Testimony before Consumer Affairs Committee
Bruce R. Beemer, Chief of Staff
Pennsylvania Office of Attorney General
April 11,2012

Good Morning Chairman Godshall, Chairman Preston, members of the Consumer Affairs Committee, and members of the public. Thank you for allowing me the opportunity to provide testimony on behalf of Attorney General Linda Kelly on this most important issue of identity Theft.

Identity Theft is one of the fastest growing and most difficult crimes facing the Commonwealth and the nation. Identity Theft can have a far reaching and disastrous impact on victims, often preventing individuals from purchasing a home or even getting a job, and those who fall prey often face an uphill battle to restore their good name.

Identity Fraud incidents are on the rise nationally by about 13 percent in 2012 from rhe previous year, and effecting about 10 million Americans* In fact, an identity is stolen every 4 seconds in the U.S. with an average cost to restore a stolen identity of about $8,000. Victims spend on average about 600 hours recovering from identity theft crimes. Pennsylvania ranks fifteenth nationally in the number of identity theft complaints (79.2 comptaints per 100,000 population or over 20,000 complaints just in 2010 alone).

As Pennsylvania's top law enforcement agency, the Office of Attorney General has dedicated staff focused on protecting the citizens of the Commonwealth from identity thieves and scam artists through public outreach and by prosecuting to the fullest extent of the law, those who use another's personal information to commit fraud.

Our community outreach presentation: How to Protect Yourself Against Identity Theft, is a power point production aimed at involving the audience through some "Do's & Don'ts" of ID Theft. Each year more than 10 million Americans have their personal information—including name, social security number, bank account or credit card number—stolen. Often thieves use this information to open phony credit card, bank or utility accounts. Occasionally, the perpetrator will use the victim's identity to secure benefits such as healthcare. This type of fraud, commonly referred to as medical identity theft, can lead to enormous problems for the victim, such as having future benefiis reduced, denial of medical coverage, and unpaid bills which often compromises credit,

Prevention and awareness are truly the keys in fighting this epidemic, as the identity fraud victim often faces monumental hurdles in an effort to recover his or her financial losses and restore their good name and credit rating. Scammers have become ever more sophisticated, and they have many more tools at their disposal with the world wide use of the internet, e-mail and social networking sites.

While computers and e-mail make it easier to communicate with people instantaneously and on a global scale, one can also access an enormous variety of information and share personal items, such as photos and videos. This ability is often abused by scammers who use the information lo identify victims. A scamrner will often use a hijacked Facebook or email accountPo steal the identity of one individual and then "solicit" help from their friends online, often asking potential victims to wire them money or provide personal information that can be used later. For example, a common Facebook trick is the scammer who steals an identity and then reaches out to afriend or relative, claiming he or she is stranded in another country and is in need of money for an airplane ticket home. in these situations, we often stress to individuals that they must think beyond the story, as the scam is designedto get you to act quickly, and thus act before you really think through the request.

In fact, consumers share a significant amount of personal information on social networking sites that is frequently used to authenticate a consumer's

identity. Sixty-eight percent of people with social media profiles shared their birthday information (with forty-five percent providing month, date, and year); sixty-three percent shared their high school name; eighteen percent shared their phone number; and twelve percent shared their pet's name. All of these are prime examples of personal information a company would use to verify your identity.

Despite the enormous uptick in computer related identity crime, the most common way for someone to have their identity stolen remains a relative, friend, co-worker or other person known to the victim. Approximately 28% of identity theft victims knew the source of their crime, while 22% were victims of computer related identity crime. Lost or stolen wallets, including checkbooks and credit card accounts, makes up 15% of identity theft, with corrupt businesses or employees responsible for about 13% of all identity theft crimes. The vast majority of criminal prosecutions in the Commonwealth for identity theft and related crimes are the result of a law enforcement investigation which identifies a person known to the victim as the culprit.

While law enforcement has had some success overall in obtaining justice for victims who know the scammer, obtaining justice for victims of compurer related scams is extremely difficult. Many scams originate in foreign countries or are extremely difficult to trace due to the increased sophistication of hackers and spammers. The biggest weapon and defense to these identity thieves is education and prevention, especially as it relates to our most vulnerable citizens. The Office of Attorney General spends considerable time and effort around the Commonwealth stressing to senior citizens and others that if a telephone or email solicitation sounds too good to be true, then you must consider it a likely scam and never provide personal information without verification. For example, one of the newer scams law enforcement has been dealing with throughout the Commonwealth is a computer solicitation which asks victims to buy credit cards from a local convenience store and then share the card information to receive prize money.

Law enforcement has clearly benefited in recent years from the passage of legislation here in the Commonwealth that makes it easier to prosecute offenders who steal the identity of another, either through the use of the computer and social networking sites or other more traditional means. Police and prosecutors have successfully utilized newer criminal statutes (See Identity Theft, 18 Pa.C.S. § 4120; Unlawful Use of a Computer, 18 Pa.C.S. § 7611; Computer Trespass, 18 Pa.C.S. § 7615) with older statutes (See Forgery, 18 PA.C.S. § 4101; Bad Checks, 18 Pa.C.S. § 4105; Access Device Fraud, 18 Pa.C.S. § 4106) to track down and prosecute identity theft offenders. Although these statutes are not as broad and encompassing as some federal statutes (such as mail and wire fraud), in the vast majority of cases they provide the ammunition necessary to bring offenders to justice.

Due to the new and sophisticated mechanisms employed by "professional" scammers and the often significant logistical hurdles associated with prosecution (jurisdiction, identification, extradition), the best approach to help residents of the Commonwealth is considerable education and outreach so that individuals are not placing themselves in a situation where they can have their identity stolen. In a number of cases, however, people are victimized through no action on their part (see the recent news stories about ten million Visa and MasterCard holders having their personal information compromised). Overall, the Office of Attorney General and other law enforcement agencies throughout the Commonwealth must continue to push education of consumers and individuals on the front end while vigorously investigating and prosecuting identity theft when these unfortunate incidents occur.

I very much appreciate the opportunity to provide these remarks to the Committee and on behalf of Attorney General Linda Kelly pledge that we will work with you in every way possible to continue to address this problem which has impacted so many of our residents, I would be happy to take any questions you might have.