S. HRG. 113–907

PRIVATE INDUSTRY'S ROLE IN STEMMING THE TIDE OF PHONE SCAMS

HEARING

BEFORE THE

SPECIAL COMMITTEE ON AGING

UNITED STATES SENATE

ONE HUNDRED THIRTEENTH CONGRESS

SECOND SESSION

WASHINGTON, DC

WEDNESDAY, NOVEMBER 19, 2014

Serial No. 113–32

Printed for the use of the Special Committee on Aging

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
46–919 PDF WASHINGTON : 2022

SPECIAL COMMITTEE ON AGING

BILL NELSON, Florida, *Chairman*

ROBERT P. CASEY JR., Pennsylvania
CLAIRE MCCASKILL, Missouri
SHELDON WHITEHOUSE, Rhode Island
KIRSTEN E. GILLIBRAND, New York
JOE MANCHIN III, West Virginia
RICHARD BLUMENTHAL, Connecticut
TAMMY BALDWIN, Wisconsin
JOE DONNELLY Indiana
ELIZABETH WARREN, Massachusetts
JOHN E. WALSH, Montana

SUSAN M. COLLINS, Maine
BOB CORKER, Tennessee
ORRIN HATCH, Utah
MARK KIRK, Illinois
DEAN HELLER, Nevada
JEFF FLAKE, Arizona
KELLY AYOTTE, New Hampshire
TIM SCOTT, South Carolina
TED CRUZ, Texas

KIM LIPSKY, *Majority Staff Director*
PRISCILLA HANLEY, *Minority Staff Director*

CONTENTS

PRIVATE INDUSTRY'S ROLE IN STEMMING THE TIDE OF PHONE SCAMS

WEDNESDAY, NOVEMBER 19, 2014

U.S. SENATE,
SPECIAL COMMITTEE ON AGING,
Washington, DC.

The Committee met, pursuant to notice, at 2:00 p.m., Room 562, Dirksen Senate Office Building, Hon. Bill Nelson, Chairman of the Committee, presiding.

Present: Senators Nelson, McCaskill, Donnelly, Collins, and Scott.

OPENING STATEMENT OF SENATOR BILL NELSON, CHAIRMAN

The CHAIRMAN. Good afternoon.

Senator Collins and I have run this committee in a bipartisan way and we decided early on that one of the things we wanted to do in looking out for the interest of senior citizens was to go after the people who are perpetrating fraud on them. We first started out focusing on the Jamaican phone scams. Then, we moved on to tax identity theft, Social Security fraud, and then some very despicable grandparent scams. We set up a fraud hotline, where we have received thousands of calls for help, and for the record, that number is 855–303–9470.

Fraud is going to continue, not only against seniors, but against all people, but we started chipping away at it with regard to seniors. After the Jamaican phone scam hearing, new legislation was passed and signed into law in Jamaica and it spoke to the specific crimes that were being committed against our seniors, where these syndicates down there would call seniors and basically seduce them into sending money out of their bank accounts. The Jamaican authorities have made 100 arrests, but there have been only a handful of convictions, and we still are pressing for extradition. You extradite one of them here and let an aggressive U.S. Attorney go after him and put him away in the slammer and the rest of the fraudsters down in Jamaica will get the message.

We have pushed agencies to coordinate their efforts to go after people taking advantage of our seniors. We have encouraged law enforcement to actually prosecute the lawbreakers and, therefore, to scare away the copycats, and, we have pressed private industry to be good corporate citizens.

Today, Senator Donnelly and I introduced legislation to make it easier for seniors to actually know who is calling them and to give them tools to protect themselves from these fraudsters. This legis-

lation which we have just put out as part of the educational process, called the Phone Scam Prevention Act, I encourage our members to take a look at it.

Now, the most common scam begins with a fraudster placing—and "fraudster," by the way, is too nice a term—thugs, criminals. The most common scam begins with them placing phone calls to unsuspecting individuals, informing them that they have won a foreign lottery, or that a grandchild has been injured or arrested, and then these thugs tell their potential victims that they must make an advance payment to cover taxes and other fees before their lottery winnings can be released, or that the money is needed to help the grandchild who is now hurt or in jail.

This criminal thug instructs the senior to go to a retail store to purchase a reload card, and the victim will pay the cashier the amount of the money that they wish to load onto the card, and as soon as the transaction is complete, then that reload card carries that value. Each of the cards—and this is just one example—they have a PIN number, and they scratch off that PIN number—it is unique to the amount of money put on that card—and it is used, that PIN number, to apply the card's fund to some other account, like a prepaid debit card account, so, when the victim provides the PIN number to the scammer, the thug can immediately apply that money that has been loaded onto that reload card to the debit card that is held by the thug.

Now, recognizing the fraud associated with these kind of products, many of the companies have acted without regulatory or legislative action. Two of the debit card companies here today, Green Dot and InComm, have announced plans to drop these products that have been used so effectively by the thugs, and, even though these products can serve very legitimate purposes, these two companies have decided to do the right thing and we certainly applaud you all about that and we are looking forward to hearing from you.

The third major debit card company, Blackhawk, has also tightened up its security measures on a similar reloadable card. This company have cited this committee's work in fighting fraud as one of the reasons why you have made the changes, and we are looking forward to hearing about those changes and what is the security of the card that you continue to promote.

What Susan and I have done in this committee, we tried to make a difference in the lives of a few of our seniors, and we are going to hear today from private industry, the debit card companies, and the retailers about why they have taken the actions they have taken.

Now, let me say that in an hour, we are going to have a series of five votes, so we are going to try to compress this thing in, because we would not in any way have you wait in recess until we could get back from the votes. That would just take too long in the course of conducting five votes.

Senator Collins.

OPENING STATEMENT OF SENATOR SUSAN M. COLLINS, RANKING MEMBER

Senator COLLINS. Thank you very much, Mr. Chairman.

I would ask unanimous consent that my entire statement be printed in the record because I am going to shorten my remarks in light of the votes so we have more time for our witnesses.

Before we hear from our witnesses, however, I want to take this opportunity to personally thank you for your leadership of this committee, which has been tremendous, and for the unfailing courtesy that you have shown to me, as your Ranking Member, to the other members of this committee, and to those who have testified before us. That has truly been a hallmark of your tenure as the Chairman, and our achievements as a committee trace directly to the bipartisan, indeed, nonpartisan tone that you set and the spirit of comity and cooperation that have prevailed as a result, so, I thank you for that great leadership.

I also want to commend your staff, as well as my own staff, and thank them for their hard work during the past two years. It is, as you mentioned, fitting that the last hearing that you and I will lead as the Chairman and Ranking Member examines once again the problem of scams targeting American seniors and how we can stop them. This incredibly important topic has rightfully been the focus of much of our hearings during the past two years. Indeed, we have held eight hearings on frauds and other scams targeting our seniors, and as in the case of the Jamaican government changing its laws, as you mentioned, I believe that we have made a real difference.

One common theme that has emerged from these hearings is the role played by prepaid debit cards. It is difficult to say exactly how much money Americans lose through scams that involve these prepaid debit cards since many victims do not report their losses. My staff was telling me that the FTC ranks the State of Maine 42nd in the reporting of frauds, and I think that reflects the nature of the seniors in my State rather than the fact that there is a lower incidence of fraud. Indeed, the Jamaican lottery scam particularly targeted northern New England.

The FTC does estimate that Americans report losing nearly $43 million through prepaid debit card scams last year alone. Because these cards are widely available and convenient, and because the money transferred using them is untraceable, these cards have become the monetary tool of choice for scammers. This is especially true, as the Chairman indicated, for cards that can be reloaded with money, which have a unique PIN that customers can use to transfer funds.

In a typical scam, the con artist will pressure the victim into purchasing reloadable cards, putting money on the card, and then sharing the card's PIN number with the scammer. Thus armed with the PIN, the scammer can transfer the money to his or her own prepaid debit card account and then access those funds from an ATM, through PayPal, or even by buying and reselling consumer goods on the Internet.

Now, I want to emphasize that there are many legitimate reasons why consumers would want to use prepaid debit cards. They are especially important to lower-income consumers who may not

have access to traditional banking services. Still, it is important that we understand what can be done by card providers and retailers to make it more difficult for criminals and con artists to use these cards to advance their nefarious schemes.

The witnesses whom we will hear from today will describe the actions that they are taking to push back against these scammers. Some retailers have also joined the battle by training their sales clerks on what they can do to spot customers who are engaging in suspicious transactions with prepaid cards. I very much appreciate the willingness of the members of this panel to come forward and give us your insights.

Again, Mr. Chairman, thank you for your extraordinary leadership. Although we will be serving in different capacities in the next Congress, I am confident that we are going to continue to be partners when it comes to working together to protect America's seniors. Thank you.

The CHAIRMAN. Senator Collins will be the Chair of this committee next year, and because of her extraordinary leadership, this committee will be in great hands. I certainly want to echo the kudos that you gave to the staff, and this is an example, often overlooked, where the staff works together in a bipartisan way.

Now, if the members of the committee will indulge me, since we are racing the clock because of the votes, I am going to defer my questions and I will turn to you all first, but let us get right to our panel.

First, Steve Streit. He is the CEO of Green Dot Corporation. Then Skeet Rolling, the Chief Operating Officer of InComm. Next is William Tauscher, the CEO and Chairman for Blackhawk Network Holdings, and then Lisa LaBruno, Senior Vice President of Retail Operations at the Retail Industry Leaders Association.

Mr. Streit, if you could keep your comments limited to five minutes, we will go through and have everyone and then we will get into the questions, and Senator Collins will be the first to question.

STATEMENT OF STEVEN W. STREIT, CHIEF EXECUTIVE OFFICER, GREEN DOT CORPORATION

Mr. STREIT. Thank you, Senator. I will save time by not introducing myself and I will live edit as we go for the purpose of time.

The CHAIRMAN. Please.

Mr. STREIT. Green Dot has been a leader in developing techniques to help prevent telephone scams, and so it is my pleasure to join you all today and deepen our ongoing partnership with your important committee in helping to protect seniors from falling prey to these types of phone scams.

Green Dot is a 15-year-old entrepreneurial start-up that invented what is known today as the prepaid debit card industry. Prepaid debit cards have become popular bank account products for millions of Americans because they are convenient, easy to use, easy to get, and, generally, much lower in cost compared to traditional bank checking accounts or credit cards, and, by the way, these cards are not anonymous and, in fact, are fully PATRIOT Act compliant.

While Green Dot is the largest prepaid debit card provider in the United States, many of the nation's largest banks and financial

services companies now also sell prepaid debit cards to consumers as the product has become increasingly more popular and more mainstream.

Around 2003, Green Dot needed to find an easy way for customers to reload their prepaid card with cash at many different retailers from coast to coast. The challenge back then was that the retailer point-of-sale systems—those are the cash register systems—were fairly old, inflexible, and inconsistent from retailer to retailer, so, Green Dot created a product called the MoneyPak. The MoneyPak was designed to allow prepaid card customers to add cash to their prepaid card at many retail stores without the retailer having to modify their existing point-of-sale equipment.

The innovation behind the MoneyPak was the PIN method of reloading, and this is where the customer, as you pointed out, Senator, buys a PIN, which is a multi-digit secret code number, for a certain amount of money and then goes online or telephones a computer to have the value of that PIN applied to their prepaid card account. The success of the PIN method allowed us to sell the MoneyPak product at thousands of retailers, which then led to the creation of the Green Dot Reload Network, which offers users of many different brands of prepaid cards the ability to add cash at any Green Dot retail location.

Today, the Green Dot Network serves customers from nearly 200 prepaid card programs who can add cash to their prepaid cards at nearly 100,000 retailers from coast to coast. In 2013, the Green Dot Network processed more than 40 million reload transactions on behalf of millions of Americans who rely on their prepaid cards as their FDIC bank account of choice.

While the PIN method of reloading facilitates the safe reloading of cash on behalf of millions of honest customers each year, it has, unfortunately, also become susceptible to exploitation by scammers who target seniors with confidence scams. Such scams are designed to convince a senior, as you pointed out, that they have won a prize or a car or some similar enticement and that the way for the senior to collect the prize is to buy a MoneyPak or a similar PIN product sold by other companies, many of which are at this table today, and then provide that secret PIN number associated with that MoneyPak to the scammer.

This method is called—the fraud is called victim-assisted fraud because a scam can only happen when a willing victim purposely cooperates with a con artist, buys the MoneyPak, ignores the warnings on the package not to tell anyone their PIN number, and then they give away their PIN and their name and other personal information anyway to the con artist because the victim truly believes the con. In other words, the con artist is so convincing on the telephone that they actively facilitate the scam, so, the victim wants to give their money to the con artist, thinking it is legitimate, and because that victim wants to give away the money, it has been very, very hard for us to stop, despite many different techniques that we have shared with you over the years.

Given the victim-assisted nature of the fraud and our inability to completely eradicate the nefarious use of our MoneyPak PIN product, Green Dot has decided to discontinue the PIN method of reloading a card altogether. We have moved fully to a more modern

and more fraud-resistant card swipe reload process, and the swipe reload process is more fraud resistant because swipe reloading—just as the name implies, you take your card and you swipe it at the register—requires the actual card holder to be present in the store with their card in their possession in order to facilitate the reload, so, without the PIN, the scammer will have no method of instructing the senior to buy a product and no method of redeeming any associated PIN number, and we think that will kill the fraud on our products.

The PIN product has already been removed from our largest retailers, including Walmart and many other Green Dot retailers, and will be completely unavailable in all Green Dot retailers by the end of the first quarter of 2015, in just a few short months. Today, the vast majority of Green Dot reloads are already performed using the swipe method of reloading and not a PIN number.

Green Dot is proud of our efforts to protect our nation's seniors from scams, and we are certainly ready and willing to continue to work with law enforcement, this committee, and others towards the protection of our nation's most vulnerable customers.

After we all speak, I will be available, of course, to answer any questions you may have.

Thank you.

The CHAIRMAN. Mr. Rolling.

STATEMENT OF R.B. "SKEET" ROLLING, CHIEF OPERATING OFFICER, INCOMM

Mr. ROLLING. Thank you. Chairman Nelson, Ranking Member Collins, and members of the committee, thank you for holding this hearing on the prepaid industry's role in mitigating elderly-targeted fraud and for inviting InComm to participate. I am pleased to share what we are doing to eliminate the ability of fraudsters to take advantage of seniors through what we refer to as victim-assisted fraud.

My name is Skeet Rolling and I am the Chief Operating Officer for ITC Financial Licenses, which is an affiliate of InComm that offers numerous financial services products, including the Vanilla Reload Network. I have been investigating and working to prevent fraud for over 30 years. I started my career as a law enforcement officer. I then helped manage credit and debit card operations for ten years for what is now Synovus Financial Corporation, after which I spent 11 years leading the development for fraud and risk management products for TSYS, one of the world's largest payment processors. I have been with ITC Financial for the last 11 years, leading InComm's compliance, fraud, and anti-money laundering teams. I am also a member of the Executive Board of the Columbus, Georgia, Better Business Bureau.

Founded in 1992 and headquartered in Atlanta, Georgia, InComm is a leading global distributor and technology provider of payment products and solutions with over 1,700 employees worldwide. We are registered with FinCEN as a money service business and we are fully licensed to—as a money transmitter authorized to offer our financial products in all 50 States as well as three Territories. We are subject to the oversight of State banking regulators as well as to the CFPB at the Federal level.

We are proud to offer the Vanilla Reload Network. Consumers rely on Vanilla Reload for an easy, safe, and convenient way to add funds to their card accounts. The vast majority of consumers, 99.9 percent, use our product legitimately and in the manner intended.

One of the biggest fraud-related issues our industry faces is the mitigation and prevention of victim-assisted fraud. This fraud is difficult for industry participants to detect and eliminate because the scams rely on legitimate consumers being deceived into using a reload network product to send money to a criminal whom they believe to be either a family member or a trusted individual. These criminals are ruthless, often preying on the elderly, and they continue to find new ways to scam victims.

Fraudsters have recently revived the grandparent scam, as you referenced, Senator, posing as a relative of the victim who is in dire need of financial assistance. Even when the retail clerk warns the victim, and even when warnings are placed on the products, victims are so convinced by the fraudster's story that they often ignore the warnings and fall victims.

InComm takes its responsibility to consumers very seriously. We have over 60 employees dedicated to compliance, anti-money laundering, and fraud prevention. We have a robust suspicious activity policy with protocols in place to identify fraudulent activity and we take actions to prevent fraud where suspected. We have invested significant resources to develop and institute best practices to warn consumers about victim-assisted fraud and to monitor, spot, and stop this type of fraud. We have met with the IRS, with the Secret Service, with the CFPB, with State regulators, and representatives of this committee to discuss these best practices.

We spend significant time and resources training retailers which sell our products to recognize and warn seniors about fraud. We have created a fraud laboratory in our business to test our own products against the latest criminal techniques. We eliminated ATM access on our GPR cards in countries where we observed large amounts of fraud in order to prevent the withdrawal of stolen funds in those countries, with Jamaica being one of those. We implemented program restrictions, such as cash access, to make our products more difficult for fraudsters to use.

Further, as a leading innovator in the gift card and prepaid market, it is technology that is our most important tool in mitigating fraud. InComm has developed proprietary swipe reload technology which allows a customer to swipe that GPR card at the point of sale to facilitate the reload transaction. This process not only is more convenient for consumers, but it also eliminates victim-assisted fraud by preventing cash from being transferred via the use of a PIN. By offering card-present reloads, only the person holding that card can load funds to it.

That is why on October 24, we announced that we were expanding our swipe reload technology and that we will be retiring the Vanilla Reload PIN packs from our stores by March 31, 2015.

Thank you again for your efforts in calling attention to this serious problem and for organizing this hearing to allow prepaid industry officials to discuss our proactive efforts to eliminate victim-assisted fraud. I look forward to answering any questions you may have. Thank you.

The CHAIRMAN. Mr. Tauscher.

STATEMENT OF WILLIAM Y. TAUSCHER, CHIEF EXECUTIVE OFFICER AND CHAIRMAN OF THE BOARD, BLACKHAWK NETWORK HOLDINGS, INC.

Mr. TAUSCHER. Chairman Nelson, Ranking Member Collins, distinguished members of the committee, thank you for the opportunity to testify today. I look forward to describing Blackhawk's aggressive approach to preventing victim-assisted fraud against seniors and other consumers. Blackhawk is grateful for the committee's leadership on this important issue.

Blackhawk is a leading payment network, offering a broad range of prepaid products and payment services in the U.S. and 21 other countries. We support the physical and digital distribution of a variety of prepaid products, including gift cards and general purpose reloadable, GPR, cards. The Reloadit pack used in our GPR program is sold in over 10,000 locations, mostly grocery stores like Safeway, Giant Eagle, Hannaford, and Winn Dixie, as well as convenience stores and specialty stores.

Blackhawk has been working hard in recent months to implement a variety of technologies to combat victim-assisted fraud. Our key anti-fraud efforts over the years include monitoring GPR card and Reloadit pack activations and transactions using sophisticated fraud detection software, training retail employees about victim-assisted fraud, ensuring consumer awareness of fraud threats, and coordinating with law enforcement and regulatory agencies. A detailed discussion of our anti-fraud measures is included in my written testimony.

GPR cards and other prepaid financial service products offer value and convenience as a substitute to traditional debit cards, credit cards, and bank accounts. Consumers can add money to GPR cards by choosing among several different load methods. The most common method consumers use is a quick load option in which consumers purchase a Reloadit pack or a similar product at a store and then reload their GPR card by going online or calling a toll-free number to provide a ten-digit PIN number found via scratch-off on the back of the Reloadit pack.

Recently, Blackhawk added a new method for consumers to reload GPR products by creating the Reloadit Safe. This allows the cardholder to store their funds and decide when they want to load funds to their GPR card, and, if they have multiple cards, which cards they want to load. This has been an optional feature of Reloadit to date. Unlike the quick load option or the swipe reload option, the customer is required to set up a Reloadit Safe account with an e-mail address, a valid password, a unique device identifier, and a separate self-assigned PIN different than the scratch-off PIN. This creates a safe that will only permit the customer to load money from a specific device after a minimum 30-minute delay from the purchase of the Reloadit pack. From then on, customers control when their money is moved and to which GPR account or accounts they added into their safe.

We are pleased to announce today that by March 2, 2015, customers will no longer be able to use the quick load method. From then on, the customer will purchase a Reloadit pack, go online to

their Reloadit Safe, enter the user ID and password to open the safe, and enter the ten-digit Reloadit number. The safe will verify that the device ID matches the device through which the safe was created. This method is essentially the same account authentication process used by major financial institutions for mobile and online banking applications.

Further, Blackhawk will enhance the safe to allow us to monitor activations and activity based on the specific device, such as smart phone, tablet, and computer, that the customer uses to link to a safe. Once the device is used to create a safe, that device will not be able to create another safe. The enhanced safe will allow Blackhawk to intervene in possible fraud scenarios before the funds are transferred from a Reloadit pack.

Today, customers can also reload their GPR cards by swiping their card at a register and giving the store clerk cash for reload, but, only 50 percent of all retail locations in our program offer reload on swipe today. We are currently assisting many of our retail partners in converting their point-of-sale hardware to allow swipe reload. It is a big investment by them, and we are pleased to announce that by the end of 2015, all of the retail locations in our program who sell these products will accept swipe at the register.

We also work extensively with law enforcement on these issues at the local, State, and Federal levels, and we work to educate retail partners and consumers about potential fraud threats. The results of our extensive effort is less than one percent of transactions involving Reloadit packs constitute potential fraud. However, we are diligently working to enhance fraud protection as we continuously adapt to ever-changing threats.

Thank you again, and I would be welcome to take questions.

The CHAIRMAN. Thank you.

Ms. LaBruno.

STATEMENT OF LISA LaBRUNO, SENIOR VICE PRESIDENT, RETAIL OPERATIONS, RETAIL INDUSTRY LEADERS ASSOCIATION

Ms. LABRUNO. Thank you, Mr. Chairman. Chairman Nelson, Ranking Member Collins, members of the Special Committee on Aging, thank you for the opportunity to testify at today's hearing regarding the role of the private sector in deterring phone scams targeting seniors.

My name is Lisa LaBruno and I am the Senior Vice President of Retail Operations at the Retail Industry Leaders Association. By way of background, RILA is the trade association of the world's largest and most innovative retail companies.

The issue of senior scams is, unfortunately, a growing problem and one that our members take very seriously. I applaud the committee for holding today's hearing on this important issue, because we know that criminals are persistent and they will prey on anyone, including the elderly.

At the outset, it is important to understand that our retail members carry tens of thousands of products in a given store and that the vast majority of the time, we do not produce, design, or manufacture these items. We rely on the expertise of our vendors to create great products that our customers want. At the same time,

since we are closest to the customer, and above all, we value the relationships we have with them, we want to make sure, to the extent possible, that the products are being used safely, comply with all necessary laws and regulations, and most importantly, provide value to the customer.

Today's hearing is focused on so-called reloadable pack cards, which are prepaid cards that have grown in popularity with our customer base. They provide a valuable service by transferring funds easily and affordably between two individuals. According to statistics by the providers of these reloadable pack cards, over 99 percent of all transactions using these cards are for legitimate purposes.

Unfortunately, these reloadable pack cards also appear to be just one of the latest mechanisms for fraudsters to con people, including the elderly, out of their money. There is no failsafe way that retailers can guarantee that these types of scams will never occur using these products. However, more can be done by all stakeholders, including law enforcement, card providers, and merchants by providing consumer education, strengthening safeguards built into these products, and partnering with law enforcement to deter criminal activity on the front end and arrest and prosecute criminals on the back end.

While retailers are an important player in this process, we are only one link in the chain, and so we appreciate when our customers, law enforcement, prepaid card vendors, regulators, and Congress bring to our attention areas of abuse. As responsive companies built on a foundation of trust with our customers, we want to see to it that we do our part to minimize the fraud that could occur on these transactions.

Retailers have taken various steps to mitigate the risk of seniors falling prey to these scams, including employee training, signage, and point-of-sale enhancements. For example, many retailers train their staff to identify signs of common scams in order to prevent the transaction from proceeding and protecting their customers from loss. Many of these reloadable products have large warning labels directly on the package warning customers about the dangers of giving the PIN to unauthorized users.

Additionally, point-of-sale information can be used to educate customers about the dangers of fraudsters. POS enhancements have been installed to alert retailers and the reloadable card vendor to possible suspicious activity and to stop the transaction when certain thresholds are met.

However, despite our best efforts, unfortunately, people can always fall victim to scams of any kind. Recently, Green Dot and InComm announced plans to pull their product from store shelves by the end of first quarter 2015. We fully expect that all RILA members will comply with this deadline, and, we have also learned that Blackhawk plans to enhance the security aspects of its reloadable pack cards. We look forward to learning more.

To be clear, it is not RILA's role to stand between the relationships that merchants have with their vendors, and so we look forward to seeing what types of innovative new products will come into the marketplace that will satisfy our customers' demand for these services while enhancing the security of these transactions.

Finally, we must make sure that law enforcement has all of the resources and tools necessary to combat these crimes.

Thank you, and I look forward to answering your questions.

The CHAIRMAN. Thank you.

Senator Collins, your questions.

Senator COLLINS. Thank you very much, Mr. Chairman.

Mr. Streit, Mr. Rolling, and Mr. Tauscher, I want to start my questions by asking each of you the same question. When a senior comes to you and says, I am the victim of a scam in which your card was involved, what do you do?

Mr. STREIT. Believe it or not, oftentimes, it is not the senior. It is typically the adult——

Senator COLLINS. A family member.

Mr. STREIT. Yes. The adult child of a senior says, "Hey, this happened to mom or dad." Mom or dad is often heard in the background, saying, "No, it is still real." In other words, the con is so good that the senior still believes it. They would call our call center—we have customer service numbers on our packaging and on the website and available elsewhere—and they would say, "Hey, I believe I have been victimized by this or that."

We ask for the account number of the MoneyPak that they have. We research the MoneyPak. These are not anonymous, so, as soon as we know the PIN number, we know exactly what card that money was loaded to, the address and name and other personal information of the alleged fraudster, and if it is our card, we block the card, seize the funds, and if there are funds remaining, immediately refund it to that family member. The individual is then turned over to law enforcement, and we have had many, many, many arrests and prosecutions. We have an entire investigative division that works with law enforcement to do that.

Oftentimes, a senior just does not believe it is true and they will wait months and months and months until somebody finally calls, and in that case, we still do all the law enforcement work, but the money is typically by that time long gone and long spent.

If it is not one of our cards, because we reload cards for over 200 banks and program managers, we immediately call that other bank and say, "Hey, this is a fraud report on one of your cards." We give them the account number, and then that bank would research their customer, block the card, and try to do the same thing.

Senator COLLINS. Mr. Rolling.

Mr. ROLLING. Thank you for that question. Our response is very similar to that of Green Dot. When we take the initial report, we gather the details of exactly what has happened, follow the money, determine what account received that money, and ensure that we block that account as quickly as possible.

We, too, allow funds to be applied to partner cards, others that participate in our reload network. In the event we get a report of fraud on one of their accounts, we notify them immediately and request that they block that card.

In terms of caring for the consumer, we encourage that consumer to immediately file a police report and make a record of what has taken place. Every time money is applied to one of our products, it creates an electronic record every time the underlying account is used. That underlying account and those transactions are very im-

portant investigative leads that can be followed and arrests can be made in many cases.

We, too, have made many arrests related to this type of activity. We had a very significant arrest in Macon, Georgia, that involved 500 charges related to financial transaction card fraud, victim-assisted-type fraud, involving the FBI and local authorities in Macon, Georgia.

Senator COLLINS. Mr. Tauscher.

Mr. TAUSCHER. I do not really have any new things to add that were not said already. We, essentially, have all the same processes, but, I would say a couple of things.

One of the problems, of course, even though we can trace the money and we get law enforcement involved, one of the problems is the scammer is moving to get that money as fast as he can out of the system, and then the fact that you find the card, the money is gone and he is gone, so, the real effort, in our view, is to try to figure out how to put as much barriers to that happening as you can.

I am sure the other folks up here are doing the same, but we spent lots of time worrying about the frequency and the amounts of charges that go on and looking at those in a very specific say compared to cardholders and compared to stores that are distributing them, and, you can develop patterns that can actually cause you to turn off a store, turn off a particular activity, and all of that has become very helpful over the last year or so as this fraud has developed in blocking fraudsters, if you will, because there is a pattern. They are, by definition, trying to get more money either out of an individual than the individual normally handles, out of the store than the store might handle, or into a series of accounts in a way that is different than a pattern we have seen, so, besides all of the issues that Steve and—were covered here, I would just say that this whole idea of using fraud detection systems to look for aberrations is a key element of what we try to do.

Senator COLLINS. Just very quickly, because my time is rapidly expiring, for a stolen bank credit or debit card, the consumer is protected in that losses are limited to $50 as long as the loss or the theft is reported in two days. I believe the new Consumer Financial Protection Bureau has just proposed regulations that would extend a similar kind of stop loss for your kinds of cards. Very quickly, do you support those? Mr. Streit.

Mr. STREIT. We do. The regulation is Reg E, and that applies to deposit accounts, and so we are fully supportive in our Reg E shop today. In other words, our bank complies with those same Reg E laws that any checking account would offer or any credit card would offer a consumer.

The difference is that these are not accounts. In other words, the person who has been scammed is not a Green Dot customer. They are not an account holder. They do not have any bank account with us. The scammer, if you will, is the one who has the bank account, either with us or with one of our partner banks. He utilizes our deposit services, so, in that case, there is no name. The person scammed is often anonymous. You do not know who that is and they do not have an account with us to block or to protect, so, it

is a different kind of a thing. It is a transference of funds, but, on the deposit account, you are correct. Deposit holders are protected.

Senator COLLINS. That is not really my question, and I know my time has expired, but——

The CHAIRMAN. No, continue.

Senator COLLINS. What I am asking is if someone purchases through you, one of your three companies, a card and loads $200 on it and that is ripped off by a con artist and then the senior realizes that, do you protect them from that loss by refunding the money if it is reported within two days the way it would work for a credit card or a debit card.

Mr. STREIT. Maybe, Skeet, you can answer it better.

Mr. ROLLING. Sure. Today, we do not. We consider it just as if they had given $200 in cash away or any other financial services device, so, that is not reimbursed at this point. No, ma'am.

Mr. TAUSCHER. The same is true for our company.

I do think—I do think there is going to be a period of time where we are all going to have to reconsider that over the next six months. Whether we will come down on that side of that point of view, I do not know. Today, we look at it exactly like Mr. Rolling and Mr. Streit do and behave in the same way, so, it is—but, it is a difficult question, and, obviously, it is different than people sort of stealing money out of a bank account, but, still, somebody at the end of the day is out the money.

Senator COLLINS. Thank you.

The CHAIRMAN. Senator McCaskill.

Senator MCCASKILL. Well, let me just follow up. Since she was out of time, I will try to follow up. It is like stealing money out of a bank account, because to that senior, that money is there and they see that as their bank account. Now, it may not be a traditional bank account, but it is their money and it is, they think, being held by you safely, so, do you believe that the regulation that has been proposed by the Consumer Financial Protection Bureau is going to put you on the same footing as if someone got my card number off my credit card and charged—she said $200—let us say somebody ripped off my credit card information and fraudulently charged $150 on my credit card. I would only be liable for $50 of that.

Mr. STREIT. Right.

Senator MCCASKILL. Why is the rule that is being proposed going to put you on equal footing with a credit card company under that situation, and do you support that? Yes or no?

Mr. STREIT. Yes. We already——

Senator MCCASKILL. Okay.

Mr. STREIT. Not only do we support it, we already do it.

Senator MCCASKILL. Okay.

Mr. STREIT. I want to—I am not trying to be argumentative. I am very respectful of this and I am deep into the topic and deeply concerned about it, but we are conflating terms here accidentally, and it is easy to do because it is a complex business.

If you have a prepaid card, that is an FDIC bank account that, if it is issued by a Reg E compliant bank like Green Dot bank, you are covered in every way, which you just said, and every manner, shape, and form, and, in fact, this year alone, we will do something

like $20 million in charge-offs related to refunding consumers money that they have lost on their bank account.

Senator MCCASKILL. Okay.

Mr. STREIT. The product, though, that we are here speaking about is a deposit slip. It is not a bank account. There is no name associated with it. There is no account associated with it. It is a transfer—I am trying to think how to explain it better—you are not putting it on an account. You are suspending it and then you are giving it to the bad guy to put on his account. It never goes onto an account, and that is why you eliminate the PIN.

To your point, by getting rid of the PIN pack, it avoids that problem. There is no way to do that, but, the PIN card itself is simply a deposit slip. It would——

Senator MCCASKILL. It is not being held in a bank——

Mr. STREIT. I am having trouble explaining it better, but——

Senator MCCASKILL. It is not being held in a bank. It is being held in suspension.

Mr. STREIT. Yes. It is a deposit slip

Senator MCCASKILL. Okay.

Mr. STREIT. That is transferred, and that is the difference——

Senator MCCASKILL. Does it say anywhere on your marketing, when you say——

Mr. STREIT. Oh, yes. Absolutely.

Senator MCCASKILL. I do not want to——

Mr. STREIT. Yes.

Senator MCCASKILL. It says, reload prepaid cards. Make same-day payments. Add money to PayPal account. Is there a check there that says you will not get it back if it is ripped off?

Mr. STREIT. It is, yeah. In the instructions on the back, if you take a look at it, we make sure—first of all, the warning is gargantuan and we keep using more shocking colors, and you have to scratch through the warnings just to get to the number—that this is a—we are doing what the consumer instructs. If they instruct us to move that money to an American Express card account or to a Green Dot card account or to an account by someone—and we do that and the account is credited, the product's job is done.

The challenge here, which is why we are eliminating the product, is that the product itself has not done anything wrong and the company has not lost anyone's money. The problem is, the consumer—let me give you a better analogy.

Maybe this is——

Senator MCCASKILL. The consumer——

Mr. STREIT. [continuing.] A better way to explain it——

Senator MCCASKILL. I understand what is happening.

Mr. STREIT. Yeah.

Senator MCCASKILL. The consumer is being duped——

Mr. STREIT. Yes.

Senator MCCASKILL. [continuing.] Into thinking they are giving their money to——

Mr. STREIT. To somebody real, right.

Senator MCCASKILL. [continuing.] Somebody real, and in reality——

Mr. STREIT. They are not.

Senator MCCASKILL. [continuing.] They are being ripped off. I get what is happening.

Mr. STREIT. Yeah.

Senator MCCASKILL. Let me get to the prosecution part. You say there have been a lot of successful prosecutions. Do you have analytics on any of that? Can you tell me how many people has the money been recovered, and/or gone to prison, and/or been convicted of felonies? Do any of your three companies keep the analytics on——

Mr. STREIT. We do——

Senator MCCASKILL. [continuing.] Company successful prosecutions?

Mr. STREIT. Prison, I do not know. I cannot tell you that part, because I do not know that—by the way, I am the CEO and we have a fabulous team of over 300 people who work in risk and fraud, and if our head of fraud operations were here, maybe they could tell you that. So, prison——

Senator MCCASKILL. Well, I think it would be helpful for the committee to learn that.

Mr. STREIT. Yeah. Well, we could supply——

Senator MCCASKILL. I would like to know——

Mr. STREIT. Oh, you bet.

Senator MCCASKILL. —and what do you see as the barriers, any of you, toward successful prosecution in terms of your relationship with law enforcement or them saying, this is too de minimis for us to worry about. I mean, I am thinking back in my experience. If one of your companies called me and said, "Hey, we have got a con artist and we know they have taken this amount of money," I would want to know that this was someone who had done this repeatedly, or I would say, "You need to be in municipal court—"

Mr. STREIT. Well, the secret to prosecution, and Skeet is on the front lines in his company and would probably know more about the operational aspects of it—the trick is keeping great record-keeping and being able to give evidence to law enforcement so they can have a successful prosecution. Simply saying, "Hey, we think Joe Blow took $50," does not excite law enforcement necessarily, and, again, when they speak to the victim, oftentimes the victim says, "No, no, I meant to do that. I did do that." So, there are some jurisdictions that may not believe there has been a crime committed at all in that particular case, so, it is a little bit more complicated.

To your point, absolutely. You keep records. You keep track of it. You come up with compelling evidence to help law enforcement say, "Wow. Follow this trail." We think there is this much money. We see a pattern here with multiple accounts off multiple banks, and we have had many, many arrests and are quite proud of that and we can certainly give you a list of those and give you a sense of how we monitor that.

Skeet, at your company, you may have better information. I know you are more hands-on.

Mr. ROLLING. Sure. Senator, a couple of comments. In the course of fraud prevention and detection, there are two real disciplines. One is controlling the opportunity for the fraud to occur and the

other is to harden the target, make it more difficult for that crime to occur. We work in both dimensions.

Frankly, what we struggle with—and when I say, controlling the opportunity, I am talking about consumer awareness. For the purchasers of these products, users of these products, how can we better protect them? How can we make them aware of the risk related to these products and what you should do and what you should not do, and we have been very up front and candid and communicative about how to use these products successfully. We also train our retailers. We have tips for our retail partners, and we have a huge distribution network, and we cause them to be trained to make sure they can spot the issues, as well, there.

In terms of hardening the target, we are doing exactly that by retiring this product, going to a more robust method with the swipe reload such that these issues will go away.

Senator MCCASKILL. Right. Well, my time is out, and I do not mean to cut you off, but I want to be respectful of the fact we have votes.

Mr. ROLLING. Sure.

Senator MCCASKILL. We have been working—it is a little bit like robo calls. Phone companies are not the problem, but they are in the best position to help us stop robo calls and they have not really stepped up, and we have done a lot of hearings on this in my subcommittee over in Commerce on the robo call space. This is very similar.

You all are in the best position to stop this, and I know you are working on it, but I look forward to working with the Chairman on your—and the new Chairman—on legislation that we can put, maybe, together to combine these two areas that would delineate clearly the responsibilities of informing consumers and protecting consumers——

Mr. STREIT. It is a great idea, and you will find a very willing and cooperative—I do not know much about the phone companies, but in terms of the prepaid industry, you will find a very willing group. It harms our reputation. It harms our fabulous brand name.

Senator MCCASKILL. Yes.

Mr. STREIT. It is a horrible thing. It is a disgusting thing.

Senator MCCASKILL. Well, they have not been quite as willing to do that——

Mr. STREIT. No, but we have a——

Senator MCCASKILL. [continuing.] We are working on it.

Mr. STREIT. We have a tremendous division that does just that, and we should work together more on it.

Senator MCCASKILL. That is great. Thank you.

Mr. STREIT. You bet. Yeah.

Mr. TAUSCHER. Senator, just to add, I do not have the data, either, but I believe that while the fraud itself is too big, it is certainly a smaller number of the whole. The amount of people that we are catching today are not nearly enough. It is a pretty small number.

Senator MCCASKILL. I figured that.

Mr. TAUSCHER. I do not have the data. It is not like we do not catch any. I am sure my friends on the right here catch lots, but, clearly, the steps that we are talking about today that they are tak-

ing, that we are taking, are all aimed at reducing this fraud, and I think we sincerely think we can do that.

Senator MCCASKILL. Okay.

Mr. TAUSCHER. Frankly, if it does not do it, then we are going to keep working on it.

Senator MCCASKILL. Thank you.

The CHAIRMAN. Senator Donnelly.

Senator DONNELLY. Thank you, Mr. Chairman, and I want to thank you and Ranking Member Collins, to commend you for your unwavering commitment to our seniors through your leadership in this committee. It has been an honor to be part of this committee.

I want to thank you and your staff for helping on the field hearing we had in Indianapolis this summer in regards to this very subject of scamming seniors. The cooperation, the assistance, the information we got was, I do not know if the word is scary or alarming or something, but the message that everybody should take away of how vulnerable our seniors are. Our State alone registered almost 25,000 cases of fraud and almost 4,000 cases of identity theft in our State, almost a $2,000 average on each one.

Mr. Tauscher, I wanted to ask you, in regards to—you talked a little bit about your monitoring systems to spot potential fraud. At what point does your system first flag a transaction as possibly suspicious?

Mr. TAUSCHER. Well, there are really a series of places it does it. Clearly, at the point of sale, there are both limits and frequency checks, so, if someone is using—attempting to load money that is over and above the amount that we have set up as a limit, there is a flag. If they are attempting in a store to frequently load money or multiple are—our average store today does not sell multiple of these reloaded chips a day, so when we see activity of that level, we literally move in to alert the store. At a certain level, we will shut the store down entirely and take it out of that business, so, that is the first line of attack.

With our new safe system, we are able to watch the money as it is sitting in the safe, if you will—it is not the money, but if the Reloadit process is sitting in the safe—and track it through that process and what the customer does to it. Of course, it gives the customer a lot more control on what they do, and then, of course, as the money moves on to different cards, so, there is a series of different steps where the systems are monitoring what is going on and setting up alerts.

Probably one of the most successful things that we have been able to do—again, I am sure Mr. Rolling and Mr. Streit have done the same thing—is something not talked about today, is our store, our distribution stores were suffering a lot of fraud, and that fraud began to peak this year and go down substantially because we were able to set up alerts and turn stores off, and that was fraud where, as an example, a store manager would be called at night and told by a fraudster to load a bunch of cards up and give him the numbers, and he was calling from corporate to do a test, and they would go off and do that and a lot of money would be stolen in that regard, and, we have managed with some of these limits, as an example, to pretty well eliminate that or really shut it down.

The whole fraud tracking barrier thing that we all are attempting to do is a science. It is one that sort of moves. You have to keep understanding what the fraudster is doing and then constantly checking. The good news is that we have on a real-time basis—we are hooked to the point-of-sale transaction on a real-time basis. We are hooked to the loading transaction on a real-time basis. We are hooked to the usage of the GPR transactions on a real-time basis, so, we really have sight into all of this.

Senator DONNELLY. Do you rely at all on the expertise or the ability of the person who is working at the store, or is it all computer-driven——

Mr. TAUSCHER. No——

Senator DONNELLY. [continuing.] That computer algorithms pick these up?

Mr. TAUSCHER. We have done just what has been talked about before. We spent a lot of time and energy educating the store personnel, literally have created videos for store training. I brought along an example of something we have done here recently that was a pretty big step for us, actually. We took this sign, which not only talks about the fraud but spells out the kinds of fraud that is currently, and we have now posted it literally on the racks that carry these cards, so, sitting on the rack is this large sign that says, "Read this. These are the kinds of things that you should beware of." We have done the same thing on the website, and in these systems or the usage of these cards, people often go to the website, so, there is clearly an opportunity here to use our websites, to use our point of sale, and to use our people in the store to get them educated.

As Steve said, one of the real problems here is that sometimes the person who has been defrauded will sit and argue with a store person——

Senator DONNELLY. Right. I understand.

Mr. TAUSCHER. —who is trying to talk them out of doing it. It is really a sad situation.

Senator DONNELLY. Yes. Now, obviously, you run different operations. When you get together, do you ever talk about best practices or what has been most successful for you in reducing fraud or in protecting our seniors? Obviously, there are industry conferences and stuff, but, you know, there are proprietary computer systems and other things. Do some of you have a product that you look up and go, "Oh, my God, this has worked so much better for us this year." Will you work with others on getting that through, as it is not so much a competitive advantage as it is just protecting your customers?

Mr. ROLLING. Sure. There is ongoing dialogue to that end today. We share best practices that are industry initiatives, where—that promote the collaboration and the sharing of information and the development of best practices, so yes sir, that is a resounding yes that we will share. You know, we would like to have ongoing dialogue with this committee for the same end, because my fear is we are going to move this issue from this portion of prepaid somewhere else, in another financial services product, and we need to find that, where it lands, and then prepare to defend that area, as well.

Senator DONNELLY. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator.

Mr. Tauscher, since Blackhawk's card is going to be the only available reload card once the other two have retired their product, are you concerned that the thugs are going to come and invade your space since the other two are going to be swiping cards?

Mr. TAUSCHER. I guess we have a fair amount of confidence that what we have built here will put up real barriers for thugs. The fact that a thug has to set up this safe, give us an e-mail, a password, let us understand the device he has used to set it up so we can use the identity recognition we have for that, all the timing and the way that the safe works gives us a pretty good barrier to trap and catch thugs and these results.

The facts are, while this kind of system that we have employed today has been used and is being used by banks in their online and mobile banking applications, this will be the first time it has really been used broadly in the prepaid industry, and, as you said, or as you noticed I said earlier, we are going ahead and putting across our network next year the swipe reload mechanism, and, if it turns out during the course of next year that we have not created a better mousetrap—one, by the way, we would be delighted to share if it does what we believe it will do—if we have not created a better mousetrap, then we will move to swipe reload.

We think there are some very good reasons to maintain the Reloadit Network. The consumers are clearly used to using it. There are some use cases, as an example, when someone wants to reload their child's card and the child is somewhere else, this will allow for that, so we think there are some very good cases of what this can help. We think we have put enough protection and barrier to make it an issue that we can make go away or at least be reduced dramatically.

I will say it again. If it turns out we become the focus of it, if it turns out that what we have done is not working, we are laying a complete back-up plan to be able to go to swipe reload.

The CHAIRMAN. Mr. Streit and Mr. Rolling, what do you think about his mousetrap?

Mr. STREIT. I would never comment on another man's mousetrap.

No, I do not know. To be honest with you, this is the first I am hearing of it, and I am no technology whiz kid, so I would rely on those more knowledgeable, but, it certainly seems like a step in the right direction.

I can tell you, at Green Dot, we tried everything under the sun, as you all know from our previous meetings together, geolocation, device tracking, shutting down cards.

The challenge for us proved to be too great. Either you were blocking the fraudster but accidentally also blocking innocent people, and that resulted in a legitimate person becoming furious, and that was a problem, or the senior themselves, even though you are preventing them from scams, would write a letter to our regulator saying, "Hey, Green Dot held my funds," and then you have an angry regulator, because they just do not want to believe it is fraudulent.

We just felt like we were in a position where we could not win no matter what we did, and that is why six, seven months ago, we

said, let us get rid of this thing and get out of it. Well worth—life is too short, if you will, and it is harming people, and that is not our goal in life, so——

The CHAIRMAN. Did you consider anything like his mousetrap?

Mr. STREIT. Well, that is very unique. What Blackhawk has come up with is unique and it may well work very, very well. They have good technology and so—I just do not know enough about it, Senator. I am sorry, but——

The CHAIRMAN. Mr. Rolling, do you think that he can offer a safe reloadable product?

Mr. ROLLING. I only know what I heard today, Senator. What I will tell you is that any traction or resistance we can cause for the criminals will be a very good thing.

Generally, my experience is, once you show them a decline for their current pathway, they will move on to another area. We look forward to learning more about it and hearing what the results are with it.

Mr. STREIT. That is right.

The CHAIRMAN. Approximately when did you all offer these products to begin with? How many years ago?

Mr. STREIT. Oh, gosh. Well, MoneyPak hit the market back in 2003, I want to say, so quite a bit of time, and——

The CHAIRMAN. Then, why do you think fraudsters gravitated to your products?

Mr. STREIT. Well, I have a belief—there is no way to find out scientifically. You cannot do a survey of fraudsters, but, I have a belief, and Skeet, you may have it. I think as—fraud will find, what is the phrase, the least—the path of least resistance, and I think the MoneyPak was so convenient, is so convenient, and priced properly and so available that they thought, oh, here is a great way to use that.

In the past, they used check fraud. In the past, they used money transfer companies. In the past—we run a bank, and part of bank training going back 50 years was teaching tellers how to spot a senior citizen being manipulated by a younger person with her in the lobby of the bank, so, this tells you how many years ago this kind of thing was happening.

As technology gets better and as seniors are more and more on Facebook, which is a huge outlet for seniors, you are now seeing fraud pop up on Facebook, the grandparent scheme and all kinds of text messages in the name of your relatives, and that is a whole new one now.

I think it all—it is a tough thing. The trick is to make our product so difficult to use for that, or not to have them at all, that the fraudsters go somewhere else, but I do want to be clear, and we said this earlier and you know this on the committee, the fraud will not end. It is just going to keep going to the next innovation.

The CHAIRMAN. Well, how do you, Mr. Rolling and Mr. Tauscher—short answers, please, because the vote has started—how do you run a profitable business with these guys coming in and taking advantage of your customers?

Mr. TAUSCHER. Well, this—you know, our business is not unique to fraudsters. Anybody in the financial services business, from banks to prepaid companies, are subject to this fraud and we fight

it every day. You heard some numbers of people that are in the risk department from Steve and Mr. Rolling, and the facts are, it is just a continuous fight, and the trick is to keep all of it to a level that we still have viable products. One of the hardest things to do here is to take some balance with all the methods you want to do to eliminate fraud and still keep a product. I mean, this GPR product we are talking about is generally loved by the people who are using it.

The CHAIRMAN. Mr. Rolling, 30 seconds.

Mr. ROLLING. Yes, sir. I have worked the fraud issues in the banking industry, in the processing industry, and in the prepaid industry. Security mechanisms are a cost of doing business. Fraudsters are after us continually. We have to continue to innovate, create, and use technology to our best advantage and take good care of our consumers.

The CHAIRMAN. Mr. Tauscher, let us say you decide to move on to the swipe card. Where is the criminal going next?

Mr. TAUSCHER. Well, I—I think, without question, there are plenty of places in the financial system for criminals to do things, and as Mr. Rolling said, we do not always know. The truth is, they tend to find the weakest point in all that you are doing, and you spent lots of time trying to game play and figure out what that is, but besides the fact these are thugs and criminals, they are not stupid and it makes it very difficult as an enemy. As I think you so eloquently said, Mr. Rolling, this is just a continuous fight. It is a cost of our doing business and we just cannot—we cannot relinquish any of our responsibilities in this regard.

The CHAIRMAN. Okay. Now, let me tell you what I am going to encourage my colleague, as the future Chairman of this committee, to do with her staff and our staff, as well. Since you all are getting rid of the reload cards, we have these Jamaican scammers calling us all the time. I mean, they are sloppy, they are aggressive, and they continue to call here. They continue to call our staff, and so, we are going to find out if they are continuing to call us on reload cards and we will know if you have changed or not, and then we will be able to monitor your situation, as well, on these scammers calling, and, so, perhaps there will be some important feedback from you. Other than the senior calling you, we will have our professional staff calling you, as well.

All right. I am going to ask Senator Collins to stand with me, and I am symbolically, since this is our last meeting, going to hand her the gavel——and wish her the best wishes, even though she will actually take this over officially January 6th. I want you to know it has been a pleasure——

Senator COLLINS. Thank you very much.

The CHAIRMAN. [continuing.] And I give you the Chairmanship.

Senator COLLINS. That is sweet of you. Thank you.

The CHAIRMAN. The meeting is adjourned.

Senator COLLINS. The meeting is adjourned. Thank you, everybody.

[Whereupon, at 3:07 p.m., the committee was adjourned.]

APPENDIX

Prepared Witness Statements

TESTIMONY OF STEVE STREIT,
CHIEF EXECUTIVE OFFICER GREEN DOT CORPORATION

Chairman Nelson, Ranking Member Collins and members of the Committee, My name is Steve Streit and I am founder, Chairman and CEO of Green Dot Corporation, a Bank Holding Company regulated by the Board of Governors of the Federal Reserve System, and Founder and Chairman of Green Dot Bank, a State chartered, fed-member commercial bank regulated by Federal Reserve and the State of Utah Department of Financial Institutions.

Green Dot appreciates the opportunity to submit testimony for the hearing entitled "Private Industry's Role in Stemming the Tide of Phone Scams." While impossible for any person or organization to completely stop con artists and their associated criminal activity, Green Dot has been a leader in developing techniques to help prevent such scams and it is therefore our pleasure to work with the Senate Committee on Aging in an effort to protect seniors, one of America's most vulnerable populations.

About Green Dot

Green Dot is a 15 year old entrepreneurial startup that invented what is known today as the prepaid debit card industry. Over the years, prepaid debit cards have become popular bank account products for millions of Americans because they are convenient, easy-to-use, easy-to-get and are generally much lower in cost compared to traditional bank checking accounts or credit cards. Prepaid cards are especially popular with low and moderate income Americans because consumers in that economic segment often have a difficult time obtaining traditional checking accounts and credit cards, which generally require certain minimum credit score thresholds and/or a successful past history of holding a checking account in order to obtain such accounts. While Green Dot invented the prepaid debit card industry and is today the largest prepaid debit card provider in the United States, many leading banks and financial services companies sell prepaid debit cards to consumers, including Chase, American Express, U.S. Bank, Wells Fargo, Comerica and many others.

About the MoneyPak

Around 2003, as part of Green Dot's growing prepaid card business, the company needed to find an easy way for customers to be able to reload their prepaid card with cash at many different retailers from coast to coast. The challenge was that retailer "Point of Sale" (POS) systems were fairly old, inflexible and inconsistent from retailer to retailer, so, to overcome the lack of modern retail technology, Green Dot invented a "one size fits all" product called the "MoneyPak." The MoneyPak was designed to serve as a defacto "deposit slip" allowing prepaid card customers to add cash to their prepaid card at many retail stores without the retailer having to modify their existing POS equipment. The innovation behind the MoneyPak that allowed it to be sold without POS modification was the "PIN method of reloading." With the innovation of selling a "PIN," a unique multi-digit number that represented a certain amount of money, the customer could then buy a PIN for certain amount of money and then redeem that PIN online or by phone and instruct Green Dot to load the value represented by that unique PIN to whatever prepaid card they instructed. Shortly thereafter, with the PIN method of reloading in production, Green Dot was then able to open its proprietary reload system to other prepaid card companies.

This gave birth to the Green Dot Reload Network, which offered users of many different brands of prepaid cards the ability to add cash to their prepaid card at any Green Dot retail location. Because of the MoneyPak's ubiquity and ease of use, it became an almost immediate hit with consumers and grew in popularity in proportion with the growth of the prepaid debit industry itself. Today, the Green Dot Network serves customers from nearly 200 prepaid programs, including Green Dot customers, who can add cash to their prepaid cards at nearly 100,000 retailers. In 2013, the Green Dot network processed more than forty million reload transactions on behalf of millions of Americans who rely on prepaid cards as their bank account of choice.

Victim Assisted PIN Fraud

While the PIN method of reloading facilitates the safe reloading of cash on behalf of millions of honest customers each year, the PIN method of reloading a card has also become susceptible to exploitation by scammers who target seniors with con-

fidence scams. Such scams are designed to convince the senior that they have won a prize or some other similar enticement and that the way for the senior to collect the prize is to buy a MoneyPak (or a similar competitor's product) for a specified amount of money and then provide the secret PIN number associated with that MoneyPak to the scammer. This is the equivalent of the senior telling a stranger their debit card account number and providing them their secret PIN, or providing a con artist with their bank account number and their online login secret password. As the Committee knows, the scammer immediately uses that secret PIN to empty the MoneyPak and transfer the associated funds to their own account. At that point, the senior's money is gone and the scammer is gone.

This method of fraud is called "Victim Assisted Fraud" because the scam can only happen when a willing victim purposely gives away their personal information to a stranger. Because the victim themselves actively facilitates the scam, it has been very difficult to stop. Based on dispute filings, we believe Victim Assisted Fraud represented approximately $30 million in cash loads in 2013 out of total load volume through Green Dot's network of approximately $20 Billion, or less than one-quarter of 1 percent of loads. While this amount of fraud is not material in statistical terms, Green Dot recognizes that it is certainly material to the senior who fell victim to the confidence scam.

In an effort to help stop this type of scam, Green Dot has spent millions of dollars to combat victim assisted fraud. Such measures include:

A. Developing technology to help identify potentially nefarious transactions and blocking the PIN before the fraud can be completed. This has helped somewhat, but often times ends up snaring too many honest customers along with the scammers.
B. Developing methods to quickly track the flow of funds after being notified by a victim of such a scam. This allows Green Dot to attempt to block and recover funds for the victim and to provide law enforcement with detailed information on the scammer. This has helped somewhat, with Green Dot reclaiming millions of dollars in scammed money and returning that money to victims, while helping law enforcement to make a number of key arrests both domestically and internationally.
C. Blocking cash withdrawals on its Green Dot Bank issued debit cards at ATM machines outside the United States so that scammers won't want to use Green Dot Bank issued cards as the receiving account of such stolen funds. This has been effective, but Green Dot Bank issued cards represent only a portion of the overall prepaid card industry.
D. Last, Green Dot has spent many millions of dollars reprinting and distributing all MoneyPak packaging with large red warning notices where the PIN is located urging consumers to never give out their secret PIN number. We have also worked with consumer advocates, the Better Business Bureau and law enforcement agencies to place warnings and create videos on helping educate seniors on confidence scams. However, it would appear that this tactic has not achieved the intended goal because the seniors ignore the warnings, convinced that the con artist is genuine.

All these tactics in aggregate have indeed helped somewhat. However, given the "Victim Assisted" nature of the fraud and our inability to completely eradicate this nefarious use of our MoneyPak PIN product, Green Dot has decided to discontinue the PIN method of reloading a card altogether, and instead, move fully to a more modern and more fraud resistant "card swipe" reload process. The swipe reload process is a more fraud resistant reload method because "swipe reloading" requires the actual cardholder to be present with their card in the store in order to reload, so, without the PIN, the scammer will have no method of instructing a senior to buy a product and no method of redeeming any associated PIN number.

Of course, confidence scams have been around for hundreds of years and we understand that seniors will always need to be cautious of strangers bearing gifts, but at least Green Dot's MoneyPak will no longer be able to be used by scammers to facilitate such fraud.

The PIN product has already been removed from Walmart and many other Green Dot retailers and will be completely unavailable in all Green Dot retailers by end of Q1 2015. Today, the vast majority of Green Dot reloads are already performed using the swipe method of reloading and not a PIN number.

Green Dot is proud of our efforts to protect our nation's seniors from scams, and we are ready and willing to continue our work with law enforcement, the Committee and its members to explore other ways in which we can enhance the protections for our nation's most vulnerable consumers.

About Green Dot

Green Dot Corporation is a bank holding company that owns Green Dot Bank, a State member bank located in Provo, Utah. We are regulated by the Board of Governors of the Federal Reserve System and the State of Utah Department of Financial Institutions. We have approximately 800 domestic employees with offices in Pasadena, California; Palo Alto, California, Bentonville, Arkansas, Provo, Utah, Sandy, Utah, Tampa, Florida and Birmingham, Alabama.

Green Dot's mission is to reinvent personal banking for the masses with a sole focus on low cost, fair and easy to use banking products for low and moderate income Americans. Our accounts feature no penalty or overdraft fees of any kind and short, simple and clear disclosures. Green Dot cards and reload services are available to consumers at 100,000 retailers nationwide, online and via the leading app stores. Each year, Green Dot will open more than 5 million new FDIC insured bank accounts for Americans who were either previously unbanked or underserved by traditional banks.

Green Dot prepaid cards are not anonymous and are fully compliant with the USA PATRIOT Act. Green Dot products adhere to our customer covenant of clear disclosures, no minimum balance requirements and no penalty fees ever and our products routinely win numerous awards and positive recognition from the nation's leading consumer groups. Furthermore, Green Dot is publicly on record of supporting the CFPB's newly announced proposed rule on prepaid cards. See the attached press release for further information.

TESTIMONY OF R.B. "SKEET" ROLLING, CHIEFOPERATING OFFICER, INTERNATIONAL COMMUNICATIONSINTERNATIONAL, INC. (INCOMM)

Chairman Nelson, Ranking Member Collins, and members of the Committee, thank you for holding this hearing on the prepaid industry's role in mitigating elderly targeted fraud and for inviting InComm to participate. We have followed closely the Committee's efforts to investigate and reduce fraud perpetrated against some of our nation's most vulnerable citizens, and I am pleased to be here today to share what InComm is doing to eliminate the ability of fraudsters and scam artists to take advantage of seniors in what we refer to as "victim-assisted fraud."

My name is R.B. "Skeet" Rolling and I am the Chief Operating Officer of ITC Financial Licenses, an affiliate of InComm that offers numerous financial services products, including the Vanilla Reload Network. I've been investigating and working to prevent fraud for over 30 years. I started my career as a law enforcement officer. After a brief stint in retail corporate security, I entered the banking industry and helped manage all facets of credit and debit card operations for what is now Synovus Financial Corporation for 10 years. For the next 11 years I led the development and delivery of fraud and risk products for TSYS, one of the world's largest payment processors. I've been with ITC Financial Licenses for the past 11 years, leading our compliance, fraud and anti-money laundering teams for all of InComm's business globally. In addition, I frequently speak at industry conferences on matters such as identity theft, fraud, and compliance. I am also a member of the executive board of the Columbus, Georgia Better Business Bureau. During my time in the financial services industry, I have seen many types of fraud, each of which the industry has aggressively worked to eliminate. The prepaid industry's efforts to eliminate victim-assisted fraud are no exception.

InComm is a leading global distributor and technology provider of gift cards, prepaid cards, and payment solutions across a wide variety of retail industries around the globe. Headquartered in Atlanta, Georgia since its founding in 1992, InComm has grown to employ 1,700 people in 30 countries across 5 continents. ITC Financial Licenses is registered with FinCEN as a money services business (MSB) and is authorized to offer InComm's financial services products in all 50 States, the District of Columbia, Puerto Rico and the U.S. Virgin Islands. To that end, ITCFL is licensed as a money transmitter by 46 States and the 3 territories, and is subject to the oversight of the banking regulators in each of those jurisdictions, including the Florida Office of Financial Regulation, where Chairman Nelson is from, and the Maine Bureau of Consumer Credit Protection, where Ranking Member Collins is from. At the Federal level, we are regulated primarily by the Consumer Financial Protection Bureau (CFPB).

InComm and ITCFL are proud to offer the Vanilla Reload Network. Our network has grown to be the second largest reload network in the country, with approximately 250,000 customers using the network monthly through nearly 70,000 retailer locations nationwide. Vanilla Reload allows consumers to load funds to their general purpose reloadable (GPR) prepaid cards, so that they may use those cards to shop online or in retail, pay bills, transfer money, and manage their spending and saving. Consumers rely on Vanilla Reload and similar industry solutions for an easy, safe, and convenient way to add funds to their card accounts, especially those customers who are either unbanked or who use these card accounts as a bank account replacement. The vast majority of consumers—99.9 percent—use Vanilla Reload legitimately.

In terms of fraud prevention, one of the biggest issues our industry faces is the mitigation and prevention of victim-assisted fraud. This type of fraud is difficult for industry participants to detect and eliminate because the underlying scams rely on legitimate customers being deceived into using a reload network to send money to a criminal. The retail transaction initiated by the victim occurs as any typical, legitimate transaction, and funds are subsequently redeemed to a GPR card in a likewise typical manner.

This fraud typically takes the form of a promise of free money, winning the lottery or qualifying for a loan. The criminals are ruthless, often preying on the elderly, and unfortunately they continue to find new ways in which to scam unsuspecting victims. Most recently, fraudsters have revived the "grandparent scam"—posing as a relative of the victim who is in distress and in dire need of immediate financial assistance.

In a typical scenario, the fraudster convinces a victim to load money onto a reload product and then the victim provides the PIN to the fraudster. Once the fraudster has the PIN, he is able redeem the money onto a prepaid card and then either quickly spend the funds or withdraw the cash from an ATM. This is very difficult to prevent as the fraudster has effectively fooled the victim into believing that he

or she is helping a family member in need or is otherwise providing the PIN to a trusted individual. Even when the clerk at the checkout warns the victim and even when warnings are placed on products, victims are so convinced by the fraudster's story that they ignore the warnings and ultimately fall victim to the scam.

Even at InComm, we have witnessed this criminality on a most personal level, when the grandmother of one of our own employees purchased a competitor's reload PIN product and lost thousands of dollars to a fraudster who pretended to be a grandson in need of money to cover hospital and legal expenses following a car crash. Even the cashier's warnings did not deter the victim from going through with the transaction—the fraudster's story was so convincing that all she could think about was the well-being of her grandson.

InComm and ITCFL take our responsibility to our consumers very seriously. ITCFL has over 60 employees dedicated to compliance, anti-money laundering, and fraud prevention. We have invested significant time and resources since we launched Vanilla Reload to develop and institute best practices to warn consumers about the dangers of victim-assisted fraud and to monitor, spot, and stop this fraud. We've created a fraud lab to test our products with the latest criminal techniques—as fraudsters evolve and change their methods, so do we.

We train the clerks selling these products to warn customers prior to purchase, place warnings on websites, we've started a GPR blog used to educate consumers about the use of GPR products and to warn them about scams, hired a social media coordinator to monitor potential fraud activity that occurs online, and we send a fraud resource guide to our retail partners across our network.

InComm has eliminated ATM cash access on its GPR card products in countries where we observed a large volume of fraud in order to prevent fraudsters from withdrawing stolen funds in those countries. We have a robust suspicious activity policy with protocols in place to identify fraudulent activity, such as multiple reloads from various locations, and we take actions to prevent fraud, such as freezing or requesting a third party prepaid issuer to freeze the underlying prepaid account to prevent ATM withdrawals or purchases when fraud is suspected.

Further, at InComm we have consistently sought to develop new technology and implement program restrictions to make our products more difficult for criminals to use. On our GPR prepaid cards, we have many daily, monthly, and dollar-based limits on ATM withdrawals, reloads, and other activities that help reduce fraud and subsequent losses.

Perhaps most importantly, InComm has developed proprietary swipe reload technology which allows a customer to swipe a GPR prepaid card at the point of sale to facilitate the reload transaction. This process is not only more convenient for customers, but also eliminates victim assisted reload fraud by preventing the cash from being transferred via use of a PIN. By offering card-present reloads, only the person holding the card can load funds. We've invested significant amounts of money, time, and resources in helping our retailers overcome the expense and effort necessary to implement our swipe reload technology at their stores and point of sale systems. We were pleased to be able to announce on October 24, 2014 that (i) InComm added an additional 15,000 swipe reload locations (bringing the total swipe reload locations to over 55,000), and (ii) InComm will remove the Vanilla Reload PIN packs from stores by March 31, 2015. The combination of these actions demonstrates our dedication to weed out fraud and prevent criminals from misusing our network, and to continue to provide a safe, easy, and convenient way for our customers to add funds to their accounts.

InComm's experience has taught us that there are three ways to significantly reduce fraud and criminal use of financial products. First, consumer awareness. That's why we take steps to warn our consumers about the threat of scams across various media and work with our retail partners to do the same. Second, industry awareness. We have met with the IRS, Secret Service, the CFPB, State banking departments, and representatives of this Committee to discuss fraud and to determine best practices to combat fraud. We are an active participant within our industry trade group, the Network Branded Prepaid Card Association (NBPCA), and one of our executives is the current Chairman of that group. We spend significant time and resources educating the retailers which sell our products, and train their employees to recognize and warn seniors about fraud issues. Third, use of technology. As a leading technology innovator in the gift and prepaid market, this is our greatest strength. We have developed technology—our swipe reload platform—that will eliminate elderly targeted, victim-assisted fraud in our reload network. Because of this advancement in technology and our efforts to make it available to all of our retail partners, we will be retiring the reload PIN product by the end of the first quarter in 2015.

Thank you again for your efforts in calling attention to this serious problem and for organizing this hearing to allow the prepaid industry to discuss the steps we are taking to proactively eliminate opportunities for fraudsters to take advantage of seniors. We will continue to do our part to eliminate victim-assisted fraud, while simultaneously enhancing the reload experience or our customers.

TESTIMONY OF WILLIAM TAUSCHER, CHAIRMAN AND CHIEF EXECUTIVE OFFICER, BLACKHAWK NETWORK HOLDINGS, INC.

Chairman Nelson, Ranking Member Collins, distinguished members of the Committee, thank you for providing me the opportunity to testify today on the subject of private industry's role in preventing victim-assisted fraud against seniors. My name is Bill Tauscher and I am Chairman and Chief Executive Officer of Blackhawk Network Holdings, Inc. I look forward to describing today Blackhawk's innovative and aggressive approach to deterring, preventing, and mitigating this pernicious type of fraud against seniors and other consumers. Blackhawk is grateful for the Committee's attention to this important subject over many months and your leadership in raising awareness about it.

About Blackhawk Network Holdings, Inc.

Blackhawk is a leading payment network utilizing proprietary technology to offer a broad range of prepaid products and payment services in the United States and 21 other countries. Our companies support the physical and digital distribution of a variety of prepaid products, including gift cards, general-purpose reloadable ("GPR") cards, corporate reward cards, incentive cards, rebate cards, prepaid telecom handsets, and airtime cards across a global network totaling over 180,000 stores worldwide. Our GPR program, however, reaches under 20,000 locations in the U.S. And, our Reloadit packs are sold in over 10,000 locations, including Safeway, Albertsons, Giant Eagle, Kroger, BiLo, Casey's, Dave's, Winn Dixie, Harveys, Sweet Bay, Meijer, Food Lion, Hannaford, Save-a-Lot, Supervalu and WaWa stores. Our network provides significant benefits to those who purchase the products and services we offer and to our distribution partners who sell those products. For consumers, we provide convenience by offering a broad variety of quality brands and content at retail locations and online, enhanced by customer promotions and loyalty incentive programs that may be offered by our distribution partners. For these partners, we provide a significant, high-growth and highly productive product category that drives incremental store traffic and customer loyalty. Blackhawk serves in a variety of capacities in the prepaid market. We are a program manager for bank-issued network-branded card products. We are licensed money transmitter that issues Discover-branded reward cards and the Reloadit™ pack (a GPR card reload and bill payment product), and, we are a distributor for both store-specific and network-branded gift cards.

Blackhawk's heritage of innovative prepaid developments began in 2001, when it was a subsidiary of Safeway Inc. Since our inception, we have looked at the industry with fresh eyes, always seeking to solve customer needs to grow our partners' business. Our first consumer insight led to a pioneering breakthrough—to provide gift cards where they were more convenient for consumers, including grocery stores. Over the years, we have continued to research what consumers want and have rapidly brought these innovations to market. In addition to expanding our product line to capitalize on the full spectrum of prepaid products, we have also greatly expanded the brands we offer and the locations—both digital and brick-and-mortar—where we offer them.

Blackhawk's Reloadable Financial Services Products

Consumers have realized that prepaid financial service products offer value, convenience and flexibility. As the industry has evolved, Blackhawk has brought together a broad selection of GPR cards in one place, developing a proprietary reload network that is one of the lowest-priced, and most convenient. We are proud to distribute to our retail partners and to process transactions for a diverse set of GPR card products, including those offered by NetSpend, PayPal, Green Dot, AccountNow, Univision, T-Mobile, and others. In addition to offering a large selection of GPR products under one roof, Blackhawk also offers PayPower™, our own proprietary GPR card brand with desirable features, such as free direct deposit and online or phone bill pay, and competitive pricing.

Blackhawk makes it easy and secure for consumers to add value to their GPR cards by choosing any of these three different load methods:

Quick Load: Under the quick load option consumers can purchase a Reloadit pack at a retail location to load anywhere from $20 to $950. After purchasing the Reloadit pack, the consumer reloads the GPR card by going online or calling a toll-free number to provide a 10-digit PIN number found on the back of the Reloadit pack, a scratch-off PIN. This is how Reloadit and similar products were originally setup to operate for ease of use and consumer convenience. Ninety-nine percent (99 percent) of consumers who use this method do so in legal, non-fraudulent ways that

serve their needs, such as funding a GPR card held by a child or grandchild who is away at college or by a contractor or household helper who is using a GPR card. Blackhawk's introduction of Reloadit Safe was a refinement of the product. With the further enhancements we will introduce in March next year (including the elimination of quick load with the scratch-off PIN and the introduction of enhanced fraud mitigation efforts, described in greater detail below) we will substantially improve fraud mitigation for Reloadit.

Reloadit Safe: Recently, Blackhawk has added a new method for consumers to reload GPR products participating in our Reloadit network. We have created the option for consumers to use the Reloadit Safe, which allows cardholders to store their Reloadit pack number securely and conveniently. When consumers want to load funds to their GPR card(s), the Reloadit Safe provides them the opportunity to decide from which Reloadit pack they want to load funds, when such funds should be loaded, and the amount of funds that should be transferred from the Reloadit pack to their GPR card or cards.

The Reloadit Safe enables Blackhawk to mitigate fraud through a variety of tools. Unlike the quick load option, the Reloadit Safe requires customers to provide an email address, password, a unique device identifier and a separate self-assigned PIN—different than the scratch-off PIN. The self-assigned PIN is created to allow the user to authenticate Safe access when an unknown or new device attempts to log in and gain access to the Safe. This creates a Safe that will only permit the customer to load money from a specific device after a minimum 30-minute time delay from the purchase of a Reloadit pack. The Safe also requires the customer to enter the full GPR card number into the Safe prior to transferring funds. We view the innovation of the Reloadit Safe as an effective bulwark against victim-assisted fraud. With the Safe, consumers who do not have the GPR card they want to load with them (such as when a child or grandchild has the GPR card at college) can safely load funds to that GPR card remotely through Reloadit, and, with enhancements that we will roll out in March next year (including elimination of quick load with the scratch-off PIN), Blackhawk will have enhanced monitoring capability and the ability to analyze accounts and account activity more effectively. This will allow us to identify fraud more quickly and prevent it more effectively, while still allowing consumers to retain Reloadit as a tool for accessing their funds and transferring them. I will provide more details on these enhancements later in this Statement.

Swipe at the Register: In addition to offering quick load and Reloadit Safe options to load GPR cards with the Reloadit pack, Blackhawk provides customers in an increasing number of locations with the option of funding their GPR card accounts via swipe at retail locations, rather than through the scratch-off PIN. Approximately 50 percent of all retail locations that carry our GPR products offer reload on swipe today, but, not all retailers can support this functionality today. We are currently assisting many of our retail partners in converting their point-of-sale hardware to accept "swipe at the register." This technology allows for the elimination of reloads using scratch-off PINs.

Blackhawk's Commitment to Preventing Fraud

Our research indicates that less than 1 percent of transactions involving Reloadit packs constitute potential fraud. Nevertheless, Blackhawk is committed to preventing all instances of fraud against consumers and, accordingly, has implemented significant measures to prevent and mitigate different types of fraud, including victim-assisted fraud.

The key components of our anti-fraud efforts include:

- monitoring GPR card and Reloadit pack activations and transaction monitoring using Blackhawk data and sophisticated anti-money laundering and fraud detection software, 24-hour Risk management resources and risk-based funding delays;
- educating and training our retail partners and their employees about victim-assisted fraud;
- ensuring consumer awareness of fraud threats; and
- coordinating with law enforcement and regulatory agencies.

Monitoring GPR Card and Reloadit Pack Activation and Transaction Monitoring. With respect to activation monitoring, Blackhawk performs proactive analysis of GPR card registrations and their associated attributes. We have developed and deployed a sophisticated point of sale monitoring system that provides alerts to Blackhawk Risk Management personnel in cases where potential fraud is detected based on suspicious activity, such as an unusual number of sales of Reloadit packs in a specific store or region or atypical amounts of funds to be loaded. If such cases are observed, Blackhawk Risk Management personnel have the ability to block the

purchase of Reloadit packs from a particular store or stores in our network and to delay funding for a cash transfer of money to a GPR card from an individual Reloadit pack. We have many documented incidents where Blackhawk's monitoring technology has successfully thwarted fraud attempts.

Educating/Training Retail Partners. Although we have found Blackhawk's human resources and data analytics systems to be very effective in preventing victim-assisted fraud, we recognize that a critical backstop to our efforts is ensuring that our retail partners and their employees are attuned to potential fraud threats. We frequently issue fraud alerts to our retail partners on new and trending fraud scams and so that store employees can spot potential fraud at the point of sale. We also provide periodic webinar training for our retail partners on fraud and anti-money laundering awareness. At the individual store level, our merchandisers provide information to store employees when setting up card displays and restocking the racks on which our products are sold. We also train store employees to call our 24-hour toll-free risk support hotline if potential instances of fraud arise. We evaluate the efficacy of our retailer training by conducting "secret shopper" programs around the country.

Ensuring Consumer Awareness. Of course, making sure consumers are aware of potential fraud threats is also an integral part of ensuring that they are not victimized. We have long included a "Protect Your Money" page on our Reloadit and PayPower websites explaining that the products can be the target of fraudsters looking to scam consumers. The page provides useful tips to prevent fraud and theft, a list of common scams involving Reloadit packs of which consumers should beware, links to government resources on phone scams and other types of fraud, and a toll-free number for consumers to call if they believe they are the target of a scam.

More recently, we have added a conspicuous "splash" message to our Reloadit.com homepage that every customer will see before using the site to transfer funds or pay bills. The message instructs a consumer to refrain from providing the PIN number on the back of the Reloadit pack to anyone over the phone the consumer does not know or has not met in person. The message also identifies common scams and provides a customer service line for a consumer to call if the consumer has been asked by someone else to provide Reloadit as a form of payment.

Coordination with Law Enforcement. Even as we work to educate retail partners and consumers about potential fraud threats, Blackhawk has also proactively engaged with law enforcement officials and regulators to detect and respond to new types of scams. Since October 2013, we have coordinated with the U.S. Secret Service and local law enforcement agencies from New York and New Jersey to combat phone scammers believed to be operating in New York and Florida. More recently, we have engaged with the U.S. Department of Homeland Security and the Treasury Inspector General for Tax Administration to address a fraud ring that has perpetrated a variety of victim-assisted frauds, including the "grandchild in jail" scam in which prepaid reload products have been implicated. We are committed to continuing open communication and coordination with law enforcement to prevent fraud and help hold accountable those who attempt to perpetrate fraud.

Ongoing Enhancements to Blackhawk's Anti-Fraud Regime

The current option for Reloadit customers to open a Reloadit Safe or to use swipe at the register technology, coupled with our extensive technology and educational measures, exemplifies Blackhawk's commitment to preventing fraud against vulnerable populations and to deterring scammers from targeting the Reloadit pack as a useful vehicle to commit fraud. However, the implementation of these technologies and processes are only part of a progressive fraud mitigation strategy to prevent victim-assisted fraud targeted against seniors and other potentially vulnerable populations.

We are pleased to announce today that by March 2, 2015, Blackhawk will implement important changes to the overall function of our Reloadit pack product. On that date, customers will still be able to buy a Reloadit pack at a store, but will no longer be able to use the quick load method to transfer funds to a GPR account. Instead, customers using a Reloadit pack will be required to create a Reloadit Safe that will store the Reloadit pack and will allow for the transfer of such funds from the Reloadit pack to the customers' GPR card or cards. To load funds to their GPR card or cards, consumers will purchase a Reloadit pack, go online to their Reloadit Safe, enter the user ID and password to open the Safe, and enter the 10-digit number found on the back of the Reloadit pack. The Safe will verify that the device ID used to open the Safe matches the device through which the Safe was created. This method is essentially the same account authentication process used by major financial institutions for mobile and online banking applications. The Reloadit Safe will

require the customer to add a complete 16-digit GPR card number to the Safe to effectuate the transfer of funds to the GPR card.

Further, Blackhawk will be enhancing the Reloadit Safe to allow us to monitor activations and activity based on the specific device (e.g., smartphone, tablet, computer) the customer uses to link to a Safe. In practice, this means that the customer will be identified by the device from which the customer is accessing the Safe and loading a GPR card. Customers will only be able to create one Safe per device. Once the device is used to create a Safe, that device will not be able to create another Safe. The enhanced Reloadit Safe will allow Blackhawk to intervene in possible fraud scenarios before funds are transferred from a Reloadit pack.

Beyond this updated experience for the consumer, Blackhawk is implementing a variety of new security technologies behind the scenes to monitor suspicious activity related to reloading of GPR card accounts. We will use technology to associate a Safe with a ZIP code at the time of its creation and will monitor ZIP codes of the locations where associated Reloadit packs are purchased. "Geographic Reasonability" thresholds (based on the distance between the ZIP code associated with the Reloadit Safe and the ZIP code where the consumer purchased the Reloadit pack) will alert Blackhawk when Reloadit Safe accounts are funded with Reloadit packs activated from various parts of the country. Our advanced fraud monitoring systems will track the device identifier in real-time and will analyze velocity load limits based on customer behavior. Reloadit Safe transaction activity will also be monitored based on the history of the customer's use of the Safe. This data will help allow us track usage patterns and allow our Risk Department to identify suspicious activity and stop fraud (through contacting the retail store selling the Reloadit pack or by preventing loads and transfers). We will be able to blacklist accounts and users who appear to have engaged in excessive transfers or misused the product, and, each Safe will have daily transaction limits. Today, the daily load/spend limits are $2,850, with bill payment sub-limits set at $1,000 per day. The enhanced Safe features will allow us to impose lower limits on new users, new devices, and new Reloadit Safes that are opened. Further, Blackhawk will continue to impose risk-based funding delays to assist with money recovery if scams are somehow successful. These added layers of security will allow Blackhawk to control the movement of money to a registered GPR card account with an intensified level of security.

We are also working with the retailers in our program to increase the availability of swipe reload capability for customers at the register. Although customers can currently use swipe technology at approximately 50 percent of all U.S. stores in our program that sell GPR cards, Blackhawk is working proactively with its retail partners to increase the number of swipe reload locations. We are pleased to announce that by the end of 2015, all of the retail locations in our program that sell these products will accept swipe at the register. While the conversion of in-store hardware to accept swipe reloads is an expensive undertaking for our retail partners, we believe that it is a worthwhile for them to provide consumers with another option for reloading their GPR cards and reducing instances of fraud.

At the same time as Blackhawk is expanding the fraud prevention tools in Reloadit Safe and making swipe reload more available, we are also continuing to augment our efforts to educate customers and retail employees to spot potential victim-assisted fraud. We recently created and asked our retail partners to post signage in stores directing customers to refrain from providing the Reloadit pack PIN number to anyone they do not know and identifying common victim-assisted scams. In addition, we provided our retail partners a new guidance document for employees that outlines examples of scams targeting both customers and stores, as well as tips on how employees can protect their customers when confronted with suspicious situations. We are working with the National Adult Protective Services Association to broaden the reach of our education efforts to help reduce the amount of fraud committed against senior citizens using prepaid products, and, we are looking at additional opportunities to educated seniors and others about scams.

Conclusion

We recognize that fraud cannot be totally eliminated. Combatting it takes vigilance. Working with our retail partners, law enforcement agencies, regulators, consumers, and others, Blackhawk has substantially improved its mitigation of victim-assisted fraud targeted at our customers. However, we are not satisfied. We are focused on and invested in preventing fraud from occurring, and in deterring would-be fraudsters from attempting to exploit our products for illicit uses. We are investing substantial human and financial resources to implement more layers of fraud protection and to adapt to ever-changing threats. In addition to ensuring that all locations in our network that sell these products allow swipe reloads, we believe

that our enhanced Reloadit Safe functionality further enhances both fraud prevention efforts and law enforcement tools for bringing fraudsters to justice. Thank you again for raising awareness about this important issue and for giving Blackhawk the opportunity to share our perspective.

TESTIMONY OF LISA LABRUNO, SENIOR VICE PRESIDENT, RETAIL OPERATIONS, RETAIL INDUSTRY LEADERS ASSOCIATION (RILA)

Chairman Nelson, Ranking Member Collins, members of Special Committee on Aging, thank you for the opportunity to testify at today's hearing regarding the role of the private sector in deterring phone scams targeting seniors. My name is Lisa LaBruno and I am the senior vice president of retail operations at the Retail Industry Leaders Association (RILA). By way of background, RILA is the trade association of the world's largest and most innovative retail companies. RILA members include more than 200 retailers, product manufacturers, and services suppliers, which together account for more than $1.5 trillion in annual sales, millions of American jobs and more than 100,000 stores, manufacturer facilities and distribution centers domestically and abroad.

The issue of senior's scams is unfortunately a growing problem and one that our members take seriously. I applaud the Committee for holding today's hearing on this important issue because we know that criminals are persistent and they will prey on anyone, including the elderly.

At the onset, it is important to understand that our retail members carry tens of thousands of products in a given store, and that the vast majority of the time we do not produce, design, or manufacture these items. We rely on the expertise of our vendors to create great products that our customers want. At the same time, since we are closest to the customer and above all we value the relationships we have with them, we want to make sure, to the extent possible, that the products are being used safely, comply with all necessary Federal, State and local laws and regulations, and most importantly provide value to the customer.

Today's hearing is focused on so-called "reloadable pack cards," which are prepaid cards that have grown in popularity with our customer base. They provide a valuable service by transferring funds easily and affordably between two individuals. For example, parents may use them to transfer spending money to a college graduate backpacking through Europe; a grandparent could easily send birthday money to a grandchild off at school; and the unbanked or underbanked can use this product to pay utility bills or transfer money to a landlord for rent payments. According to statistics by the providers of these reloadable pack cards, over 99 percent of all transactions using these cards are for legitimate purposes.

Unfortunately, these reloadable pack cards also appear to be just one of the latest mechanisms for fraudsters to con people, including the elderly, out of their money. In these unfortunate instances, a fraudster will dupe a victim into sending funds via one of these reloadable pack cards by tricking the victim into believing a loved one needs immediate financial assistance, that the victim's utilities will be shut off if payment is not made, that the money is needed as collateral in order for the victim to claim a large prize.

There is no failsafe way that retailers can guarantee that these types of scams will never occur using these products. However, more can be done by all stakeholders, including law enforcement, the companies that design, manufacture and service these reloadable pack cards, and merchants, by providing consumer education, strengthening safeguards built into these products, and partnering with law enforcement to deter criminal activity on the front end, and arrest and prosecute criminals on the back end.

While retailers are an important player in this process, we are only one link in this chain, and so we appreciate when our customers, law enforcement, pre-paid card vendors, regulators and Congress, bring to our attention areas of abuse. As responsive companies built on a foundation of trust with our customers, we want to see to it that we do our part to minimize the fraud that could occur on these transactions.

Retailers have taken various steps to mitigate the risk of seniors falling prey to these scams including employee training, signage, and point-of-sale enhancements. For example, many retailers train their staff to identify signs of common scams in order to prevent the transaction from proceeding and protecting their customers from loss. Many of these reloadable products have large warning labels directly on the package warning customers about the dangers of giving the PIN to unauthorized users. Additionally, point-of-sale information can be used to educate customers about the dangers of fraudsters. POS enhancements have been installed to alert retailers and the reloadable card vendor to possible suspicious activity and to stop the transaction when certain thresholds are met.

In discussing this issue with our member companies they were quick to share with us success stories and enhancements they are making on their own. One retailer provides an annual training for their employees focused on consumer fraud and elder abuse. This training identifies some of the common scams of which they

are aware of and directs their colleagues to be on the lookout for red flags suggesting that a customer may be the victim a scam. If a colleague suspects a customer may be a victim of a scam, the colleague is directed to alert the customer to the risk of fraud and ask the customer to reconsider the purchase. This training has paid off. For example, an elderly Connecticut couple this past summer went to a store to purchase prepaid cards because they had been misled into believing their grandson was in police custody and directed to purchase prepaid cards to make a bail payment on his behalf. A colleague warned the couple of the risk of scams, and the couple did not proceed with the purchase after confirming with the police that their grandson had not been arrested. A store in Rockland County, NY, prevented a similar scam against a senior customer who believed the IRS told her to purchase prepaid cards to pay off back taxes. In addition to employee training, this store has also posted signage at all of its prepaid card displays advising customers to be aware of such scams. These are just a few of the many examples of what retailers are doing to protect their customers.

However, despite our best efforts, unfortunately people can always fall victim to scams of any kind. Recently, we were made aware that two of the largest providers of these reloadable pack cards—GreenDot and InComm—have announced plans to pull their product from store shelves by the end of first quarter of 2015. We fully expect that all RILA members will comply with this deadline, and, we have also been made aware that a third provider of these products—Blackhawk—plans to enhance the security aspects of its reloadable pack cards; we look forward to learning more about the modifications Blackhawk is making.

I want to make one thing clear—it is not RILA's role to stand between the relationships that merchants have with their vendors, and so we look forward to seeing what types of innovative new products will come into the marketplace that will satisfy our customers' demand for these services, while enhancing the security of these transactions.

Finally, we must make sure that law enforcement has all the resources and tools necessary to combat these crimes. It may be appropriate for Congress to examine whether the laws on the books today are sufficient to act as a deterrent for criminals engaging in this behavior in the first place.

In closing, RILA appreciates the opportunity to testify before the Committee on this important issue. We want to work with you, our suppliers and partners in law enforcement to enhance the security of these products, while still filling a need in the marketplace. Thank you and I look forward to answering your questions.

Statements for the Record

STATEMENT OF SENATOR SUSAN M. COLLINS, RANKING MEMBER

Chairman Nelson, before we get started, I would like to take this opportunity to thank you for the extraordinary leadership you have provided this Committee these past 2 years. The never-failing courtesy you have shown to me and my staff, to the other members of the Committee, and to all who have testified before us has truly been the hallmark of your tenure as Chairman. Our achievements as a Committee trace directly to the bipartisan tone you set, and the spirit of comity and cooperation that have prevailed as a result.

Your high standards have carried over to your staff as well, and I would be remiss if I did not thank them also for all of the hard work they have done on behalf of the Committee.

It is fitting that the last hearing you and I will lead as Chair and Ranking Member examines once again the problem of scams targeting America's seniors, and how to stop them. This incredibly important topic has rightly been the focus of more of our hearings in the past 2 years—eight, counting today—than any other issue we have explored together as a committee.

Our work on this topic began with a hearing early last year on the notorious "Jamaican Phone Scam," run by sophisticated criminal gangs operating out of boiler rooms in Jamaica. Before our hearing, these con artists placed an estimated 30 thousand phone calls every day to victims in the United States, and stole an estimated $300 million each year from tens of thousands of American seniors.

As a result of our hearing, the Jamaican government finally reformed its laws to target the scammers, and Federal prosecutors have since indicted dozens of individuals on conspiracy charges for their participation in these scams.

One common theme that has emerged from these hearings is the role played by prepaid debit cards. It is difficult to say exactly how much money Americans lose through scams involving prepaid debit cards, since many victims don't report their losses. The Federal Trade Commission, however, says that Americans reported losing nearly $43 million through prepaid debit card scams last year alone. Because these cards are widely available and convenient to use, and because money transferred using them is untraceable, prepaid debit cards have become the monetary tool of choice for scammers.

This is especially true for cards that can be "reloaded" with money, which have a unique PIN that customers can use to transfer funds. In the typical scam, the con artist will pressure the victim into purchasing reloadable cards, putting money on the card, and then sharing the card's PIN with the scammer. Armed with the PIN, the scammer can transfer the money to his or her own prepaid debit card account and then access those funds from an ATM, through PayPal, or even by buying and reselling consumer goods on Internet auctionsites.

There are many legitimate reasons why consumers would want to use prepaid debit cards, and I note that these cards are especially important to lower-income consumers who may not have access to traditional banking services. Still, it is important that we understand what can be done by card providers and retailers to make it harder for criminals and con artists to use these cards to advance their nefarious schemes.

The witnesses who are testifying before us today will describe the actions some prepaid debit card companies and retailers have already taken to push back against the scammers, including phasing-out PIN-based reloadable cards and issuing prominent warnings to customers to be on their guard against fraud. Some retailers have also joined the battle by training their sales clerks on what to do when they spot customers who are engaging in suspicious transactions with prepaid cards. I appreciate the willingness of the witnesses to describe these efforts, and I look forward to their testimony.

Mr. Chairman, before the witnesses begin, allow me to thank you again for your leadership of this Committee. Although we will be serving in different capacities next session, I am confident we will have the opportunity to continue our work together to protect America's seniors.

Nov 13 2014

CFPB Proposes Strong Federal Protections for Prepaid Products

Bureau's Proposal Includes New 'Know Before You Owe' Prepaid Disclosures

WASHINGTON, D.C. – Today the Consumer Financial Protection Bureau (CFPB) is proposing strong, new federal consumer protections for the prepaid market. The proposal would require prepaid companies to limit consumers' losses when funds are stolen or cards are lost, investigate and resolve errors, provide easy and free access to account information, and adhere to credit card protections if a credit product is offered in connection with a prepaid account. The Bureau is also proposing new "Know Before You Owe" prepaid disclosures that would provide consumers with clear information about the costs and risks of prepaid products upfront.

"Consumers are increasingly relying on prepaid products to make purchases and access funds, but they are not guaranteed the same protections or disclosures as traditional bank accounts," said CFPB Director Richard Cordray. "Our proposal would close the loopholes in this market and ensure prepaid consumers are protected whether they are swiping a card, scanning their smartphone, or sending a payment."

Prepaid products are consumer accounts typically loaded with funds by a consumer or by a third party, such as an employer. Consumers can use these products to make payments, store funds, get cash at ATMs, receive direct deposits, and send funds to other consumers. Prepaid products are often bought at retail stores or online. Prepaid products are amongst the fastest growing types of consumer financial products in the United States. For example, the amount of money consumers loaded onto "general purpose reloadable" prepaid cards grew from less than $1 billion in 2003 to nearly $65 billion in 2012. The total dollar value loaded onto general purpose reloadable cards is expected to continue to grow to nearly $100 billion through 2014.

This proposal would apply a number of specific federal consumer protections to broad swaths of the prepaid market for the first time. The proposal would cover traditional plastic prepaid cards, many of which are general purpose reloadable cards. In addition, the proposal would cover mobile and other electronic prepaid accounts that can store funds. The prepaid products covered by the proposal also include: payroll cards; certain federal, state, and local government benefit cards such as those used to distribute unemployment insurance, child support, and pension payments; student financial aid disbursement cards; tax refund cards; and peer-to-peer payment products.

Prepaid Protections

Many consumers use prepaid products as an alternative to traditional checking accounts. Currently, however, there are limited federal consumer protections for most prepaid accounts. The proposal would ensure that most prepaid account consumers would have important protections under the Electronic Fund Transfer Act after registering their account. The protections are generally similar to those checking account consumers already receive and include:

- **Easy and free access to account information:** Under the CFPB proposal, financial institutions would be required to either provide periodic statements or make account information easily accessible online and for free. Unlike checking account customers, prepaid users typically do not automatically receive periodic statements. The proposal would ensure that consumers are able see their account balances and a history of their transactions and fees.

- **Error resolution rights:** The proposed rule would require financial institutions to work with consumers who encounter errors with their account. Currently, prepaid customers who are double-charged for a transaction or charged an incorrect amount may not be guaranteed a practical way to fix the problem. This proposal would require financial institutions to investigate errors that consumers report on registered accounts and to resolve those errors in a timely manner. If the financial institution cannot resolve an alleged error within a certain period of time, it would be required to temporarily credit the disputed amount to the consumer to use while the institution finishes its investigation.

- **Fraud and lost-card protection:** The proposal would protect consumers against unauthorized, erroneous, or fraudulent withdrawals or purchases, including when registered cards are lost or stolen. Consumers receive this protection on their credit and debit cards, but it is not guaranteed on prepaid products. If consumers lose their prepaid card or find erroneous or fraudulent charges on their prepaid account, the rule would limit their responsibility for transactions they did not authorize and create a timely method for them to get their money back. As long as the consumer promptly notifies their financial institution, the consumer's responsibility for unauthorized charges would be limited to $50.

Know Before You Owe: Prepaid Fees

The Bureau's proposal also includes new "Know Before You Owe" prepaid disclosures that would provide consumers with standard, easy-to-understand information about the prepaid account. Consumers cannot always tell what fees apply to their prepaid cards before purchasing them because such disclosures are inside the packaging or hard to find online. The current lack of an industry-wide standard on prepaid-card fee disclosures can make it difficult for consumers to comparison shop and make well-informed decisions. Under the proposal, prepaid consumers would have access to:

- **Standard, easy-to-understand information upfront:** The CFPB's proposal includes two required forms, one short and one long, with easy-to-understand disclosures. The short form would concisely and clearly highlight key prepaid account information, including common costs like the monthly fee, fee per purchase, ATM withdrawal cost, and fee to reload cash onto the account. In addition, under the CFPB's proposal, consumers would have to receive or have access to a full set of the account's fees and related information before acquiring the account. The long form would contain all of the fees on the short form, plus any other potential fees that could be imposed in connection with the account.

- **Publicly available card agreements:** To facilitate comparison shopping, this proposal would require that prepaid account issuers post their account agreements on their websites. Additionally, issuers would be required to submit those agreements to the Bureau for posting on a public, Bureau-maintained website.

The proposed disclosures are available at:
http://files.consumerfinance.gov/f/201411_cfpb_prepaid-model-sample-disclosure-forms.pdf

Credit Protections

The proposal also includes strong protections in connection with credit products that allow consumers to pay to spend more money than they have deposited into the prepaid account. Under the proposed rule, if consumers choose to use a credit product related to their prepaid account, they would be entitled to the same protections that credit card consumers receive today. These protections largely stem from the Truth in Lending Act and the Credit Card Accountability Responsibility and Disclosure Act of 2009. The protections that would also apply to prepaid credit products include:

- **Ability to pay:** Like credit card issuers, prepaid companies would be required to first make sure consumers have the ability to repay the debt before offering credit. Under the proposal, companies cannot open a credit card account or increase a credit line related to a prepaid card unless they consider the consumer's ability to make the required payments. For consumers under 21, the companies would be required to assess these consumers' independent ability to repay the credit.

- **Monthly credit billing statement:** Prepaid companies would be required to give consumers the same monthly periodic statement that credit card consumers receive. This statement would detail consumers' fees, and if applicable, interest rate, what they have borrowed, how much they owe, and other key information about repaying the debt.

- **Reasonable time to pay and limits on late fees:** Prepaid companies, like credit card issuers, would be required to give consumers at least 21 days to repay

their debt before they are charged a late fee. Additionally, late fees must be "reasonable and proportional" to the violation of the account terms in question.

- **Limited fee and interest charges:** During the first year a credit account is open, the total fees for prepaid credit products would not be allowed to exceed 25 percent of the credit limit. Card issuers generally are prohibited from increasing the interest rate on an existing balance unless the cardholder has missed two consecutive payments. Card issuers may increase the interest rate prospectively on new purchases, but must generally give the consumer 45 days advance notice – during which time the consumer may cancel the credit account.

The CFPB's proposal also includes some additional protections to ensure that the prepaid account and the credit product are distinct, such as:

- **Thirty-day waiting period:** The CFPB's proposal would require companies to wait thirty days after a consumer registers the prepaid account before they could formally offer credit to the consumer. This would allow consumers to get experience with the basic prepaid account before deciding whether they want to apply for a credit product.

- **Wall between prepaid funds and credit repayment:** Prepaid companies could not automatically demand and take credit repayment whenever a prepaid account is next loaded with funds. Further, prepaid companies could not take funds loaded into the prepaid account to repay the credit when the bill is due unless the consumer has affirmatively opted in to allow such a repayment. Even then, companies cannot take funds more frequently than once per calendar month. Payment also cannot be required sooner than 21 days after the mailing of the periodic statement.

In May 2012, the CFPB issued an Advance Notice of Proposed Rulemaking on prepaid cards. The Bureau carefully reviewed all of the comments received and conducted outreach in the development of this proposal.

The proposed rule and disclosures will be open for public comment for 90 days after its publication in the Federal Register. A copy of the proposed rule, which includes information on how to submit comments, will be available Thursday at: http://www.consumerfinance.gov/regulations/

A CFPB study of the prepaid market can be found at: http://files.consumerfinance.gov/f/201411_cfpb_study-of-prepaid-account-agreements.pdf

###

The Consumer Financial Protection Bureau is a 21st century agency that helps consumer finance markets work by making rules more effective, by consistently and fairly enforcing those rules, and by empowering consumers to take more control over their economic lives. For more information, visit ConsumerFinance.gov..

○