PENNSYLVANIA
BANKERS ASSOCIATION

Testimony Before The PA House Consumer Affairs Committee
on the Issue of Identity Theft
Allegheny County Courthouse, Pittsburgh
April 11,2012

Thank you, Mr. Chairman and members of the House Consumer Affairs Committee, for this opportunity to testify on behalf of the Pennsylvania Bankers Association concerning the issue of identity theft.

My name is Todd Moses and I am Senior Fraud Manager at PNC Financial Services Group, Inc., located here in Pittsburgh

The Pennsylvania Bankers Association is the statewide trade association representing approximately 152 financial institutions of all sizes located throughout the Commonwealth including national and skate banks, bank and trust companies, trust companies, savings institutions, and their subsidiaries and affiliates.

Identity theft is one of the most prevalent types of fraud. Identity theft, also called "account takeover fraud" or "true name fraud," involves criminals stealing personal information about individuals and assuming their identities by applying for credit in their names, running up huge bills, not paying creditors and generally wrecking victims' credit histories. Criminals steal personal information from mailboxes and dumpsters through telemarketing scams and computer hacking. There have even been instances in which paying employees in retail establishments or financial institutions to copy down information about customers has occurred, although this is rare. Congress declared identity theft a federal crime in 1998 by passing the Identity Theft and Assumption Deterrence Act with punishment of up to 15 years in prison.

I'd like to focus my remarks on three areas: first, how financial institutions assist in protecting their customers against identity theft; second, steps consumers should take if they have become victims of identity theft; and, third, ways consumers can avoid becoming victims of identity theft.

I. Banks work diligently to protect their customers from identity theft.

Banks use a combination of safeguards to protect their customers' information, such as employee training, strict privacy policies, rigorous security standards, and encryption systems,

Many banks have special fraud detection software to help flag ID theft. This software constantly monitors accounts for suspicious activity – often identifying fraud and notifying customers before they are aware of the problem.

Bank customers are protected from loss. Most bank-related incidents of ID theft limit customer liability to $50 of unauthorized charges, and most lenders will waive that. Still, restoring an individual's identity can be an inconvenience, so it is important to take precautions to avoid becoming a victim.

Banks invest time and resources to ensure account and identity information is fully secured. Those efforts have been fruitful as identity theft has been declining over recent years and claimed the fewest victims in 2010 than in any year since data has been available.

In 2010, 8.1 million Americans were victimized by identity fraud, a 28 percent decline from more than 11 million victims in 2009, and the lowest level since Javelin Strategy and Research began reporting on fraud in 2003.1

Total annual fraud decreased from $56 billion in 2009 to $37 billion in 2010, the lowest level in the eight years that data has been collected.1

Due to the zero-liability fraud protection offered by most banks and credit card companies, most victims don't experience any out-of-pocket costs. Those who did suffered an average cost of $631, an increase from recent years due to "friendly fraud", which is conducted by an acquaintance of the victim, and new account fraud, in which accounts are opened without the victims' knowledge.1

A sharp decline in data breaches helped reduce identity fraud cases. In 2010,404 data breach cases were reported, which exposed 26 million records, compared to 604 cases in 2009, which exposed 221 million records. Only a minority of banks reported check fraud losses from ID theft. On average, 16 percent of check-related losses were due to ID theft, according to the American Bankers Association Deposit Account Fraud Survey (2011).

Most ID thefts take place offline. ID thieves rely on paper documents by invading mailboxes, glove compartments and trash cans to steal and misuse information

1 *Identity fraud Report*, Javelin Strategy & Research (2011). Retrieved at www.JavelinStrategy.com
2 *Deposit Account Fraud Survey*, American Bankers Association (2011). Retrieved at www.aba.com
3 *Identity Fraud Report*, Javelin Strategy & Research (2009). Retrieved at www.JavelinStrategy.com

According to a 2009 survey by Javelin Strategy and Research, information breaches occurred in the following categories: 43 percent from lost or stolen wallets, credit/debit cards or checkbooks; 19 percent while conducting a transaction; 13 percent from friends, family, in-home employees and neighbors; 11 percent from home computers (hacking, viruses or phishing); 11 percent from data breaches; and three percent from stolen paper mail. More recent studies have not included these statistics.[3]

Businesses, consumers and law enforcement all have vital roles and responsibilities in combating ID theft. We must work together to solve the problem.

II. **If a customer becomes** a victim of ID theft, the bank is there to help.

Once contacted, banks immediately take action by closing accounts when appropriate and beginning an investigation

Most banks have special 800 numbers and websites devoted to helping victims of identity theft.

Many banks offer special worksheets, phone numbers and standardized affidavits to send to other businesses that may need to be contacted. This special affidavit is available from the Federal Trade Commission at www.consumer.gov/idtheft.

Consumer Tips for Victims:

If an individual suspects that his or her identity has been stolen, the person should call their bank and credit card issuers immediately so they can start working on closing their accounts and clearing their name.

The mdividual should file a police report and call the fraud unit of the three credit-reporting companies (see phone numbers below).

They should consider placmg a victim statement in their credit report.

The person should also make sure to maintain a log of all the contacts he or she makes with authorities regarding the matter. The individuals should write down names, titles, and phone numbers in case they need to re-contact them or refer to them in future correspondence.

For more advice, contact the FTC's ID Theft Consumer Response Center at 1-877-ID THEFT or www.consumer.gov/idtheft.

[1] *Identity Fraud Report*. Javelin Strategy & Research (2011) Retrieved at www.JavelinStrategy.com
[2] *Deposit Account Fraud Survey*, American Bankers Association (2011) Retrieved at www.aba.com
[3] *Identity Fraud Report* Javelin Strategy & Research (2009). Retrieved at www.JavelinStrategy.com

III. Consumer Tips to Avoid Becoming a Victim

- Consumers should not give their Social Security number or other personal credit information about themselves to anyone who contacts them.

- Always remember to tear up receipts, bank statements and unused credit card offers before throwing them away.

- Keep an eye out for any missing mail.

- Don't mail bills from your own mailbox with the flag up.

- Review your monthly accounts regularly for any unauthorized charges through the Internet, phone or ATM statements.

- Order copies of your credit report once a year to ensure accuracy.

- Choose to do business with companies you know are reputable, particularly online.

- When conducting business online, make sure your browser's padlock or key icon is active, indicating a secure transaction.

- Never give out personal financial information in an email or over the phone.

- When using social networking sites, never include personal contact information including telephone numbers, Social Security number, birth date, email addresses, physical address, mother's maiden name or other information that could provide sensitive information to fraudsters or hints to passwords.

- Don't open email from unknown sources and use virus detection software.

- Protect your PINs (don't carry them in your wallet!) and passwords; use a combination of letters and numbers for your passwords and change them periodically.

-Report any suspected fraud to your bank and the fraud units of the three credit reporting agencies immediately.

- The fraud unit numbers are: TransUnion (800) 680-7289 Experian (888) *397-3742* Equifax (800) *525-6285*

I hope this information is helpful to the Committee. I would be pleased to try and answer any questions and I again appreciate this opportunity to appear before you today.

[1] *Identity Fraud* Report Javelin Strategy & Research 120111 Retrieved at www.JavelinStrategy.com
[2] *Deposit Account Fraud Survey*, American Bankers Association 120111. Retrieved at www.aba.com
[3] *Identity Fraud Report* Javelin Strategy & Research (2009). Retrieved at www.JavelinStrategy.com