Statement of

Kirsten Trusko
President and Executive Director

of the
Network Branded Prepaid Card Association

Before the

Subcommittee on Fiscal Responsibility & Economic Growth

Senate Finance Committee

Hearing on Tax Fraud through Identity Theft

March 20, 2012

Chairman Nelson, Ranking Member Crapo, and members of the Subcommittee, I appreciate the opportunity to appear before you today on behalf of the Network Branded Prepaid Card Association (NBPCA) and its members. My name is Kirsten Trusko and I am NBPCA's President and Executive Director. I have served in this position for going on three years. Prior to joining the NBPCA, I co-founded and lead the prepaid card and consumer driven healthcare management consulting and technology practices for a top 5 global consulting firm.

The NBPCA is a non-profit trade association founded in 2005 representing a diverse group of organizations that take part in delivering network branded prepaid cards to consumers, businesses and governments. Our membership includes financial institutions, card organizations, processors, program managers, marketing and incentive companies, card distributors, law and media firms and touches a vast majority of the network branded prepaid cards.

Overview of Network Branded Prepaid Cards

Network branded prepaid cards comprise a diverse group of extraordinarily popular products that serve a vital public need. Network branded prepaid cards bear the logo of a payment network (American Express, Discover, MasterCard or Visa), and work similar to credit and debit cards. Prepaid cards are issued by banks or licensed money service businesses. Prepaid cards allow for customized payment solutions for a range of payment situations that in the past were unwieldy and expensive. Card issuers can leverage the flexibility of network branded prepaid cards to create solutions that address many common consumer needs, offering a safe, easy-to-use alternative to paper-based products such as checks, cash, and even vouchers.

There are several parties involved in bringing prepaid cards to market. They include: (1) the payment networks, (2) the banks or licensed money service businesses which issue the prepaid cards, (3) the program managers which assist the issuing bank in setting up, marketing and operating the card program, (4) the processors which process the card programs on behalf of the issuers and program managers, and (5) the retailers and other third parties who distribute the cards to businesses and to consumers.

General Purpose Reloadable Cards

The general purpose reloadable (GPR) card is one of the most flexible prepaid products. GPR cards are typically purchased by a consumer for their personal use to pay for point-of-sale purchases, pay bills, and/or access cash at ATMs. GPR cards may be purchased online or in retail locations from a variety of providers. Funds may be loaded onto the card by the consumer at retail locations offering prepaid card reload services or by direct deposit of wages or benefits.

Convenient access to these prepaid cards with pricing that is often lower than other financial tools have been key drivers of their popularity among consumers. The cards are available in more than 200,000 retail locations and bank branches. The wide availability of the cards is particularly appealing to the 60 million Americans who are unbanked or underbanked, who have limited or no access to bank branches in their neighborhoods or cannot qualify for checking accounts.

How GPR Cards are Obtained

GPR cards are typically obtained in one of two ways. A potential cardholder may go to a web site of one of the many financial institutions or program managers which

offer GPR cards. Alternatively, the consumer may go to a retail location or check cashing service to obtain a temporary prepaid card. In the retail environment, the customer would hand over to the retailer funds for the purchase of the card and the initial amount to be loaded to the card. The retailer will then send a message to the processor of the temporary card indicating that the card had been purchased and the amount on the initial value load. The processor then activates the temporary card for the value of the initial load.

These temporary cards are essentially limited-functionality cards, with value loads that generally do not exceed $500, and do not provide cash access or permit the card to be reloaded until the purchaser has provided personal information to the program manager or processor, and that information is then verified. Once the information has been verified, the program manager or processor sends a fully functional personalized prepaid card to the purchaser. Once the fully functional card is received by the cardholder, and the cardholder activates the card, the card is reloadable by the cardholder. The cardholder is provided an ABA routing number and an account number which is associated with the prepaid card account, which the cardholder can provide to employers or other parties, including government agencies, for purposes of direct depositing wages, government benefits or tax refunds to the cardholder's prepaid card account.

Bank Secrecy Act (BSA)

GPR cards are issued by regulated banking institutions or by other highly regulated organizations, such as state-licensed and FinCEN-registered money service businesses (MSBs). Issuers of prepaid cards are subject to examination, review and

supervision by either state banking or other departmental regulators, federal banking regulators, the Internal Revenue Service or a combination of all of these agencies.

Banks which issue GPR cards are legally required by the USA PATRIOT Act and the BSA to have an effective anti-money laundering (AML) compliance program that addresses customer due diligence, suspicious activity monitoring, currency transaction reporting and OFAC screening, as well as other BSA reporting and recordkeeping requirements.

Additionally, under a recent final rule issued by FinCEN addressing prepaid access, providers and sellers of GPR cards are classified as MSBs and are required to maintain effective BSA compliance programs that address customer due diligence, suspicious activity monitoring, currency transaction reporting and OFAC screening, as well as other BSA reporting and recordkeeping requirements.

Under the BSA, both the issuer and provider of a GPR card have the obligation to implement risk-based procedures for verifying the identity of each customer to the extent reasonable and practicable. The procedures must enable the issuer and or provider to form a reasonable belief that they know the true identity of each customer. These procedures must be based on the assessment by the issuer and provider of the relevant risks, including those presented by the various types of accounts maintained by the issuer, the various methods of opening accounts provided by the issuer and provider, the various types of identifying information available, and the issuer's/provider's size, location, and customer base.

As part of their BSA compliance programs, issuers and providers of GPR cards must collect the following four pieces of personal information from a prospective

cardholder: (1) name, (2) street address, (3) identification number, and (4) date of birth. This information is collected by the program manager or processor when the purchaser either acquires the card online or contacts them to convert the temporary card to a fully functional card. After this information is collected, as required by the BSA, the program manager or processor will use non-documentary verification systems in an attempt to verify the prospective cardholder using the information provided. The applicant is verified using one or more identity verification services which are used by financial institutions or brokerages to verify customer identity. The process used to verify identity is the same as is used by a financial institution when a consumer applies for a credit card or online bank account. The process may be automated, manual or a combination of manual and automated processes, depending on the program manager and processor. If the information is successfully verified, the cardholder is approved for a fully functional GPR card. If the information is not successfully verified, the program manager or processor will either decline to establish the account or require the prospective cardholder to provide additional information, such as a copy of a government-issued identification card, prior to approval of the cardholder. If the program manager or processor cannot successfully verify the identity of the prospective cardholder, the account is not established.

Identity Theft

As is the case with the providers of credit cards and other financial products, issuers and program managers of prepaid cards are faced with fraudsters who attempt to establish prepaid card accounts using stolen identities. The process of preventing fraud starts well before the fraudster tries to load the funds to a prepaid card—the

original identity theft has occurred in the fraudster's efforts to gain the tax refund in the first place. The prepaid card is just the acceptance method.

Industry Efforts

The NBPCA acknowledges that, like any payment system, prepaid cards are susceptible to abuse and misuse and, in particular, the use of prepaid cards in connection with tax return fraud was identified as a significant problem during the prior tax return processing season. Once this problem was identified, members of the NBPCA acted aggressively to address this problem.

Prepaid Anti-Fraud Forum

In 2011, the NBPCA formed the Prepaid Anti-Fraud Forum (PAFF). PAFF brings together leading practitioners, and collaborates with law enforcement, establishes leading practices, and hosts educational forums for members to learn from guest experts. To combat tax fraud the PAFF solicited input from industry participants and, prior to the beginning of this tax return processing season, compiled a confidential handbook discussing various fraud mitigation strategies. This confidential handbook has been shared with issuers, program managers and processors of prepaid cards. Although this statement necessarily omits greater detail, to avoid tipping off potential fraudsters on methods being implemented to mitigate the use of prepaid cards in tax refund fraud, the anti-fraud practices can be broken down into four high-level categories:

1. Fraud detection and processing at the application stage;

2. Fraud detection and processing at the post-application stage;

3. Fraud detection and processing at the ACH deposit stage; and

4. Additional questions triggered by suspected fraudulent ACHs.

As part of these processes, among other actions, industry participants are:

a. Watching for patterns of suspicious activity when activating the GPR card.

b. Identifying “hot” ZIP codes and fraud trends in various regions of the country.

c. Undertaking transaction monitoring and suspicious activity monitoring.

d. Undertaking additional processes when incoming ACH loads are identified as being an income tax refund.

e. Rejecting and returning ACH value loads to Treasury when there is a suspicion that the transaction may be the result of fraud.

f. Freezing accounts when fraud is suspected.

g. Filing suspicious activity reports when fraud is suspected, which reports are available to law enforcement and the IRS.

h. Working with the IRS, Department of Justice, and FBI when new fraud trends are identified.

i. Working with victims of identity theft, including supplying to the consumer all the information they have available on the ID theft, all records including those of the account opening, and any transactions on the account.

j. Assisting federal and local law enforcement in investigations of suspected tax refund fraud.

The industry efforts have so far resulted in over $1Billion of value loads to prepaid cards being returned to the IRS based on attempted fraudulent tax refunds.

The PAFF is developing a close working relationship with the IRS Criminal Investigation Division, the Department of Justice, and the FBI to enable more effective information sharing to prevent the use of prepaid cards in tax refund fraud.

IRS Efforts

As the IRS implements additional processes to prevent tax refund fraud, we would caution that such processes must take into consideration the large number of legitimate filers who rely on prepaid products to receive their tax refunds. The fraud-prevention benefits of additional processes and procedures must be balanced against the burdens borne by the unbanked taxpayers who are depending on the timely receipt of their tax refunds. Such processes should be implemented in a manner reasonably anticipated to takes into account the risks presented and the numerous safeguards already implemented by the industry.

Thank you for the opportunity to appear before you today . The NBPCA stands ready to work with you and I would be happy to answer any questions you may have.

DOCS/1096526.7