U.S. Department of Justice

National Drug Intelligence Center

Office of the Director

319 Washington Street, 5th Floor
Johnstown, PA 15901-1622

(814) 532-4601
Fax: (814) 532-4690

January 17, 2007

Mr. Anil D. Aggarwal
Chairman of the Board
Network Branded Prepaid Card Association
P.O. Box 180
Sherborn, MA 01770

RE: Response dated November 15, 2006, to National Drug Intelligence Center (NDIC) Assessment *Prepaid Stored Value Cards: A Potential Alternative to Traditional Money Laundering Methods*.

Dear Mr. Aggarwal:

This is in response to your letter dated November 15, 2006, regarding the NDIC Assessment *Prepaid Stored Value Cards: A Potential Alternative to Traditional Money Laundering Methods.* While we understand your concern, NDIC is quite confident in the accuracy of this Assessment. In fact, the Assessment has received overwhelmingly positive feedback from representatives of various federal agencies including the Executive Office of National Drug Control Policy (ONDCP), U.S. Department of the Treasury, U.S. Secret Service, U.S. Department of Homeland Security, and the Drug Enforcement Administration (DEA). Also, the Assessment was examined by the applicable representatives at ONDCP, Treasury (main), DEA, and the Financial Crimes Enforcement Network (FinCEN) prior to publication. Moreover, NDIC indicated in the Assessment (on page 8) that because the cards have demonstrated economic benefits, any regulations applied should be balanced in order to protect consumers without inhibiting growth of the industry. However, there clearly exists vulnerability in the prepaid card industry for exploitation for illicit money laundering purposes as reported in our Assessment. From the concerns you expressed in your letter, and our item by item response which follows, it is also clear that most of your concerns can be attributed to ambiguity that exists in the roles and responsibilities of the numerous participants in the prepaid card industry. This ambiguity has been recognized by the U.S. Department of the Treasury and, as stated within our Assessment, new regulations designed to clarify the roles and obligations of issuers, sellers, and redeemers or prepaid cards are currently under review.

NDIC has considered each of the concerns that were raised by the Network Branded Prepaid Card Association (NBPCA) and provides the following responses:

NBPCA Concern: **(Item 1)** NBPCA asserts that network branded prepaid cards are not "unregulated or loosely regulated" because all such cards are issued by highly regulated financial institutions, and as such are "subject to exam, review, and oversight and are managed by entities that are required under applicable law (e.g., the Bank Secrecy Act) to have anti-money laundering practices and policies and related internal controls in place."

NDIC Response: The NDIC Assessment does not indicate that stored value products are unregulated—in fact, the term "unregulated" is never used in the Assessment. However, it is very clear that these products are, in fact, loosely regulated in comparison to many other types of financial products.

Issuers, sellers, and redeemers of stored value are specifically defined as Money Services Businesses (MSBs) by the Bank Secrecy Act (BSA). However, because the terms used in the MSB definition are not clearly defined, it is unclear which participants in stored value card programs—including the "highly regulated" financial institutions—function as "issuers, sellers, and redeemers" under the current regulations. Additionally, issuers, sellers, and redeemers of stored value are specifically exempt from many MSB BSA requirements. According to FinCEN, the only applicable federal requirements for issuers, sellers, and redeemers of stored value are the Currency Transaction Report (CTR) rule and the requirement to implement anti-money laundering (AML) policies. Because the roles of stored value program participants are not specified by the BSA, it is unclear exactly which of these participants are responsible for implementing the required AML compliance programs. For the purposes of NDIC's Assessment, the following terms were used to define the roles played by these parties:

- 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, automated teller machines (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.

Conversely, banks and other non-bank financial institutions that offer traditional account relationships—which provide services similar to those of network branded prepaid cards, including the ability to deposit, withdraw, and electronically move funds—are typically subject to a great deal of regulatory oversight. Although most network branded stored value products meet the description of "accounts" set forth in

the USA PATRIOT Act's International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001, which defines an account as "a formal banking or business relationship established to provide regular services, dealings, and other financial transactions," the Act does not specifically identify stored value products as accounts. Therefore, it is unclear whether many of the regulations which apply to traditional account relationships—including Customer Identification Program (CIP) requirements—also apply to stored value products.

Because the roles of issuers, sellers, and redeemers of stored value are not defined by the BSA, banks are clearly responsible only for "exam, review, and oversight" of the program manager's pooled account, and not for activity conducted by the program manager's customers. Many proactive and responsible banks, program managers, and processors have implemented exam, review, and oversight programs; however, it remains unclear which of these parties should legally bear this responsibility.

NBPCA Concern: **(Item 2)** NBPCA claims that the following four-bulleted factors decrease network branded cards' usefulness for money laundering purposes.

- Because all network branded cards are processed through an electronic payments system, the issuer can "terminate a card's usefulness at any time and without having possession of the card."
- The funds associated with prepaid cards can be frozen by the card issuer or forfeited entirely, unlike paper instruments which hold their own value and cannot be remotely stopped.

NDIC Response: The purpose of the USA PATRIOT Act's International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001 is "to increase the strength of United States measures to *prevent*, *detect*, and *prosecute* international money laundering and the financing of terrorism." While the ability to stop the flow of funds after money laundering activity has been detected is highly valuable, the above referenced factors provide only that functionality and do not contribute to the prevention, detection, or prosecution of money laundering offenses. The Assessment asserts that the stored value industry needs standards by which money laundering can be prevented, identified, and prosecuted; not merely stopped after it has been detected.

- Network branded cards "leave an easily traceable trail of use—including place, time, date, amount, and often the nature of the transaction"—which, in the case of personalized cards, is linked to a known person.

NDIC Response: While it is true that network branded cards leave an electronic record which includes place, time, date, amount, etc. of each transaction, there are no regulations which determine the length of time each program manager must require these records to be maintained. When money laundering occurs, these records are invaluable to the investigation and eventual prosecution of the activity, and must be maintained long enough to benefit law enforcement. Money remitters, another type of MSB, are required to maintain relevant records for a minimum of five years. As there

is no Suspicious Activity Report (SAR) filing requirement for issuers, sellers, or redeemers of stored value products, less diligent program managers may not chose to make law enforcement aware of any activity which may be identified using this transactional data.

Additionally, there is no guarantee that this transactional data is linked to a known person. As the goal of money laundering is to separate the funds from their illicit source, it is highly unlikely that a launderer would chose to use his or her true identity to obtain a network branded card; in fact, it is most likely that these cards will be associated with fraudulent identification when used to facilitate money laundering.

- Because funding for cards is often "made by check, bank credit or debit card, an account-to-account transfer, or a funds transfer via an [automated clearing house] transaction from an existing corporate or government bank account" the underlying funds are subject to BSA or Financial Action Task Force AML requirements.

  NDIC Response: NBPCA's implication seems to be that the cards, therefore, do not represent a money laundering risk because the "tainted" funds have already entered the financial system through other means. While the NDIC Assessment focuses primarily on the placement stage of money laundering—the stage in which tainted cash first re-enters the legitimate financial system—it is important to recognize that these cards are also used during the layering and integration stages, in which the sources of funds would include checks, debit cards, account-to-account transfers, etc. Although those funds were, consequently, already subject to BSA there are still opportunities to "prevent, detect, and prosecute" money laundering during the later stages of the process. Exploiting opportunities to detect illicit money movement in the later stages of the money laundering process is especially important when combating terrorist financing.
  While use of these types of funding sources likely accounts for a large portion of legitimate cardholder activity, many network branded cards are designed for use by unbanked and underbanked customers. The threat of use of these cards for the placement of cash is very real, and recent developments in the prepaid market will make it even easier for money launderers to add cash value to prepaid cards. MasterCard Inc. has developed a point of sale (POS) network called rePower which will allow customers to reload network branded cards with cash, and Visa U.S.A. has already launched ReadyLink, a POS system that will also allow unbanked customers to load cards with cash. ConveniaLoad allows some network branded cardholders to reload their cards with up to $999 in cash at any Wells Fargo, Bank One, U.S. Bank, or Wachovia locations without establishing a relationship with that bank.

NBPCA Concern: **(Item 3)** NBPCA asserts that it is untrue that "anonymous" prepaid cards often have liberal load limits and frequently permit ATM access. Anonymous cards cannot be used in this fashion because the only "anonymous" cards are semi-open system (prepaid gift) cards which cannot be reloaded or redeemed at ATMs. Additionally, NBPCA claims that all open-system cards are "strictly" regulated by the payments networks, which impose daily limits on

the amount of cash that can be added to or withdrawn from the card. "Uniform compliance" with guidelines is ensured because the payment networks' guidelines "extend globally."

> ***NDIC Response:*** The NDIC Assessment did not indicate that "anonymous" cards offer these types of functionality; rather, the Assessment indicates that liberal limits on card value and reloading exists regardless of identification standards. The text of the Assessment is as follows: "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." However, cards that are obtained using fraudulent identifying information might as well be anonymous.
>
> NDIC research indicates that U.S. program managers allow various daily cash reloading limits as well as daily total card value limits, sometimes in excess of the guidelines established by the payments networks. At the time the research for the Assessment was completed, Wired Plastic—which offers Visa and MasterCard branded products—allowed unlimited cash reloading at select locations. As of November 22, 2006, when an NDIC representative spoke to a Wired Plastic customer service agent named Annie, Wired Plastic had no daily total card limit and a daily cash load limit of $2,500. According to the U.S. Department of the Treasury, MasterCard suggests a daily total card limit of $2,500; Wired Plastic's policies are clearly a violation of this guidance.
>
> A review of international card programs indicates that payments networks' guidelines are not enforced globally. For example, ExactPay, a Visa branded prepaid card issued by First Curacao International Bank N.V., a private offshore bank in Curacao that operates under the bank secrecy laws of the Netherlands Antilles, is specifically marketed to allow anonymous, unlimited financial transactions.

NBPCA Concern: **(Item 4)** NBPCA claims that it is inaccurate to state that it is unclear whether the providers of stored value products are required to perform CIP "because most network branded prepaid cards are issued by banks or other regulated financial institutions which are subject to the Bank Secrecy Act (BSA) [therefore] such institutions routinely require CIP for the issuance of re-loadable, cash-accessible prepaid cards."

> ***NDIC Response:*** NBPCA implies that issuing banks verify the identities of cardholders in accordance with appropriate federal regulations. According to FinCEN, the issuing bank's obligation to verify its customers' identities ends with the account owners—in this case, the stored value program manager—and does not extend to the owners' customers (the cardholders).
>
> Because stored value products are not specifically named in the USA PATRIOT Act's definition of accounts, NDIC analysis concluded that it is unclear whether these products are accounts and therefore also unclear whether CIP should be performed for each cardholder. The USA PATRIOT Act requires that all persons who hold accounts have their identities verified and compared to the identities of known or

suspected terrorists or terrorist organizations, in the interest of protecting national security. If neither the banks nor the stored value program owners are performing identity verification, there is no way to prevent known and suspected terrorists from obtaining stored value cards, and therefore having access to bank account-like functionality.

NBPCA Concern: **(Item 5)** NBPCA states that NDIC suggested that "the practice of issuing prepaid cards without photo identification is riskier than the practices used to verify identity with other payment products." NBPCA also notes that practices used to identify customers are derived directly from the credit card industry; that "financial institutions use well-defined, non-documentary methods, as permitted by CIP rules and regulatory guidance, to verify the identity of the customer."

NDIC Response: NDIC did not indicate that issuing prepaid cards without photo identification is "riskier" than methods used to verify other payment products (i.e., credit cards); rather, NDIC indicated that this method is riskier than the methods (including photo identification) used to verify the identities of persons opening traditional bank accounts due to the bank account-like functionality offered by the cards. The text of the NDIC Assessment is as follows: "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."

NBPCA Concern: **(Item 6)** NBPCA asserts that issuing banks have access to transactional data compiled by stored value card processors and use this data to monitor suspicious activities.

NDIC Response: While banks do have access to transactional information available to the processor—which is necessary to perform AML duties—NDIC's analysis concluded that, under current regulations, the issuing banks' AML responsibilities end with the program manager's activities and do not extend to cardholders' activities. Again, all MSBs—including the ambiguous issuers, sellers, and redeemers of stored value—are clearly required to implement their own AML programs; however, until the rules concerning issuers, sellers, and redeemers of stored value are clarified it remains unclear whether banks should play a greater role in this process.

NBPCA Concern: **(Item 7)** NBPCA suggests that card readers can be used only to provide the card number and issuing bank identification number, and cannot be used to determine the value of network branded cards.

NDIC Response: While the value associated with any particular stored value card is clearly not available from the magnetic stripe, a card—coupled with a card reader connected to the payments networks—can be used to access processor data in order to determine the general value of the card. For example, by authorizing a specific amount, law enforcement officials could determine whether that card is worth more or less than the amount authorized. This function would be especially valuable to law enforcement if stored value becomes included in the definition of Reports of International Transportation of Currency or Monetary Instruments.

One mission of NDIC is to identify threats and vulnerabilities that may be exploited by drug money launderers, and offer recommendations to address those when applicable. The referenced Assessment does such by identifying the cards as an emerging threat and a potential alternative to traditional money laundering methods, and it offers recommendations to address this emerging threat.

Sincerely,

Irene S. Hernandez
Acting Director

Cc: Mr. Charles Klingman (U.S. Department of the Treasury)
Mr. L. Jeffrey Ross (U.S. Department of the Treasury)
Mr. Tom Lasich (Department of Homeland Security)
Mr. Paul Valvano (Department of Homeland Security)
Mr. Donald C. Semesky (Drug Enforcement Administration)
Mr. William F. Baity (Financial Crimes Enforcement Network)

Return to *Prepaid Stored Value Cards: A Potential Alternative to Traditional Money Laundering Methods*