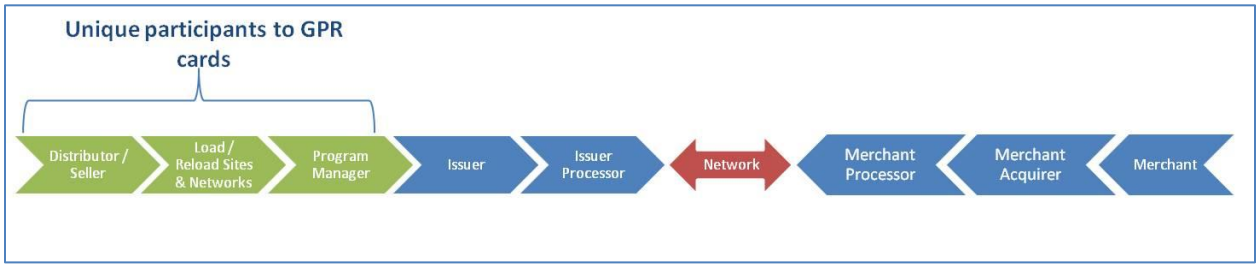
By their nature, debit and credit card issuance and management are under the direct distribution and control of the financial institution. The GPR prepaid card industry, however, has successfully developed a different delivery system to meet the product requirements of convenience and accessibility that includes a large number of non-bank service providers. Within the value chain, the GPR prepaid card industry has three additional participants that are not included in the traditional bank or debit card environment. These three participants are:

Program Manager: Under contract with a financial institution, the program manager designs and runs the card program. The program manager also supports issuance, delivery, and distribution of GPR cards and in some instances, is responsible for providing customer service.

Distributor / Sellers: The distributor often represents multiple GPR prepaid card products and works to develop a comprehensive contract network of sellers by shipping card inventories to the endpoint locations operated by the Sellers. Sellers, ranging from big box retailers, regional grocers, national drug store chains, C-stores and Internet retailers down to small bodegas, market the cards to customers.

Load / Reload Sites & Networks: A retail merchant that handles initial value loads or a Money Service Business (MSB) operating a network to provide reload services to cardholders through physical and virtual reload sites.

Figure 1: The GPR Prepaid Card Value Chain



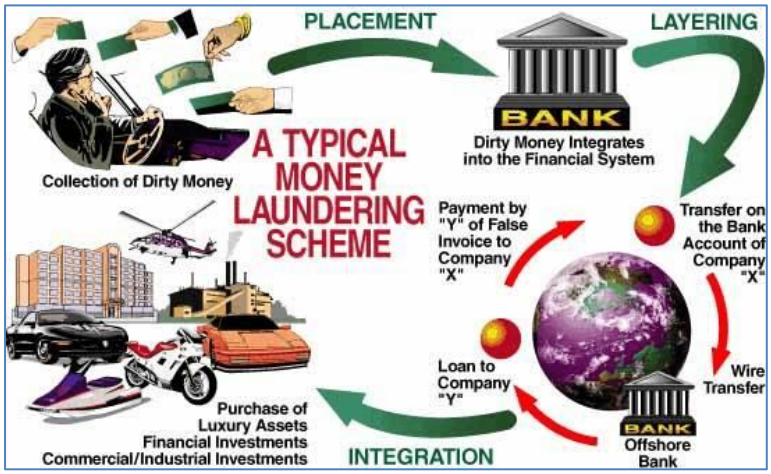
It should be noted that as the GPR prepaid card industry evolves, financial institutions have launched prepaid card programs and integrated the distribution, load, and program management functions internally. For example, in May 2012, JPMorgan Chase launched the Chase Liquid card. This card is distributed through Chase branch locations and value is added to the cards at branch locations or via Chase ATMs. Other financial institutions that have launched prepaid card programs include U.S. Bank, PNC, and Regions Bank.

II. Money Laundering and GPR Prepaid Cards

FinCEN describes money laundering as the process of making illegally-gained proceeds (i.e. "dirty money") appear legal (i.e. "clean").[6] This process is actually a three-stage process and involves the:

1. **Placement** of illegally-gained proceeds into the financial system.
2. **Layering** of these proceeds by conducting multiple financial transactions to make detection difficult.
3. **Integration** of these proceeds into the legitimate economy (e.g. investments in assets or business ventures, purchases of goods and services).

Figure 2: The Money Laundering Cycle[7]



Without proper risk measures in place, GPR prepaid cards could be used in each stage of the money laundering process. By way of example, in the placement stage, illegal funds are used to purchase and initially load prepaid GPR cards. During the layering stage, the illegal funds are transferred between GPR prepaid cards or the funds are withdrawn at ATMs to purchase and load additional GPR prepaid cards. Upon sufficient layering of the funds, the GPR prepaid cards are then used to integrate the funds through purchases, remittances, or cash withdrawals.

In order to mitigate the money laundering risks associated with GPR prepaid card programs described above, risk measures (through either regulatory agencies or self-regulation) have been or need to be implemented to mitigate the attractive money laundering attributes of these cards while at the same time minimizing any negative impact to legitimate users. From a risk mitigation standpoint, it should be noted that the risk of financial loss from money laundering is quite different from the loss risk of credit and debit card programs to the card issuer. In the case of credit and debit cards, when payment fraud activity occurs there is a measurable financial loss that is generally absorbed by the card issuing financial institution. In the case of the money laundering transaction cycle, there is no direct financial loss to the card issuer, distributor or seller. The primary risks associated with money

laundering faced by financial institutions include compliance, regulatory, and reputational risks.

III. Regulatory Environment: Anti-Money Laundering Measures

Money laundering has existed long before the advent of prepaid cards. In an effort to prevent and detect money laundering activities, Congress passed the Bank Secrecy Act (BSA) in 1970 requiring that U.S. financial institutions assist government agencies in their fight against money laundering. The Financial Crimes Enforcement Network (FinCEN), a bureau within the U.S. Treasury Department has the authority to issue and administer regulations under the BSA. These regulations include, but are not limited to:

> Filing of currency transaction reports (CTRs): CTRs must be filed for each deposit, withdrawal, exchange of currency, or other payment or transfer, by, through, or to a financial institution, which involves a transaction in currency of more than $10,000 with limited exceptions for "exempt persons".
>
> Filing of international transportation of currency or monetary instruments reports (CMIRs): CMIRs must be filed by each person (including a bank) who physically transports, mails, or ships currency, traveler's checks, and certain other monetary instruments in excess of $10,000 at one time into or out of the United States.
>
> Filing of suspicious activity reports (SARs): SARs must be filed by financial institutions with the Financial Crimes Enforcement Network (FinCEN) for any suspicious transaction that could be a possible violation of law or regulation.

The BSA has been amended multiple times since 1970, including the passage of the USA Patriot Act (Patriot Act) in 2001. As required by the Patriot Act, the U.S. Treasury Department, through FinCEN, adopted regulations that require financial institutions and MSBs to implement reasonable Customer Identification Procedures (CIP), also referred to as Know Your Customer (KYC). Given the previously noted GPR card value chain and its unique distribution model that includes nonbank financial institutions and MSBs, it is important to understand where each distribution participant falls under the BSA regulatory environment.

Financial institutions that issue prepaid cards are covered by BSA and therefore must comply with BSA regulations. The Federal Financial Institutions

Examinations Council (FFIEC) issues and updates a BSA/AML Examination Manual that provides guidance to examiners and the banking industry on identifying and controlling risks associated with money laundering. In the most recent manual, there is a section devoted to the examination procedures for assessing the adequacy of a bank's systems to manage risks associated with prepaid cards.

The load/reload networks that facilitate the transfer of funds onto GPR cards are required to register as MSBs with FinCEN and must comply with BSA regulations including the development and monitoring of an AML program by a designated compliance manager. Similar to the FFIEC, FinCEN has also issued a BSA/AML Examination Manual for MSBs.

Until recently, the BSA/AML obligations for the other GPR distribution participants – program managers and sellers – were not as defined as they were for issuers and load/reload networks. However, this changed on July 27, 2011, when FinCEN issued a final rule on prepaid access under the BSA that imposed BSA/AML regulatory obligations for both "providers" and "sellers" of prepaid access.[8] Without going into the full definition of the "provider" of prepaid access, it ultimately is the participant in a prepaid program that serves as the principal conduit for access to information from its fellow program participants. Based on the definition provided by FinCEN, this participant will most often be the program manager or the issuing financial institution (who already has BSA/AML obligations). If the program manager is deemed to be the "provider" by either the parties to the prepaid program or by FinCEN, it will be required to register as an MSB with FinCEN and comply with the same MSB regulations as the load/reload networks and other MSBs.

Certain "sellers" of GPR cards now also have BSA/AML obligations. FinCEN defines a "seller" of prepaid access as any person who receives funds or the value of funds in exchange for an initial loading or subsequent loading of prepaid access. However, only those "sellers" of GPR cards which can be used before customer verification or who have not implemented "policies and procedures reasonably adapted to prevent" the sale of prepaid access to funds exceeding $10,000 to any person on any day are covered under FinCEN's new rule.

Under the prepaid access rule, providers must register as MSBs, and both providers and sellers are required to implement AML programs that must include the following elements:

1. Procedures to collect, verify, and retain customer information including name, address, date of birth and identification number
2. Submission of SARs for suspicious transactions of $2,000 or more
3. Maintaining transactional information for a period of five years

The BSA regulations directly address anonymity concerns associated with GPR prepaid cards. GPR prepaid card issuers and MSBs facilitating the addition of funds to these cards cannot be in compliance with the BSA without implementing procedures to both know their customers and verify their customers are who in fact they claim that they are. Further, under FinCEN's most recent prepaid access ruling, GPR prepaid card program managers and sellers of these products could also be required to implement these procedures dependent upon the structure of the program or the type of prepaid access being sold. While anonymous GPR prepaid cards can be obtained through programs and issuers outside the United States (for example, http://instantvcc.eu/cards.html) that allows the anonymous cardholder to add additional value to the card, these products are ultimately prohibited in the United States through BSA/AML regulations. In fact, given FinCEN's prepaid access rule, there could be multiple parties that are required to implement and perform KYC or CIP procedures on individuals wishing to obtain and load value onto a GPR prepaid card depending upon the structure of the specific program.

IV. Industry Self-Regulation: Anti-Money Laundering Measures

In addition to the BSA/AML obligations imposed by regulatory authorities to mitigate the anonymity risks associated with GPR prepaid cards, industry participants, under FFIEC guidance as well as guidance from the Network Branded Prepaid Card Association, have adopted multiple measures that provide mitigation to money laundering risks of GPR prepaid cards. These measures generally address the convenience, accessibility, and liquidity of funds loaded into a prepaid account.

GPR prepaid card programs vary greatly as do the target audience for the different programs. For example, some GPR prepaid cards are targeted for the teen and student market, others target travelers, and many are intended to be a direct replacement to a traditional DDA. The variations in these programs make a "one size fits all" approach to risk mitigation impractical. Therefore, risk measures implemented for the various GPR prepaid card programs differ. For this reason, not all of the following risk measures might be adopted by every GPR prepaid card program available in the United States and these measures will also vary by card

program in terms of their specific limitations. [See Appendix for description and list of reviewed GPR prepaid programs]

Card Value Limits:

Thirteen of the fifteen reviewed GPR prepaid card programs disclose a maximum card value allowed within its respective cardholder terms and agreement. Of the thirteen programs that disclose a maximum card value, eleven of these programs have a maximum that is $10,000 or less and two programs have a maximum of $15,000. Of the two programs that do not disclose a card value limit, one program's cardholder terms and agreement states that "the maximum value of your card may be restricted." The remaining program does not impose a card value limit based on a phone conversation with the card issuer's customer service.

These maximum card values for many GPR prepaid card issued in the U.S. significantly limits their attractiveness for the placement of "dirty" money - the first stage of the money laundering process. To launder substantial amounts of money would require a money launderer to obtain and activate many prepaid cards. Many of the programs reviewed aggregate the value of all card accounts with a specific issuer to determine the maximum value. Therefore, an individual with two cards issued by the same financial institution that limited card value to $10,000 could not maintain a balance greater than $10,000 in total on the two cards combined.

Value Load Limits:

Value can be added to GPR prepaid cards through a number of methods. All of the programs reviewed offer value loading via direct deposit. All programs offered this with payroll checks and many also offer this load option with government benefit checks. Cash funding is another popular and widely accepted value load method. Cash value can be loaded onto cards through a variety of ways, including at the card issuing bank's ATMs and tellers or through reload networks and MSBs. Other value adding load funding options include checks, ACH transfers from DDAs, electronic transfers from debit and credit cards, transfers between prepaid cards, and even transfers from alternative payment providers such as PayPal. Access to these loaded funds depends on the deposit methodology used. Cash funding offers the quickest liquidity with funds generally available within 30 minutes of the load. Funds loaded via direct deposit are usually made available the day of the load. Fund's availability when loading via ACH and other electronic transfers can range from one to five days and with checks the availability can range from three to seven days.

Prior to describing the load limits in place, it should be noted that to add value to all cards beyond the initial load requires that the card be registered with the issuing financial institution per the USA Patriot Act discussed above. Given that some GPR prepaid cards are loaded with value prior to this registration, most of the card programs reviewed place more stringent load limit restrictions on initial card loads. Further, access to these funds prior to registration is restricted from foreign transactions and often cash withdrawals.

Thirteen of the fifteen card programs reviewed place varying limitations on adding value to its cards. These limits mitigate money laundering risks by making it more difficult to both place and layer large sums of "dirty" money onto GPR prepaid cards without having an extensive "money mule" or "smurf" network of individuals involved in the organization. A few of the programs reviewed have daily or monthly load limits regardless of the method or type of value load. The daily load limits generally range from $2,500 to $7,500 and the monthly load limits are as high as $10,000. However, most of the programs reviewed have different daily and monthly limit amounts that are dependent on the value load type and methodology. For these programs, the riskier the load type from a money laundering perspective, the more stringent the value limit. For example, in all programs reviewed with variable limits by load type, cash load limits were lower than load limits for direct deposits. Cash daily value load limits generally range from $500 to $2,000 while direct deposit daily load limits are as high as $7,500 day. Further, when considering these value load limits, value loaded across all cards held by a single cardholder within a card program are aggregated. Therefore, holding multiple cards within a GPR prepaid program would not allow the cardholder to exceed these limits and offer no advantages from a money laundering perspective. Further, many of the load networks and MSBs that facilitate the adding of value impose their own limitations on top of the issuing bank or program manager's value load limits per FFIEC AML guidance.

Spending and Cash Withdrawal Limits:

Spending and cash withdrawal limits reduce the money laundering attractiveness of GPR prepaid cards as it mitigates the risks of layering and integrating of "dirty" money – the final steps of the money laundering process. Every GPR prepaid card program reviewed imposes spending limits on its cards. A vast majority (twelve out of fifteen) of the programs impose maximum daily spend limits. These maximums generally range from $2,000 to $5,000 though one program does have a $10,000 limit. Three of the programs reviewed do not impose a maximum daily spend, but rather impose single transaction spend limits. Two of these programs do not allow

any single transaction of $5,000 or more while the other program limits transaction size to $600.

Most GPR prepaid cards allow for cash withdrawals through the same methods as debit cards. Value loaded onto a GPR prepaid card can be withdrawn via an ATM, Point-of-Sale (POS) terminals equipped with cash back functionality, and in-person at the card issuer's branch locations. Obtaining cash at the ATM or POS is the most common method of cash withdrawal from GPR prepaid cards; although POS cash-back withdrawal limits are often limited to less than $100 due to the merchant's cash handling limitations. Often times, the issuer of the GPR prepaid card is either unknown to the card holder and/or does not have a branch footprint near the cardholder so in-person cash withdrawals are rare. However, the recent emergence of financial institutions integrating the GPR prepaid card distribution model in-house, could lend itself to more in-person cash withdrawals.

Thirteen of the fifteen reviewed GPR prepaid card programs disclose maximum daily cash withdrawals allowed within its respective cardholder terms and agreement. These limits vary by withdrawal channel. Daily ATM withdrawal limits range from $300 to $3,000 with many having a daily maximum no greater than $500. In-person cash withdrawal limits are substantially higher than the ATM limits, ranging from $400 to $5,000. POS cash withdrawals are generally subject to the maximum daily spend limits discussed above. One of the programs that does not disclose its limits imposes a $500 daily withdrawal limit for the ATM and in-person channels based on a phone call with a customer service representative. The other program includes language in its cardholder terms and agreement stating that "we may limit the amount, number or type of transactions you can make on your card."

V. Unaddressed Risks with GPR Prepaid Cards

Although risk measures are currently in place to limit the attractiveness of GPR prepaid cards to facilitate money laundering, two unaddressed attributes of GPR prepaid cards might help facilitate money laundering – transferability and transportability. These traits are not unique to GPR prepaid cards and actually apply to any payment card types.

Even with robust CIP procedures in place under the auspice of the Patriot Act, payment cards can be transferred and used anonymously. It is very simple for a GPR prepaid card owner to load value onto cards and then give them, along with the cards' PIN values, to another individual for use. When using a card, there are no

requirements at the POS or ATM to provide identification to prove that the name on the card is in fact the person making the transaction. In fact, MasterCard's[9] operating rules do not allow for merchants to require ID for card transactions and Visa's[10] identification verification requirements for a retail transaction do not include positive cardholder identification.

For non-PIN verified transactions, network rules require that merchants confirm that a cardholder's signature matches the signature on the back of the card. Unfortunately, this process is rarely followed and more often than not, outright ignored at the POS since the merchant is rarely held liable for the acceptance of a fraudulent card transaction. As a way to mitigate this particular risk, card issuers should monitor the velocity, type, and location of both value loads and transactions to potentially identify this type of anonymous use.

Further, since GPR prepaid cards are nothing more than a thin piece of plastic with access to thousands of dollars, it is much easier to transport substantial sums of money compared to bulk cash. This portability element has been shown to be an attraction for money launderers seeking to move "dirty" money across borders.[11] Because of this feature of GPR prepaid cards and in an attempt to limit cross-border exchanges, FinCEN proposed a new rule that would require anyone entering the U.S. to disclose if they are in possession of more than $10,000 that is contained on a "tangible prepaid access device," which includes prepaid cards.[12] To enforce this proposed regulation, the Department of Homeland Security intends to develop the capability to identify individuals entering the U.S. carrying prepaid cards in excess of $10,000.

Enforcement of this proposed rule could prove to be both challenging and present privacy issues.[13] Also, as discussed previously, most GPR prepaid cards limit the amount of value that can be stored on the card's account to less than $10,000. While it is possible for multiple cards in aggregate to contain over $10,000 in value, it would be rare for a single card to have access to that dollar amount. Also, issuers and program managers aggregate card values thus having multiple cards with aggregate value of over $10,000 is a difficult and time consuming proposition requiring a money launderer to use cards from different programs and issuers. In the spirit of this proposed rule and in light of the portability of GPR prepaid cards, U.S. Customs and Border Protection should be alerted by any individual attempting to bring a large quantity of GPR prepaid cards across the border.

VI. Conclusion

As GPR prepaid card usage among consumers has grown, regulators and industry participants across the prepaid value chain have consistently taken steps to mitigate money laundering risks associated with them. Unfortunately, any monetary instrument, regardless of the risk mitigation in place, is available to facilitate money laundering at some level. Given both the regulatory and industry measures in place for mitigating money laundering risks associated with U.S.-issued GPR prepaid cards, these products are no longer the attractive instruments for money laundering that they once might have been.

The largest impact to diminish their attractiveness came when identification and registration was required - to load a card with value and to gain full use of the card requires that the card be registered to an owner – with the resulting loss of anonymity. Access to GPR prepaid products has become more controlled and the convenience of accessing large amounts of value is limited through limitations on the amount of value that they can store, the velocity and amount of value that can be loaded onto the card's account, and purchase and cash withdrawal transaction spending limits.

Although the U.S. GPR prepaid card industry is regulated from a money laundering perspective, concerns on GPR prepaid cards issued outside of the United Sates remain significant. Anonymous cards can be found outside of the United States, and the controls that issuers place on these cards often vary significantly from U.S.-issued cards. Anonymous cards without value load thresholds and spending limits are attractive money laundering instruments and pose significant challenges for law enforcement to identify illegal activities and the individuals behind them. Efforts to prevent these types of cards from crossing U.S. borders should be of high importance for law enforcement and declaration requirements at the border about the number and value of these instruments should be considered. An individual entering the United States with a large quantity or value of foreign-issued anonymous GPR prepaid cards should raise a red flag with border patrol and custom officials. In an effort to prevent the use of these cards in the United States, financial institutions and other ATM operators should consider imposing stricter cash withdrawal limits on foreign-issued GPR prepaid cards. Finally, efforts should be undertaken between U.S. agencies and foreign law enforcement agencies and regulatory bodies to collaborate and influence regulation of these products in foreign jurisdictions.

In his February 2007 paper, Sienkiewickz noted that "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." Since then, both regulators and the industry have taken the necessary steps to greatly mitigate money laundering risks associated with GPR prepaid cards issued in the United States. However, GPR prepaid cards issued outside of this country still pose a threat.

Appendix

Fifteen GPR prepaid card programs were reviewed. These programs are a sample of at least one GPR prepaid card from some of the top U.S. prepaid issuers by 2011 purchase volume according to the Nilson Report[14] and are assumed to be representative of the U.S. GPR prepaid card market.

List of GPR prepaid card programs reviewed:

1. American Express BlueBird
2. Chase Liquid
3. Comerica Convenience
4. GE Capital Retail Bank WalMart MoneyCard
5. Green Dot Bank Prepaid
6. H&R Block Emerald
7. MetaBank READYDebit
8. MetaBank AccountNow
9. MetaBank NetSpend
10. PNC SmartAccess
11. Synovous Bank Green Dot
12. The Bancorp Bank Approved
13. The Bancorp Bank PayPal
14. The Bancorp Bank RushCard
15. Wells Fargo Prepaid

References

[1] "The 2010 Federal Reserve Payment Study: Noncash Payment Trends in the United States 2006 - 2009." *Federal Reserve System*, April 5, 2011.

[2] Ibid.

[3] "Loaded with Uncertainty: Are Prepaid Cards a Smart Alternative to Checking Accounts?" *The Pew Charitable Trusts*, September 6, 2012.

[4] Romich, Jennifer L., Sarah Gordon, and Eric Waithaka. "A Tool for Getting By or Getting Ahead? Consumers' Views on Prepaid Cards." Networks Financial Institute Working Paper 2009-WP-09, October 1, 2009.

[5] Sienkiewicz, Stanley. "Prepaid Cards: Vulnerable to Money Laundering?" Federal Reserve Bank of Philadelphia Payments Card Center Discussion Paper No. 07 – 02, February, 2007.

[6] "History of Anti-Money Laundering Laws." *FinCen*. Retrieved from http://www.fincen.gov/news_room/aml_history.html.

[7] "The Money Laundering Cycle." *United Nations Office on Drugs and Crime*. Retrieved from http://www.unodc.org/unodc/en/money-laundering/laundrycycle.html.

[8] "Bank Secrecy Act Regulations – Definitions and Other Regulations Relating to Prepaid Access (Final Rule)." Federal Register 76:146 (July 29, 2011) p. 45403.

[9] "MasterCard Rules December 12, 2012." *MasterCard Worldwide*, p. 5-15.

[10] "Visa International Operating Regulations October 15 2012." *Visa Inc.*, p. 488.

[11] "Money Laundering Using New Payment Methods." *Financial Action Task Force*, October, 2010.

[12] "Bank Secrecy Act Regulations – Definition of 'Monetary Instrument' (Notice of Proposed Rulemaking)." Federal Register 76:200 (October 17, 2011) p. 64049.

[13] Matonis, Jon. "Department of Homeland Security to Scan Payment Cards at Borders and Airports," Forbes.com, November 7, 2012.

[14] "Top 50 Prepaid Card Issuers." *The Nilson Report*, Issue #997, June 2012.