ORIGINAL

HOUSE OF REPRESENTATIVES
COMMONWEALTH OF PENNSYLVANIA
COMMERCE COMMITTEE HEARING

IN RE: IDENTITY THEFT & CREDIT CARD FRAUD

NORTH OFFICE BUILDING
HEARING ROOM 1
HARRISBURG, PENNSYLVANIA

WEDNESDAY, MAY 14, 2003, 11:03 A.M.

BEFORE:
HON. GEORGE C. HASAY, CHAIRMAN
HON. THOMAS R. CALTAGIRONE
HON. JAMES E. CASORIO, JR.
HON. GORDON DENLINGER
HON. KEITH GILLESPIE
HON. JOHN R. GORDNER
HON. ADAM HARRIS
HON. HAROLD JAMES
HON. JERRY L. NAILOR
HON. DAVID REED
HON. MARIO SCAVELLO
HON. THOMAS L. STEVENSON
HON. CURTIS W. THOMAS
HON. GUY A. TRAVAGLIO
HON. JAMES WANSACZ
HON. MATTHEW N. WRIGHT
HON. THOMAS F. YEWCIC

JEAN M. DAVIS, REPORTER
NOTARY PUBLIC

ARCHIVE REPORTING SERVICE
2336 N. Second Street (717) 234-5922
Harrisburg, PA 17110 FAX (717) 234-6190

T2003-021

I N D E X

CHAIRMAN HASAY: The hour having arrived, the House Commerce Committee will now come to order. The Commerce Committee today is going to have a hearing on identity theft and credit card debt.

I would like to have the members that are here introduce themselves and the county that they represent, starting at the front table first, left to right. Dave.

REPRESENTATIVE REED: Representative Dave Reed, Indiana County.

REPRESENTATIVE YEWCIC: Representative Tom Yewcic, parts of Cambria and Somerset Counties.

REPRESENTATIVE GORDNER: Representative John Gordner, Columbia County.

CHAIRMAN HASAY: Next table.

REPRESENTATIVE TRAVAGLIO: Representative Guy Travaglio, Butler County.

REPRESENTATIVE SCAVELLO: Representative Mario Scavello from Monroe County.

REPRESENTATIVE DENLINGER: Representative Gordon Denlinger from Lancaster County.

REPRESENTATIVE STEVENSON: Representative Tom Stevenson from Allegheny County.

REPRESENTATIVE NAILOR: Jerry Nailor from Cumberland County.

CHAIRMAN HASAY: George Hasay, Luzerne, Wyoming, and Columbia Counties.

REPRESENTATIVE CALTAGIRONE: Tom Caltagirone, Berks County.

REPRESENTATIVE CASORIO: Jim Casorio, Westmoreland County.

REPRESENTATIVE GILLESPIE: Keith Gillespie, part of York County.

CHAIRMAN HASAY: The first witness we have today is Beth McConnell.

Beth, you can come forward and grab one of those microphones and begin.

Beth is with the Pennsylvania Public Interest Research Group.

MS. McCONNELL: Great. Thank you. Good morning, Chairman Hasay and other members of the committee.

My name is Beth McConnell, and I am the director of the Pennsylvania Public Interest Research Group, PennPIRG. PennPIRG is a non-profit, non-partisan, public interest advocacy organization. We represent about 8,000 citizen members across the state.

PennPIRG works to protect consumers and taxpayers as well as revitalize participation in the Democratic process. And our state and national office have long been involved in identity theft and credit card debt issues, including testifying before Congress and the state Legislature, the publication of numerous research reports and surveys, and public outreach and education. So I thank you for the opportunity to be able to comment on this issue today.

Before I begin my background comments, I would like to start by highlighting a few key proposals that PennPIRG supports to protect consumers. And then I will provide some background and contacts on those.

The first proposal that we support is prohibiting the use of a social security number as a personal identifier as well as prohibit the public posting or display of that number.

Second is to prohibit any entity from coercing consumers into supplying their social security number as a requirement for receiving goods or services.

The third is to require that institutions seek a consumer's permission before

sharing their personal information -- this is also known as opt-in -- when the federal preemption laws expire next year.

Fourth is to instruct Congress to allow those preemption laws in the Fair Credit Reporting Act to expire next year as scheduled.

And fifth is to require that credit bureaus give consumers one free copy of their credit report annually.

And I should also mention that my horoscope on the train today said that I should be forceful and I will get what I want. So maybe I should add some additional items to that list.

In the rapidly advancing information age, a consumer's personal information is a very valuable commodity. Social security numbers, information on a consumer's buying patterns, their names, addresses, and telephone numbers and other data is often bought, sold, shared, or traded among banks, credit card companies, supermarkets, retailers, and numerous other industries.

These companies turn a profit by collecting and using a consumer's personal information without the individual's permission or knowledge, in most cases. And as a result,

consumers are losing control over who has access to their personal information and how that information can be used.

Additionally, social security numbers are often used by health insurance companies, universities, government agencies, and others as account numbers or unique personal identifiers. Even if an institution does not aim to profit from the dissemination or use of this information, the collection and storage and wide use of social security numbers places consumers at great risk. Such activity makes it much harder for consumers to control or track the dissemination of their personal information and much easier for thieves to access and misuse it.

One of the most pervasive ways that we know personal information is being misused is identity theft. It is the fastest-growing white-collar crime, with a 400 percent increase in the number of reported cases between 1995 and 2000. According to the Federal Trade Commission, there were over 5,000 reported identity theft cases in Pennsylvania in 2002, up from about 2,700 the year before. And these, of course, are just the cases that we know of. And 46 percent of the crimes in

Pennsylvania involve credit card fraud, and others included unauthorized phone or utility service, bank fraud, and fraudulent loans.

Victims of identity theft face credit denials, out-of-pocket costs, and even arrest when mistaken for a thief using their name. And the FTC does estimate that it takes the average victim of identity theft 175 hours and $808 in out-of-pocket costs just to clear their own name.

These cases average two to four years to be resolved, if it can be resolved; and the cost to businesses is astronomical. In 1997, U.S. fraud losses of VISA member banks equaled $490 million, and MasterCard member banks lost $407 million.

There is one person in particular that I would like to highlight. His name is Kevin Scott of Philadelphia. And he's somebody that PennPIRG has worked with an awful lot over the last few years. A thief was able to obtain Kevin's social security number and used this information to very easily open utility accounts at several different addresses in the Philadelphia area, leaving Kevin responsible for thousands of dollars in phone, cable, gas, and electric bills.

Now, despite the fact that a duplicate

already existed in Kevin's real name at his true address, the utility companies never bothered to contact him when the fraudulent accounts were opened to verify whether or not they were, in fact, fraudulent or legitimate. The thief also committed several crimes in Kevin's name, leading to a criminal record for Kevin despite no wrongdoing of his own.

It was actually several years before he even discovered the existence of the fraud when he requested a copy of his credit report following denial of credit. And after learning of the identity theft and criminal record, Kevin contacted the police and utility companies to close the accounts and report the crime.

However, the companies that allowed the thief to open these accounts in the first place took absolutely no responsibility in solving the problem and clearing Kevin's credit report. And despite spending more than 200 hours over a period of one year just to clear his name and report, Kevin still has to deal with the aftermath.

Erroneous information continues to appear on his credit report, and he has been unable to clear his criminal record without hiring an

attorney. In fact, he called the police station at one point and alerted them to the problem. The officer said, please don't come down here because we will have to arrest you. Hire a lawyer. That's the only way that we can deal with this. And he expects to have continued problems when he attempts to refinance his mortgage.

In another instance, a student at the University of Pennsylvania was a victim of identity theft on more than one occasion. This student believes that the thief got ahold of her social security number by rummaging through her trash in which she discarded mail from the university and it contained her printed social security number. And the thief was able to use this information to open a charge account at Target, leaving the student with unpaid bills and the burden of proving her own innocence. And she estimated it took at least 20 hours over several weeks to resolve the matter.

Adding insult to injury, a consumer does not have the right to sue if their information is misused, often preventing the consumer from recouping losses as a result of identity theft. And similarly, the financial institutions or businesses that allow the fraudulent accounts to be opened are

under no responsibility to quickly or effectively clear the victim's credit report, leaving that burden on the consumer.

Furthermore, it's very difficult for law enforcement to pursue identity theft cases. The police and attorneys generally lack the resources and the expertise that they need to fully investigate and prosecute identity theft cases.

Even in instances where a case is resolved and a victim's name is cleared of wrongdoing, often their criminal record is not expunged in state and national databases. And local police also lack the authority to pursue cases in which the crime was committed in another state, which is a very common occurrence in the electronic age when crimes against Pennsylvanians can be committed over the Internet by a thief elsewhere.

Finally, many consumers are finding that refusal to provide personal information results in penalties or other forms of punishment. The Privacy Rights Clearinghouse, which is a nationally known expert on this issue, has several documented cases in which refusal to provide a social security number has resulted in evictions, denial of garbage pickup, and even the refusal of a dentist to treat a

long-time patient.

That is why we urge you to prohibit entities from coercing consumers into supplying their social security numbers as a condition of receiving goods or services, unless, of course, the collection of that number is required under state or federal law.

Several pieces of legislation have already been introduced into the House to assist identity theft victims and give law enforcement additional authority, expertise, and resources to pursue the cases. Among them are House Bills 583 and 585 through 589 sponsored by Representative Mike McGeehan, who himself is a victim of identity theft.

But while assisting law enforcement and victims is a critical part of dealing with the problem of identity theft, we also need to do much more to prevent the crime altogether. And reducing the use of social security numbers is key to that effort.

Originally, social security numbers were only meant for the federal government's use to track wages and benefits. But now these numbers are used by a multitude of public and private institutions as identification numbers or as a

security measure to confirm an individual's identity.

However, the widespread use of these numbers completely undermines of use of it as a security measure. It also provides numerous opportunities for thieves to gain access to valuable information.

Last July, the state of California began implementing legislation that prohibited the public posting or display of social security numbers and use of them as identification numbers. Despite predictions of dire consequences by industries and institutions opposed, state officials report that implementation has been quite smooth, and there have been no reports of unmanageable expense or technological difficulty. Given their success, there is now a move to include state universities, who are currently exempted from the code in California. You will find comments from Joanne McNabb, who is the chief of the California Privacy Office, attached to my testimony.

Elsewhere, some other private and public institutions have already adopted similar rules voluntarily, such as at the University of Illinois. In 2000, the University began phasing in

their policy that prohibits the public posting or display of social security numbers and expects the process to be complete by 2005.

According to Michael Corn, who administers the policy for the Office of Planning and Budget at the University of Illinois, he said that the process fit well into a plan to integrate the University's computer systems and has not resulted in a significant expenditure of resources.

The University of Pennsylvania has also begun to evaluate their collection and storage and use of social security numbers. But while I'm unaware of any official or adopted policy ending the improper use of social security numbers at the University, Penn is now working to implement recommendations of the Task Force on Privacy and Personal Information.

Additionally, we recommend that legislation be introduced to require that all consumers get one free copy of their credit report annually. Often, victims of identity theft don't know they're victims for months or years after the crime first occurred. And this allows that criminal activity to occur virtually unnoticed for far too long. By reviewing one's credit report, the

suspicious activity can be identified and stopped much quicker.

However, consumers are only entitled to a free copy of their credit report once they have already been victims or have been denied credit and know it or have been denied credit for some other reason. Otherwise, an individual must pay a fee to review their own personal information.

We can save consumers and businesses significant -- quite frankly, a significant amount of headache and money by catching these crimes earlier and by not putting a barrier between consumers and their personal financial information. Many states already allow for one free credit report annually, and we urge that Pennsylvania do the same.

We must also put consumers back in control of their personal information by requiring that financial institutions seek affirmative permission before sharing or selling personal financial information beginning in 2004. This is often referred to as opting-in.

Current federal law only requires that a financial institution inform a consumer of their right to opt-out of some information-sharing through privacy notices that are mailed annually. However,

our research shows that these notices are inadequate. They contain complicated language, small type, very confusing instructions, and the notice of the right to opt-out is buried among pages of text. Clearly, the banks and financial institutions have an interest, a financial interest, in keeping those notices as such.

However, Pennsylvania legislators can act to change this policy. While the Federal Fair Credit Reporting Act contains a provision that preempts states from changing this law, that preemption expires in 2004.

Banks and other industries are working to convince federal regulators to extend the preemption further and arguing that FCRA needs to be reauthorized in whole. That is actually not the case. If Congress does nothing, only the state preemption piece of the law will expire, giving Pennsylvania the ability to protect consumer privacy further. I urge the Legislature to instruct our Pennsylvania congressional delegation to allow this to occur.

Again, thank you for holding hearings on this very important issue. PennPIRG looks forward to working with members of this committee on

these issues. I'd be happy to answer any questions.

CHAIRMAN HASAY: Thank you, Beth, for your testimony today. It's indeed important. We will be considering a bill that restricts the use of the social security number. We almost did yesterday, except we wanted to have the prime sponsor there for questions for the members of this committee.

Any members have any questions?

REPRESENTATIVE THOMAS: Yes, Mr. Chairman.

CHAIRMAN HASAY: Representative Thomas.

REPRESENTATIVE THOMAS: Thank you, Mr. Chairman. One quick question. If I'm not mistaken, California and Illinois both have adopted statutory provisions requiring the use of digital signatures. And digital signatures are becoming a very useful tool in dealing with this whole issue of identity theft.

I was wondering if your organization had taken a look at digital signatures or taken a look at certain things, like encryption, or some of the other progressive tools that are available now to the government and also to private companies?

MS. McCONNELL: In terms of encryption, I know that that policy has worked quite well, particularly in truncation, as well, of credit card numbers that are printed on receipts, which is kind of another way to look at it. And that's a policy that's been implemented in many other states as well.

And both policies, the digital signature as well as some of this encryption, is -- well, more the digital signatures is aimed at avoiding or preventing identity theft that occurs as a result of dumpster diving, as it's called, when a thief obtains printed materials from trash cans or steals them.

However, I think while that's important, even in this day and age when so much of this information is still stolen -- it's stolen electronically, and hackers are becoming more and more experienced -- there is still some concern for the protection of our privacy, even when information is electronic.

And I think what we really need to take a look at more than anything is the sort of information that is collected that's unnecessary. It just doesn't need to be collected. What can we

reduce there in terms of that collection? And then on top of that, as you point out, how can we ensure that what we are collecting is protected?

I haven't looked specifically at the policies in California or Illinois. I don't know how well they have or haven't been working. But I will say that identity theft is still on the rise despite many efforts to safeguard the information as well as many efforts to prosecute criminals more thoroughly, which is one of the reasons why we would like to reduce the collection of that information.

REPRESENT THOMAS: Thank you. If I'm not mistaken, I think in Illinois it seems to be working pretty well around this identity theft issue. As a member of another committee, the Information Technology Committee, about a year ago or a couple years ago, we put out a blueprint in Pennsylvania.

And the issue that's in front of us for this term, this whole issue of privacy and how we can use technology to address these concerns of identity theft and the whole area of invasion of privacy, because the Internet allows me to look at all of your personal and business information and do what I want with it without any consequences.

So I really thank you for your testimony.

MS. McCONNELL: Thank you.

CHAIRMAN HASAY: Thank you. Representative Wansacz.

REPRESENTATIVE WANSACZ: Thank you, Mr. Chairman.

You mentioned here in your testimony that many states already allow for one free credit report annually. Can you give me some states that do that? And also you mentioned to Representative Thomas that businesses collect too much information already. Can you be more specific on what information you think that they collect that is unnecessary?

MS. McCONNELL: Sure. Unfortunately, I didn't come prepared with the list of states. But I do know that the state of New Jersey does allow for one free copy of the credit report. I believe the state of Connecticut does as well. I think there are a total of about 11 other states. I would be happy to forward that information to the members of the committee when I return to my office.

In terms of the second question, I'll rely -- I guess I'll relay a personal experience. I

have many of these shoppers cards in my wallet. And when I go to a CVS or a Super Fresh or other types of stores, they are billed as a way to give you greater discounts. But often what many supermarkets have done across the country is use those shoppers cards to actually track your purchases so they know what you buy. And that allows them to market products to you, whether that's a different brand of shampoo or cereal.

Now, a few years ago one individual was purchasing a large amount of alcohol at a supermarket in another state. And he was involved in a rather bitter custody dispute and divorce proceeding. And there was great concern over whether or not that information could be used against him in this particular dispute. And that's just one example.

Financial records, financial information, for example, your bank account balances and the types of things that you purchase with your debit card, that information is collected and used by the financial institution to market goods and services to you.

They also have the right to share some of that information with affiliates of the company,

which is an increasing problem following the passage of the Gramm-Leach-Bliley Act in Congress a few years ago that allowed all these mega-mergers where a bank, a savings bank, and an investment bank and a whole set of other similar institutions can become affiliates of each other and then share personal information about customers among many of these affiliates.

That's one of the reasons why shifting the law from an opt-in to an opt-out -- or I'm sorry from opt-out to opt-in is something many states are considering right now. In fact, California voters will be voting actually on a ballot initiative in 2004 on this very subject.

REPRESENTATIVE WANSACZ: I understand that. I appreciate that opt-in/opt-out.

What about when we're dealing with identity theft here? Is there ways that businesses are giving too much information that is allowing people to steal their information? I know with the social security, as Chairman Hasay said, we are going to be dealing with that probably at our next meeting. That is probably one of the ways that we can correct the problem. But is there anything else that we should be looking at?

MS. McCONNELL: Well, I think social security numbers obviously is the most important because that is often all a thief needs to open a utility account. And, in fact, if they have that number but don't have your name, you can simply go on-line and for $30 or $40 purchase a whole set of other information, including your date of birth and your address and your name and your neighbors' names and every address you have ever lived at and a whole lot of other information. So certainly getting to the social security numbers piece of it is critical.

In terms of other sorts of information that we can restrict the collection of -- you know, it's a difficult issue. It's difficult because the genie is out of the bottle, in one respect. But I think as much as we can do to not only educate consumers about their rights to refuse to give certain information but also give them the right to refuse to give information -- I can bring it back to social security numbers -- by prohibiting any entity from refusing goods or services for those people that don't want to provide that number I think is best way to handle this issue.

So I'm sorry I can't quite answer your question directly with other sorts of information

because I do think that social security numbers is probably the most important.

REPRESENTATIVE THOMAS: Mr. Chairman, I have a comment.

CHAIRMAN HASAY: Representative Thomas.

REPRESENTATIVE THOMAS: If I can comment on both of those situations. I think driver's licenses -- Pennsylvania, I think, has about 180 on-line providers throughout Pennsylvania. And I know of a couple of instances -- in fact, I saw some information on one provider who used the electronic, the on-line service, to access about 3,000 drivers' records unknowingly to the drivers.

Now, we can speculate on who bought, shared, and transferred that information. And the driver's license is one piece of ID that is commonly accepted in banks and other financial institutions.

So I think that there are probably a couple of things we need to do. One is to raise the bar of consequences for participating in a program and then accessing that kind of information. And secondly, that information on the driver's license is probably some information that should be excluded unless required under certain circumstances.

In answer to your comment, social security numbers, driver's license numbers, and some other information that comes up on the driver's license.

CHAIRMAN HASAY: Your testimony was very interesting. And I'm surprised to see the losses that MasterCard and Visa banks have had. What I do with my mail anymore that has credit card applications, bank statements -- I encourage my constituents when they get their garbage and they get credit card applications or whatever, to put them through a shredder in your house, which I have had for the last couple of years now, just to protect my identity. And I have had my garbage stolen already. There are people out there trying to do that.

We had testimony in previous hearings where it's easier for a thief to go through your garbage and get those numbers than to waste his time trying to break into houses and stealing TV sets and computers.

So thank you very much today, Beth, for your testimony.

MS. McCONNELL: Thank you.

REPRESENTATIVE DENLINGER:

Mr. Chairman, one quick question.

CHAIRMAN HASAY: One final question. Representative Denlinger.

REPRESENTATIVE DENLINGER: Thank you, Mr. Chairman.

I was just wondering, you highlighted 5,080 cases were identified last year. And I'm just interested in knowing, is there a breakdown on that between high-tech means of capturing data and low-tech, such as going through garbage? Do you have any percentage on that?

MS. McCONNELL: Those come from the Federal Trade Commission. They are consumer reports that they publish annually on a whole set of different types of fraud. They do not break down the identity theft cases by the method in which the thief obtained that information because, unfortunately, the thieves are not very forthcoming. So it's hard to know.

The way that they gain that information is from the victims who have reported, I have had my identity stolen, but they don't know how. And because it's often been many years and the thief has opened many different types of accounts maybe under many different types of names and many

different locations, it's very hard to track it back to that original incident. And that's also why it's very hard for law enforcement to resolve some of these cases.

But one thing actually I will comment on is something, of course, that you can encourage constituents to realize is that there actually is an 800 number that consumers can use to opt-out of having unsolicited credit card applications being sent to their home. It's 1-888-5optout. And by putting your name on that list, it will stop any credit card company from sending these solicitations. But that's all it does is stop the unwanted credit card solicitations. It doesn't prevent the sharing or trading or selling of your personal information in any other way.

REPRESENTATIVE DENLINGER: Could you give us that phone number again?

MS. McCONNELL: 1-888-5optout, o-p-t-o-u-t.

REPRESENTATIVE DENLINGER: Thank you.

MS. McCONNELL: Sure.

CHAIRMAN HASAY: Thank you, Beth.

MS. McCONNELL: Thank you.

CHAIRMAN HASAY: Next we have Rob

Fisher, who is the senior vice-president of Credit and Call Center Operations of Boscov's. And also with him is Brian Rider, vice-president of Government Affairs of the Pennsylvania Retailers Association.

Gentlemen, welcome. You can start at your own pleasure.

MR. RIDER: Chairman Hasay and Chairman Caltagirone and committee members, thank you for the opportunity to be here today.

Mr. Fisher has prepared testimony. But before that, I just want to make a couple of brief comments. One, other than the freshmen members on this committee, the members of the Pennsylvania General Assembly last legislative session did enact and approve -- and it was signed by the Governor -- two pieces of legislation: One, making identity fraud a crime in Pennsylvania and the other legislation outlining the specifics of what details or constitutes identity fraud. And Representative Matt Baker, your colleague, was the prime sponsor of the House Bill, who is also a victim of identity fraud personally; and Senator Stewart Greenleaf was the prime sponsor of the other vehicle. So I did want to bring that to your

attention, especially for the freshmen members, that Pennsylvania does currently have ID fraud law.

So with that, I will turn this over to Mr. Fisher. And I think, following his prepared remarks, he would like to make some comments responding to some of the comments that Ms. McConnell made, if that's the committee's pleasure.

Thank you.

MR. FISHER: Good morning. Mr. Chairman and committee members, thank you for the opportunity to present testimony today. My name is Rob Fisher. I'm vice-president of Credit and Call Center Operations for Boscov's department stores. I'm testifying today on behalf of the Pennsylvania Retailers' Association. I would like to thank Chairman Hasay and Chairman Caltagirone and the members for providing me the opportunity to testify before the House Commerce Committee.

Boscov's is a Mid-Atlantic department store chain. In addition to stores in Maryland and New Jersey, we have three stores in Delaware, three stores in New York, and more than two dozen stores in our home state of Pennsylvania.

Boscov's employs over 10,000 people.

As the third largest industry in Pennsylvania, retailers employ over 1.25 million people earning more than $25 billion in wages. The PRA is the Commonwealth's oldest and most successful retail trade association. The retail industry in Pennsylvania is comprised of approximately 30,000 establishments employing nearly 300,000.

As towns and cities grew in Pennsylvania, retailers began using their local merchants associations as a trusted repository for information about the customers with whom they dealt. In order to access these customer files, the merchant had to be willing to place his own information into the system.

There was a strong incentive to be accurate and careful with what you put in because you expected the same care from the other merchants with whom you were sharing. Trust and integrity were important. Eventually the merchants associations were merged or sold and became part of the credit reporting system we have today.

Boscov's currently has 1.1 million active credit card accounts. During the peak holiday season, about 600,000 of these customers use their Boscov's card and receive credit card

statements from us. As many of you know, consumers often use retail credit as their gateway into the larger credit market. It is very common for a Boscov's card to be the first credit card in a customer's wallet. By building a good credit relationship with us, they help build a good credit file with the credit bureaus. This, in turn, makes them eligible for other credit products, such as a car loan or even a first mortgage.

The history and success of retail is inextricably intertwined with credit granting in this country. Today, nearly 80 percent of purchases made at Boscov's stores are some type of credit card, be it Visa, MasterCard, Discover, or the Boscov's card. In 2002, consumer spending represented two-thirds of the Gross Domestic Product. If you do some simple calculations, you realize that most of the transactions in our economy don't happen in cash. They happen on credit.

Mr. Chairman, as you know, it is consumer spending that has served as the ballast in an otherwise unstable economic environment. Consumers are taking advantage of quick, low-cost credit at record rates, from first-time home mortgages and mortgage refinancings to car loans and

other consumer credit transactions.

In fact, our credit card center is also a call center where customers can work out issues such as merchandise delivery problems, place phone orders, seek assistance with Internet orders, and ask a whole host of questions about our products, services, and promotions. They can even opt-out of our mailing lists for catalogs, promotions, and store coupons if they so choose.

This is all made possible by information-sharing in the retail environment. Through information-sharing, we can not only market more specifically to our customers and meet their needs, but we can also do other things such as underwrite more credit and combat identity theft in our stores.

As you know, identity fraud is one of the fastest growing and most troublesome crimes in the United States. At Boscov's we have implemented a number of safeguards to help protect our business and our customers. As you will see, many of these procedures rely directly on the sharing of information.

When a customer applies for a Boscov's charge card in one of our stores, they must present

a current, valid state or federally issued picture ID, such as a driver's license or passport. When we pull the customer's credit bureau report, we determine if the name, address, social security number, and various other characteristics given by the customer match both the information on the ID presented and the information contained in the credit reports and also to request human review for any credit bureau report that contains a written consumer statement. Questionable applications are referred for further processing to ensure that the applicant is, in fact, who they purport to be.

ID fraud prevention does not stop when the credit application is approved. Many retailers have models or neural networks that identify unusual purchasing behavior. For example, if we see an account that is normally only used for small purchases suddenly being used to make large, high-risk purchases on-line using a different shipping address, our systems will flag the transaction as highly suspicious and it will be referred to a special unit for investigation.

Beyond these complex technical systems to identify potentially fraudulent purchases, perhaps the retailer's best weapons in fraud

prevention are our employees. Last week in the Washington, D.C., area, one of the largest ID fraud/credit card fraud rings was arrested.

A Target store employee who noticed a customer making unusual purchases with multiple credit cards tipped off the authorities. The police discovered credit card production equipment and lists containing the names, account numbers, and expiration dates for over 10,000 Visa/MasterCard accounts.

Boscov's employees have worked together to identify sets of transactions being shipped to a self-storage unit in southern Florida. When police arrived, they discovered a vast array of merchandise from multiple mail-order and Internet sites. On a weekly basis, we identify transactions that are fraudulent and notify the consumer involved, the creditor, and/or the police, when appropriate. We have dozens of apprehensions and convictions to our credit.

We also have a number of customers who either have in the past been victims of identity fraud or who believe they are likely to be victims. For these customers, we program our register system to immediately refer the sale to our credit center.

Here we will verify the customer's identity via a valid ID or password.

Sadly, ID fraud continues to grow and affect both of its victims, the merchant and the customer. It is important to understand that in virtually every case of identity theft, the retailer bears the burden of the financial loss, either through credit write-offs on our own accounts or in chargebacks on third-party transactions.

In addition to the direct financial loss, the retailer bears other costs associated with ID fraud and credit card fraud. These include payroll and benefits for customer service representatives to help consumers understand their rights and to guide them through the process of getting their credit bureau reports corrected, loss of consumer confidence in the credit system, and related lost sales.

Our losses from ID fraud continue to grow year after year despite our best efforts. We are constantly challenged to find new patterns in our many data sources that will help us identify fraudulent transactions without inconveniencing our legitimate customers. The ability to share, aggregate, and search affiliate and third-party data

sources is paramount in the effort to protect Boscov's and our valued Boscov's customers.

In closing, I would again like to emphasize the retail industry's strong support for internal measures to prevent and minimize ID fraud and credit card fraud.

Mr. Chairman and members of the committee, consumers have come to expect instant access to credit when purchasing everything from an automobile to consumer goods such as furniture, appliances, and apparel. In the final analysis, we in the retail industry have a real concern that without better federal and state safeguards for issuing identifying documents, without a structure for more cohesive police support at the local, state, and federal level, ID fraud will continue to grow and both of its victims, retailers and our customers, will continue to suffer.

Thank you again for the opportunity to testify today. I look forward to working with the members of the House Commerce Committee as you continue your efforts to reduce ID fraud. I am happy to answer any questions that you may have at this time.

CHAIRMAN HASAY: Thank you, Mr. Fisher

and Mr. Rider.

Questions? Representative Yewcic.

REPRESENTATIVE YEWCIC: Thank you. Real quick, you mentioned something about information-sharing within Boscov's. Is that information internal? Does Boscov's sell information to other retailers?

MR. FISHER: Part of the privacy legislation that was passed federally, called the Gramm-Leach-Bliley Act, all financial institutions have to provide a privacy disclosure. As part of our privacy disclosure, we do state that we may share that information. We may share public and private customer information. The consumer does have the opportunity to opt-out of that at any time.

I can tell you that other than internally supportive programs to where there is not necessarily a sale of information but we're utilizing a third party to help us sell some additional merchandise, we don't do any sale. We don't profit by selling our customer information.

REPRESENTATIVE YEWCIC: When you do your ads and promotions, which my wife likes to receive -- I can say that because she's not here -- you contract that out for other printing?

MR. FISHER: We do some of it internally and some of it we do use a partner for outsourcing, yes.

REPRESENTATIVE YEWCIC: When you do that, is that a confidential mailing list or can they use those for other customers?

MR. FISHER: No. As part of the Gramm-Leach-Bliley Act, we actually make our vendors sign a privacy disclosure that says that they agree not to use our information for anything other than what it was given to them for.

REPRESENTATIVE YEWCIC: Thank you, Mr. Chairman.

CHAIRMAN HASAY: Any other questions? Gentlemen, thank you very much for your testimony. And we're hoping that the ID theft bills that are in the House Judiciary Committee and also the social security number restriction bill that is in this committee will be taken up shortly.

Thank you again for your testimony.

MR. RIDER: Thank you.

MR. FISHER: Thank you.

CHAIRMAN HASAY: Thank Mr. Boscov on behalf of the committee as well.

MR. FISHER: Okay.

CHAIRMAN HASAY: Our next witness we have is Lieutenant George Bivens from the Pennsylvania State Police. You can proceed at your own convenience.

MR. BIVENS: Good morning, Mr. Chairman and members of the committee. I am Lieutenant George L. Bivens, Commander of the Organized Crime Section within the Bureau of Criminal Investigation for the Pennsylvania State Police. On behalf of Colonel Jeffery B. Miller, Commissioner of the Pennsylvania State Police, I would like to thank the House Commerce Committee for this opportunity today to speak on the issue of identity theft.

Identity theft is delineated in Title 18, the Pennsylvania Crimes Code, Section 4120. This statute indicated a person commits the offense of identity theft of another person if he possesses or uses, through any means, identifying information of another person without consent of that other person to further any unlawful purpose.

The unlawful activity could involve a criminal utilizing a victim's personal information in order to obtain access to loans, credit or debit cards, bank accounts, services such as telephone or

cable, or personal property ranging from groceries to automobiles.

Following the tragic events of September 11, 2001, law enforcement must also consider the use of another person's identifying information by criminals or terrorists in an attempt to gain access to restricted areas or information in order to further their criminal enterprise.

In recent years, the crime of identity theft has grown in scope with the advent of the inexpensive personal computer. Those criminals possessing familiarity with computers now have powerful resources at their disposal. By obtaining personal biographical and financial information, which is readily available on the Internet, an identity thief can pose as anyone.

Additionally, by utilizing the wide range of high-quality computer peripherals available, they are able to craft documents and identification, which allow them to create new identities or steal the identity of someone else.

Another computer-aided method of committing identity theft is known as skimming. Skimming is the practice of reading and storing the magnetic information on a debit or credit card. The

skimmed information is then re-encoded onto a blank card having a magnetic strip, thereby creating a duplicate of the victim's card.

Conversely, the technologically challenged identity thief continues to resort to time-tested low-tech methods for obtaining the personal information of a victim. Stealing mail and digging through garbage generally provides the criminal with extensive personal information to include the victim's full name, date of birth, social security number, bank account information, utilities account information, address, and telephone number. Armed with this knowledge, the identity thief is ready to apply for credit or access funds in the name of the victim.

Currently, the best source for documented statistical information concerning the problem of identity theft is the Federal Trade Commission. The FTC has been maintaining data and information regarding this crime since enactment of the Identity Theft and Assumption Deterrence Act in 1998. In furtherance of this Act, the FTC developed the Identity Theft Data Clearinghouse and its reporting vehicle, the Consumer Sentinel.

To quantify the problem of identity

theft, the following information is provided from the Consumer Sentinel:

Of 380,103 fraud complaints received nationally in 2002, the largest category of complaint was identity theft at 43 percent.

The financial costs to victims of all fraud reported in the nation during the year 2002 is estimated at nearly one-half billion dollars. And 43 percent of this figure would indicate identity theft nationwide cost victims approximately $200 million.

Individual victim cost per fraud is estimated at $2,000.

National reporting of identity theft has steadily increased since the year 2000. In 2000, which represents the first full year of reporting, 31,117 reports were received. During 2001, 86,198 reports were received. This increase indicates a 177 percent change over the previous year. Finally, in 2002, 161,819 reports were received, which represents an 88 percent increase over the year 2001.

In the year 2002, 75 percent of victims were between the ages of 18 and 49.

Of 13,119 fraud complaints received in

Pennsylvania during 2002, the largest category of complaint was identity theft at 39 percent of all complaints.

In 2002, Pennsylvania ranked 22nd among states for victims of identity theft for 100,000 population, with 5,080 victims reported.

The top three crimes committed in concert with an identity theft in Pennsylvania during 2002 were credit card fraud with 2,359 victims, phone or utilities fraud with 1,103 victims, and bank fraud with 623 victims.

The top three victim locations for identity theft in 2002 were Philadelphia with 1,202 victims, Pittsburgh with 226 victims, and Allentown with 70 victims.

Continuing, in an effort to quantify this problem, since the inception of the Pennsylvania statute regarding identity theft in 2001, the Pennsylvania State Police have received 714 complaints involving this crime. And 302 were received in the year 2001, while 412 were received in 2002. This alone represents a 27 percent increase.

This data provides a general overview of the raw, cold statistical information regarding

the crime of identity theft. What it does not provide is insight into the associated emotional problems victims of this crime encounter. Many individuals do not discover they are the victim of identity theft for months, if not years. Some victims have been duped for as long as five years.

Upon discovery, victims must spend significant amounts of time contacting creditors and credit reporting agencies in an attempt to repair the damage to their credit histories. While this is occurring, they are often unable to obtain credit and financial services, telecommunication and utility services, and even employment. Many victims report having wages garnished and tax refunds withheld.

In those instances when an identity thief has received a criminal record in the victim's name, victims have reported having licenses revoked, failing background checks, and even being arrested or detained.

Combating the crime of identity theft in Pennsylvania requires law enforcement to achieve three main objectives:

First, law enforcement personnel must be properly trained and informed regarding this

crime.

Second, they must be appropriately staffed with criminal investigators to conduct these sometimes in-depth and lengthy investigations.

Finally, the public needs to be provided with information concerning methods to protect themselves from identity theft as well as information regarding the steps to take should they become a victim. Each of these objectives will be explored more fully.

In Pennsylvania, the state police are tasked with providing police services to those areas and citizens who find themselves without their own police department. We are a full-service department, performing functions ranging from traffic enforcement to criminal investigations.

Our criminal investigators are responsible for the investigation of all types of crime. As such, our investigators must receive training and obtain expertise in all facets of criminal investigations.

Training specific to identity theft and fraud is available to them and Pennsylvania's law enforcement community through numerous sources. Some examples are, the Pennsylvania State Police

Academy, the Mid-Atlantic Great Lake Organized Crime Law Enforcement Network known as MAGLOCLEN, the National White Collar Crime Center, International Association of Financial Crimes Investigators, the U.S. Department of Justice, and local banking institutions.

Generally, individual instances of identity theft are investigated by a criminal investigator assigned to one of our troop commands. In those instances when a case of identity theft is indicative of organized criminal activity, the Pennsylvania State Police rely upon the Organized Crime Division of the Bureau of Criminal Investigation.

Members of this specially selected group of investigators are strategically located in task forces throughout Pennsylvania. They work with their troop counterparts as well as local and federal investigators on cases involving large monetary losses, which are usually associated with organized groups of criminals. These groups may be associated with traditional organized crime, displaced ethnic groups, or simply enterprising local criminals.

In an attempt to deter or mitigate the

crime of identity theft, the Pennsylvania State Police provide the following information to law enforcement agencies and the general public:

First, how do I protect myself? These and other protective measures will not absolutely guarantee you will never become a victim of identity theft, but employing one or more of these can drastically reduce your risk.

Give your social security number only when it is absolutely necessary and do not carry your social security card with you. Leave it at home or in a secure place.

Periodically request a free copy of your social security personal earnings and benefit statement from the Social Security Administration, 1-800-772-1213.

Memorize your ATM password and shield the keypad when entering your password at ATM machines.

Do not place bill payments in your mailbox for pickup. Mail your bills directly from the post office.

Shred all documents containing personal information, especially bills, credit card receipts, pre-approved credit card offers, and bank

statements, before you throw them away.

Annually obtain a copy of your credit report from the three major credit reporting agencies: Trans Union, 1-800-680-7289; Equifax, 1-888-766-0008; and Experian, 1-888-397-3742.

Immediately correct all mistakes identified on your credit reports in writing. Approximately 70 percent of all credit reports contain some erroneous information.

Have your name removed from lists sold to companies offering pre-approved credit cards by contacting the three credit reporting agencies and taking advantage of their opt-out service. One number, 1-888-567-8688, reaches all three agencies.

Do not give your credit card number over the telephone unless you have initiated the call. Ensure that neither you nor the called party is using a mobile or cellular telephone.

When you purchase items with a credit card, take your receipts with you; do not toss them away.

Do not put your credit card number on the Internet unless it is an encrypted or secured site.

What if I become a victim of identity

theft? Identity theft can occur even if you have been careful about protecting your personal information because of the ever-increasing skill employed by professional thieves. The exact steps that you should take after becoming a victim of identity theft will vary depending upon your circumstances; but in most instances, the following steps should be taken.

Contact the security department of the respective financial institution, both verbally and in writing, for each account that has been opened or tampered with and close these accounts. The federal Fair Credit Billing Act limits your liability for unauthorized charges to $50, but it's your responsibility to make the appropriate notification in writing within 60 days after the fraudulent activity has been discovered. Once the financial institution acknowledges the fraud, ask them to send all three credit reporting agencies a letter confirming fraudulent activity.

In the past, one necessary step included contact with each of the nation's three major credit reporting agencies, Trans Union, Equifax, and Experian. In an effort to streamline the process, the credit reporting agencies have

agreed to begin sharing fraud-related information. As of April 15, 2003, identity theft victims need only make one toll-free call to any of the three nationwide credit reporting agencies. The information they provide will be automatically shared with the remaining agencies for inclusion in their records.

Within 24 hours of being notified, each credit reporting agency will post a security alert on the victim's credit file, which will be viewed by all lenders or other users accessing future reports. The alert will notify lenders of the reported fraud, thereby assisting them to avoid opening a fraudulent account in the victim's name. The credit reporting agencies will also remove the victim's name from the lists of pre-approved credit or insurance offers for a period of two years.

Additionally, the agencies have agreed to provide each victim with a copy of his or her credit file and to simplify the information-verification process to include deletion of fraudulent information.

File a complaint with your local police department or the law enforcement agency where the identity theft took place. Also, file a

complaint with the Federal Trade Commission Identity Theft Hotline by telephone at 1-877-IDTHEFT. Although the FTC has no criminal law enforcement authority, they can pursue civil remedies and assist victims in resolving the problems associated with the crime.

Report the fraudulent use of your social security number to the United States Social Security Administration at 1-800-269-0271. Under certain circumstances, a new social security number may be issued.

Notify your nearest United States Postal Inspection Service if you suspect the theft of your mail.

If your ATM card has been lost or if your password has been compromised, immediately notify your bank. The Electronic Fund Transfer Act limits your losses to $50 if you make this report within two business days. If you wait more than 60 days to make the report, you could lose all the money that was taken from your account.

If checks were stolen or fraudulent bank accounts were established, report this to your bank and to the major check verification companies, Telecheck, 1-800-366-2425; Certegy/Equifax,

1-800-437-5120; Global Payments/CheckRite, 1-800-766-2748. Request they notify retailers who use their service that you were the victim of identity theft.

If you're a victim of identity theft, never agree to pay any portion of the debt just to get collection agencies off the case. The Fair Debt Collection Act prohibits collectors from contacting you if within 30 days after you receive their written notice, you send them a letter refuting the debt. Along with your letter, send supporting documentation, police report, letters from credit reporting agencies, etc., to substantiate your position.

Unfortunately, it is impossible to protect yourself entirely from identity theft, but following the safeguards detailed herein can certainly reduce your risk. Publications by the Federal Trade Commission can provide further information on how to prevent identity theft. These publications can be obtained by contacting the FTC by telephone at 1-877-IDTHEFT or by visiting their websites at http://www.ftc.gov or http://www.consumer.gov. Phone counselors at the FTC can assist callers on how to take advantage of

their consumer rights and on what actions need to be taken to restore their credit.

Additionally, the Pennsylvania State Police provides numerous other services to Pennsylvania's citizenry and law enforcement community in dealing with the problem of identity theft. The Bureau of Forensic Services offers examination of questioned documents, handwriting comparisons, and patent and latent fingerprint identification and comparison.

The Polygraph Unit in many instances is required to determine the veracity of involved suspects. The Community Services Unit performs speeches and provides information to community groups concerning how to reduce the probability of becoming a victim of this type of crime. The Bureau of Criminal Investigation provides briefs, which provide information concerning prevention and response methods for crimes such as identity theft.

Finally, with the advent and ease of access to computer technology, the State Police Area Computer Crime Task Forces have become an invaluable resource to Pennsylvania law enforcement, particularly in those instances when a computer has been utilized in some way to steal an individual's

identity or commit a crime utilizing another's identity.

As you can see, the Pennsylvania State Police brings a wide variety of investigative resources to combat the evolving problem of identity theft in the Commonwealth. Through experience, we have learned to utilize and share these resources with local, state, and federal investigators. Only by sharing resources and staying ahead of the criminal mind will we be effective in this crime-fighting effort.

Finally, recent legislative changes to Pennsylvania's Identity Theft Statute have made investigation and prosecution for this crime a more efficient and effective process. Penalties have been stiffened and venue now includes the residence or employment address of the person whose identifying information has been lost or stolen or has been used without the person's consent. The clarification of venue is particularly important, as many of the crimes associated with identity theft occur in other jurisdictions, states, or countries.

In closing, I would like to thank Chairman Hasay and the members of the committee for the opportunity to address you today on this issue.

As a member of the Pennsylvania State Police, each officer carries on a tradition of excellence begun in the year 1905. As part of this tradition, it is the mission of each member to effectively investigate crime and criminal activity, provide investigative assistance and support to all law enforcement agencies within the Commonwealth, and promote public awareness concerning personal responsibility regarding crime reduction. This includes the crime of identity theft.

I welcome the opportunity to respond to any questions or comments you may have.

CHAIRMAN HASAY: Thank you, Lieutenant, for your testimony today. It was very interesting. The phone numbers that they have up there are very interesting. I intend to put a press release out on your testimony because I think those phone numbers are important. ID fraud is on the rise. It's just really rising. The public is going to have to be aware of their trash and what they do with some of the other stuff.

Some members have some questions. Representative Denlinger first.

REPRESENTATIVE DENLINGER: Thank you Mr. Chairman. Thank you very much for your

testimony. It's very helpful.

I'm just thinking through what has been presented here. Most of it deals with individuals and what can be done by the individual and what you do in relation to them. Not much is covered in relation to the business community. And they have a huge vested interest in making sure that, from their aspect, when security is breached in high-tech-type identity theft that they learn about that and that they take steps to correct internally whatever breach has occurred.

To what extent does the state police notify businesses, get in touch with them, to let them know that, in fact, a breach has occurred and perhaps even suggest steps that could be taken to correct or remedy that problem?

MR. BIVENS: Anytime that we would, through the course of an investigation, discover the source of information that has been stolen or misused, we would then go back to that source, whether that be an on-line company, whether it be a business, a bank, whatever. We would go back to them and, first of all, notify them that information had been taken from them and misused.

And secondly, if we are able to obtain

information specific to how that information was taken or misused, we would provide that to them. And we have our Computer Crime Task Force that is very knowledgeable. And if there was a hacking incident or anything, they would be able to provide them specific information about how that data had been obtained.

REPRESENTATIVE DENLINGER: Very good. Thank you.

CHAIRMAN HASAY: Representative Nailor.

REPRESENTATIVE NAILOR: Thank you, Mr. Chairman. Thank you, Lieutenant. I appreciate your testimony.

One thing that really jumped out at me here is that approximately 70 percent of all credit reports contain some erroneous information. Now, I don't know if the majority of the people in Pennsylvania go out and check their credit reports. I have not done that on myself. So I assume a lot of people probably have not done that.

That would be instrumental in catching these ID thefts at some point rather than letting them go on for some extended period. As was said earlier, that would be a good idea. It was

suggested by the first presenter, Ms. McConnell, that a free annual credit report go out to credit card holders.

Now I see Mr. Rider shaking his head. I know you are not up here now, but I did want to know what your position was because it has also been reported that you're taking the biggest hit many times on these identify thefts on products being stolen. In fact, the retailers will take the hit.

Do you oppose an annual credit report?

MR. RIDER: The problem with that, Representative, the bureaus and the credit rating retailers and regional chains like Boscov's have a close working relationship with the bureaus. The problem philosophically with asking one of the large three credit reporting agencies and bureaus to provide a free report is that's what they are in the business to do. They are for-profit entities.

And that would be like going in to see your chiropractor and asking for one free adjustment each year or going into the supermarket and say, I would like a free loaf of bread each year or going to your jeweler and saying, I would like a free wristwatch.

And that's what these businesses are

in business to do, to provide credit reports not only to other for-profit businesses but to consumers who go in and purchase that information. That's philosophically the opposition with the proposal of having to provide a free credit report annually to any consumer that requests it.

REPRESENTATIVE NAILOR: I understand. And I agree with you. Philosophically I do agree with you. But when this comes up and they are telling me, we are passing this information around to people and 70 percent of it has erroneous information in it, we are telling people about you with erroneous information and if you want it, you have to buy it --

MR. RIDER: I'm happy to go back to the three majors and ask them, with respect to the Lieutenant here, about that rate of inaccuracy. I have a feeling that the bureaus may dispute that. Again, I will definitely follow up on that for you.

REPRESENTATIVE NAILOR: Do you know where that 70 percent came from?

MR. BIVENS: I believe that was from the FTC statistics that they provide. And I would also say, sir, that I'm sure that within that 70 percent, there are a number of minor errors but

errors nonetheless.

And to back up just a minute with regard to people obtaining a copy of their credit rating, from a law-enforcement perspective, whether it's free or whether a consumer has to pay for that, it's in their best interest. And we advocate that people do obtain a copy.

REPRESENTATIVE NAILOR: Right.

MR. BIVENS: Perhaps a minor error will not impact them in any way. But, as I testified, there are people who have become victims and who have not discovered it for months or years. And certainly periodically looking at that report would allow them to detect some unusual activity, something that they did not personally engage in.

REPRESENTATIVE NAILOR: And I realize it's two different extents but I'm just concerned that 7 out of every 10 reports that are being passed throughout the business community about me or my neighbors could be incorrect in some manner.

What does it cost to get a report like that, for an individual to go and get a report like that? Do you have any idea?

MR. BIVENS: I don't know.

REPRESENTATIVE NAILOR: Brian, do you

know?

MR. RIDER: Generally it will run between $10 and $20 for an individual to put in a request for a copy of the report.

REPRESENTATIVE NAILOR: Thank you, gentlemen. Thank you, Mr. Chairman.

CHAIRMAN HASAY: Lieutenant Bivens, thank you very much for your testimony today. It's been very helpful. And we are going to get some of that information out to the public. And thank the Commissioner on behalf as well.

MR. BIVENS: I will, sir. Thank you.

CHAIRMAN HASAY: Next is Edward Bianco, who is a CPA and comptroller with the Attorney General's Office. You may begin at your pleasure.

MR. BIANCO: Thank you. Mr. Chairman and committee members, thank you for the opportunity to share with you the experience as a victim of identity theft. I sat here and listened to some of the testimony and I thought it was very excellent, especially the one given by the state policeman.

I'm here, kind of, under a different type of scenario. Most people don't even know that identity theft is being committed against them for

quite a while. I happen to be lucky in the sense one day I was sitting at work and I get this call from Sears that somebody is coming in to apply for a credit card at Sears. And the information didn't match up. So Sears was pretty proactive. And I was lucky because I had an account there for about 25 years and it just didn't match up to the information given. So they alerted me to the potential fraud.

And as I was sitting there, I really didn't think too much about it because being a CPA and being an accountant and knowing how business operates, if people can't prove that you really purchased something, then you're really not going to be out something in the long run.

And even though I did know about identity theft -- and this was a few years ago before this was really hitting the news real heavy -- I didn't think too much of it. But some of my friends said, you know, Ed, I think you ought to pay some attention to this.

So I had a contact at our credit union that I called. And she said, no, Ed, this could be very serious. She still didn't get my attention to the point where it should have been at a high level. She said, Ed, let me do something. She went to her

computer and pulled up my credit report. She said, Ed, there is a problem here. I think you need to review this.

I said -- being a little anxious then -- well, what do you mean? And she said, well, Ed, they have changed your address recently. And they have changed your employment. And I said, well, why is that a big problem if it's a fraud being created or whatever? So they said, I'll drop the credit report off to your house tonight. They said, have you noticed you have been getting mail? And I said, yeah, I've been getting mail. I haven't really looked at every piece. This was in my report that started at the 30th of the month.

So at that point we went into the different accounts. She also put me in touch with the postal inspector out of Philadelphia since the address was down there. And at that point, the postal inspector thought it was very serious what was going on.

And what had culminated at that point when I got the credit report, we noticed that not only credit cards were applied for and credit granted, but people were starting to buy products, computers, other types of equipment. And in this

case, I actually found where a piece of equipment worth about $20,000 was going to be delivered to this Philadelphia address under my name.

So I got ahold of the postal inspector again and I said, what can we do? So he said, let's try a controlled delivery. So they took possession and took everything out of my hands. They did a controlled delivery and arrested the individual at the scene.

The problem was he was just a small person in this whole incident. There was other obvious criminal activity behind him perpetrating these types of credit fraud. He was just one in the situation. But they arrested him. And I spent a lot of time traveling back and forth to Philadelphia about three times for trials. And finally, they got a conviction. He plea-bargained at his trial. There really wasn't a trial.

I had to spend an enormous amount of time just shutting down my credit, going back and forth to Philadelphia, and getting involved. But the postal inspector did a fine job, I thought, considering where we were coming from. I had all my credit stopped -- or I had all this activity before the trial locked down in a matter of a couple weeks.

Then I went back out over that period of time, like the state policeman just mentioned, to notify the credit bureaus to take the information off my report. In fact, I pulled it up two days ago because I knew I was coming here. I looked through it with a fine-tooth comb. It's fairly accurate. They are very complicated. They are long and they are almost encrypted the way they are written. So you have to first find out how they are set up.

It's just like going into -- I'm a CPA so every time we audit a business, every time we go into a business, everybody's books are different so you have to kind of figure out how the system works. And these are the same, all the different credit bureaus.

Where I feel that I'm a little different, I've had this stopped. But the average person in Pennsylvania that has a fraud committed against them is kind of in a different situation because they have to pay for it.

And right before I came over here, I went out on the Internet and Equifax offers a service for $70 a year. So if you're going to get notified, you are going to have to pay the three major credit bureaus $70 a year. And some of my

accountants on my staff that saw this as a problem, they don't have the luxury of going and locking down the credit or they didn't want to so they have signed up for this service. But they don't think it's fair because it's kind of costly. And I kind of agree with them. But I went to the extreme of actually locking it down.

I think it is serious. Like, for instance, my parents, they are in their 80s. And when you sign up for this service, you will get an e-mail anytime anybody comes into your credit. But my parents, they don't have access to computers. Now, I could probably set something up for them where they can e-mail me and then I could talk to them and see what's going on. I think it's a real problem.

Where I think -- and I know this gentleman here was concerned about the cost of getting the credit report; and being a businessperson, I agree with him. I'm sympathetic. These companies are in business to make money by developing credit. However, I do think they can do some simple things that will at least shrink that down to a much smaller percentage, maybe within like a few percentage points. Because you can't

eliminate this problem.

One of the things that I think they can do is on a simple address change, when it comes into your credit, I think they can set it up and e-mail the individual. I mean, how much does that cost? They can have a computer program set up and it can be done electronically to somebody's e-mail. They are changing my address; two, if any new accounts are set up; and, three, any inquiries at all into your credit they can do a simple e-mail to an individual.

That's not going to divulge a person's credit. That's not going to compromise their business, in my opinion. I could be wrong, but I don't think so. Just send a simple e-mail, somebody is coming into your credit.

My friend at work has that done and it's working out fine. Because then I know if I'm applying for credit, if I'm going to remortgage, if I'm going to go out and get another credit card, immediately right then and there that's going to come and tell me that. If not, why is somebody going into my credit?

We sat around and thought about this for a long time after this whole incident happened.

And we're accountants and I'm an auditor and this is part of my professional life here. I try to protect business assets when I'm doing an audit. How do you do that? You set up internal controls. Well, I feel this would be a good internal control for the public.

Other than that, I would just like to thank the committee, Mr. Chairman and Representatives, for this honor to come before you and give you my side of the story. I would be glad to answer any questions.

CHAIRMAN HASAY: Well, thank you very much, Mr. Bianco, for your testimony today. I'm sorry to hear what happened. It's happening more and more each year.

Representative Nailor.

REPRESENTATIVE NAILOR: Thank you, Mr. Chairman.

Mr. Bianco and I are good personal friends and have been for some time. I don't know of anyone in my life that is more of a stickler for detail than Ed Bianco. If it can happen to him, believe me, it can happen to any one of us.

Ed, I still don't fully understand how this happens, and it really concerns me. And we had

some discussion when this all happened. How did the post office allow for someone not even there to visit a post office to change your address and have your mail sent to Philadelphia?

MR. BIANCO: That's a really good question. I was in the post office one day after this happened and I pulled this card. And what happened was a person in Philadelphia filled out this card and mailed it to the Mechanicsburg Post Office and they changed my address. It's that simple. I can go out and do it to you now.

Now, the post office has tried to put into place some safeguards such as confirming the change. But had a mistake not been made on the day after I found this going on and they delivered mail to my house -- now, not all the mail will be stopped, just the mail they fill out, Ed Bianco. If it's family, it will come. If it's with my wife, it will come. If it's with my children in my name, it will come. But a mistake was made. They were short of help. They had a person that didn't recognize the change in the mailbox they actually delivered it to.

I saw the fake credit cards in the mail. I got them. And that's when I had the credit

report. That's when I started putting two and two together when I got the notification that they changed my address. I'm lucky.

And then at that point when I told the -- the postal people actually locked down my mail. They wouldn't give me my mail. Had I not developed a relationship with the postal inspector -- I got ahold of him on a weekend -- he wouldn't have called Mechanicsburg to unlock my mail. They wouldn't have given me my mail for weeks.

But what really concerned me -- and maybe I was naive -- was the financial information because my assets are really important to me. So I wanted to make sure they were secure. And my bank statements were ready to come out that week. If they would have had my financial information, they probably could have wiped out my accounts with a little bit more ingenuity.

And there is no way you are going to protect your social security number. You can sit here and say, you can do this. You can change it. It's really not safe. It's out there too much. There's too many things going on now electronically. It's just impossible. So the best thing, in my opinion, at least from this instance, is to get a

notification. That's why I'm in favor of that.

I can't believe that the U.S. Post Office can't -- before they change an address, a person should have to walk in with this form -- I have no problems with it -- with at least an ID, a photo ID, a driver's license. To me, it's just unbelievable. I'm just trying to deal with the system the best I can. And I know from the Commonwealth of Pennsylvania and Representatives, I know this isn't your problem in that sense, but whatever we can do to bridge that gap I think would help. And I know you are going to try and we are going to do the best we can.

REPRESENTATIVE NAILOR: Thank you.

CHAIRMAN HASAY: Representative James.

REPRESENTATIVE JAMES: Thank you, Mr. Chairman.

It's just interesting -- and as Jerry said -- that if it happened to you, it can happen to any of us. But what I was interested in is you said something about if somebody checks on your credit, they would get an e-mail --

MR. BIANCO: Yes.

REPRESENTATIVE JAMES: I was asking the chairman here because I didn't hear all of it.

That person would have to pay a certain amount of money to each credit service or can they just pay one money and all of them would do it?

MR. BIANCO: I believe it would be each. And it's about -- Equifax was $69.95.

REPRESENTATIVE JAMES: Okay.

MR. BIANCO: At least it was when I just went to the computer today and pulled it up. So it would be the three main ones. It would be approximately that per year.

REPRESENTATIVE JAMES: So what would one ask for if they wanted to do that? Would they just call the credit service?

MR. BIANCO: I believe that there are different levels of service. You can have all kinds of notifications. Here, I would be glad to give this to the committee. My friend just gets an e-mail notice that somebody is coming in to his account and, I guess, who it is.

REPRESENTATIVE JAMES: Now, on the post office, have they made a change that you have to have ID in order to change your address now?

MR. BIANCO: Probably not. I'm not aware of that.

REPRESENTATIVE JAMES: Okay. Because

it seems like everybody now is saying you have to show ID. And I guess we all have to make a call to our Congressmen to say they ought to put that change in right away.

MR. BIANCO: I probably should do that, too. I would appreciate that. It would probably get further faster.

REPRESENTATIVE JAMES: No, it probably would get faster if you do it.

MR. BIANCO: At some point you lose energy.

REPRESENTATIVE JAMES: I'm just glad that you brought it up because it raises consciousness. Therefore, I'm definitely going to make the call today to the Congressmen to do whatever they have to do in order to make that change.

Thank you very much for your testimony.

MR. BIANCO: You're welcome.

REPRESENTATIVE JAMES: Thank you, Mr. Chairman.

CHAIRMAN HASAY: Any other questions? Chairman Caltagirone.

REPRESENTATIVE CALTAGIRONE: It

boggles your mind. Any of us sitting here, any one of us sitting here could become a victim that easy, just as was said. We think there's a lot of safeguards. We keep plugging holes. We'll probably plug a couple holes this session. And they are out there thinking of some other ways. I mean, the computer is one of the worst nightmares because somehow somebody, they hack in and they get the information. Anybody is vulnerable. I think with what you just pointed out with the post office, that could happen to anybody. I think you made a good point.

MR. BIANCO: The postal inspector is even at odds with his own people because he understands the seriousness of it. And even their confirmation system is flawed because if they change your address and confirmation comes in, it's going to get forwarded to the new address.

And that's why I think they should have to have an ID to come in or some other means. I think that would be the best.

REPRESENTATIVE CALTAGIRONE: Thank you.

CHAIRMAN HASAY: Thank you, Mr. Bianco, for your testimony.

MR. BIANCO: Thank you very much.

CHAIRMAN HASAY: This hearing is now adjourned. Thank you.

(The proceedings concluded at 12:35 p.m.)

I hereby certify that the proceedings and evidence are contained fully and accurately in the notes taken by me on the within proceedings and that this is a correct transcript of the same.

Jean M. Davis, Reporter
Notary Public

Notarial Seal
Jean M. Davis, Notary Public
Derry Twp., Dauphin County
My Commission Expires Mar. 29, 2004
Member, Pennsylvania Association of Notaries