Identity Theft in Maryland

Shifting Circumstances - Continuing Challenges

DEPARTMENT OF LEGISLATIVE SERVICES 2013

Identity Theft in Maryland: Shifting Circumstances – Continuing Challenges

Department of Legislative Services
Office of Policy Analysis
Annapolis, Maryland

July 2013

Contributing Staff

Writers
Sally M. Guy
Karen D. Morgan

Reviewers
Karen D. Morgan
Shirleen M. Pilgrim

Other Staff Who Contributed to This Report
Michelle J. Purcell
Kelly M. Seely

For further information concerning this document contact:

Library and Information Services
Office of Policy Analysis
Department of Legislative Services
90 State Circle
Annapolis, Maryland 21401

Baltimore Area: 410-946-5400 ● Washington Area: 301-970-5400
Other Areas: 1-800-492-7122, Extension 5400
TTY: 410-946-5401 ● 301-970-5401
Maryland Relay Service: 1-800-735-2258
E-mail: libr@mlis.state.md.us
Home Page: http://mgaleg.maryland.gov

DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF POLICY ANALYSIS
MARYLAND GENERAL ASSEMBLY

Karl S. Aro
Executive Director

Warren G. Deschenaux
Director

July 1, 2013

The Honorable Thomas V. Mike Miller, Jr.
The Honorable Michael E. Busch
Members of the Maryland General Assembly

Ladies and Gentlemen:

Identity theft has been, and continues to be, one of the fastest growing crimes in the country. It is the single largest category of fraud tracked by the Federal Trade Commission (FTC) with over 369,000 complaints submitted in 2012. According to the FTC, Maryland ranked ninth in the country for reported identity theft complaints in 2012.

This report, *Identity Theft in Maryland: Shifting Circumstances – Continuing Challenges*, was prepared in an effort to provide a better understanding of the environment in which the crime of identity theft is investigated and prosecuted in the State. The report discusses the circumstances that allow identity theft to proliferate and the scarce resources used to limit the impact of the crime.

The report was written by Karen D. Morgan and Sally M. Guy. The report was edited by Karen D. Morgan. Shirleen M. Pilgrim provided editorial direction and reviewed the final report.

I trust that this information will be of assistance to you.

Sincerely,

Warren G. Deschenaux
Director

WGD/mjp

Legislative Services Building · 90 State Circle · Annapolis, Maryland 21401-1991
410-946-5350 · FAX 410-946-5395 · TDD 410-946-5401
301-970-5350 · FAX 301-970-5395 · TDD 301-970-5401
Other areas in Maryland 1-800-492-7122

Contents

Identity Theft in Maryland:
Shifting Circumstances – Continuing Challenges

Introduction

In its most basic form, the crime of identity theft or fraud is as old as the crime of financial fraud, which, for all intents and purposes, can be traced back to the invention of money. Financial fraud, by its very nature, often involves some form of what has come to be generically referred to as identity theft – the unauthorized use of some sort of personal identifying information (PII) to illegally acquire a thing or benefit of value.

This paper is an examination of the environment in which the crime of identity fraud is investigated and prosecuted in Maryland. The information presented in this paper is derived from interviews and conversations with law enforcement personnel and assistant State's attorneys in the five largest Maryland jurisdictions – Baltimore City and Anne Arundel, Baltimore, Montgomery, and Prince George's counties. The authors interviewed financial institution investigators and staff from the U.S. Attorney's Office for the District of Maryland, the Office of Attorney General, and the Office of Public Defender. The authors also accompanied investigators as they engaged in investigations and attended workgroup and task force meetings focused on identity theft and other economic crimes.

This paper is not intended to be a comprehensive review of the investigation and prosecution of this crime throughout the State. Rather, the authors made assessments based on what was learned by looking at the activities of the five largest jurisdictions, as noted above. This paper is also not an evaluation of how police officers and investigators do their jobs. It is, instead, an examination of the circumstances that allow identity theft to propagate and how scarce resources are used to limit the impact of this crime, as represented by efforts in the five largest Maryland jurisdictions.

A Brief History of the Internet and Identity Theft

Before the invention of the Internet and the use of electronic technology to acquire personal information, an identity thief had to personally acquire documents containing PII and/or have some personal contact with a victim to obtain his or her PII. Counterfeiting of money and credit cards, confiscation of Social Security numbers (SSNs), using PII to commit tax fraud – these are not new crimes. The advent of personal and mobile technology has been a game changer, however, and has altered identity theft from one in which its prevalence ebbs and flows depending on economic conditions to one of exponential growth. The Internet was made available to commercial traffic in 1995, making way for heretofore unimagined impacts on culture, education, socialization and the explosive growth of commerce, as well as the evolution of crimes that take advantage of the speed and convenience of online interactions.

Warning Signs

Changes in the nature of fraud from one involving legwork and physical contact to one involving an increasing reliance on access to electronic information and documents were noted as early as the 1990s. For example, in 1993, before access to the Internet was widely available, the Social Security Administration initiated 343 investigations for misuse of SSNs. By 1997, when there was significantly more access to the Internet, the number of misuse investigations had more than tripled to 1,153. This was, due, in part, to the addition of more investigators, but also due to the increasing number of misuse events. In addition, the three national credit reporting agencies, (Equifax, Experian, and TransUnion) had created units to deal with credit reporting fraud in 1992. By 1994, however, the demand for public access to these agencies due to increasing fraud complaints compelled the agencies to install toll-free phone numbers for improved public access.

The roles of the three credit reporting agencies also came under scrutiny as they historically made tens of millions of dollars annually by selling "credit headers." This information, customarily listed at the top of a credit report, included the names, aliases, birthdate, SSN, and current and previous addresses of an account holder. In response to Congressional bills introduced in the 1990s to limit the information sold in credit headers or to prohibit the practice altogether, the credit reporting agencies testified that the availability of instant credit (made possible by the sale of PII to retailers and other businesses) helped to fuel the economy. They also testified that limitations on the sale of the PII contained in credit headers could actually make verification of account holder information more difficult.

Other State and Federal Actions

By 1995, the U.S. Postal Inspection Service began tracking financial fraud through online means, a logical extension of their focus on identity theft through the physical theft of mail and the unauthorized diversion of mail. In 1996, the U.S. Secret Service began tracking fraudulent credit investigations that resulted in the issuance of unauthorized credit cards. In 1997, the Federal Bureau of Investigation (FBI) issued testimony warning Congress of the ease with which identity theft could be conducted due to technological advances. In 1998, the Secret Service warned Congress that effective encryption of sensitive data was needed due to the increasing reliance on the Internet for the transfer of financial data.

States began enacting legislation to make it a crime to possess and/or use payment device numbers (PDNs) and/or PII to obtain a benefit or something of value, that is, what has generically come to be known as identity theft or identity fraud. Arizona enacted such legislation in 1996 and California followed with similar legislation in 1997. From 1998 to 2002, many states, including Maryland, enacted legislation making identity theft or identity fraud a crime. In 1998, the federal government enacted the Identity Theft and Assumption Deterrence Act (ITADA), which made identity theft a crime that could be prosecuted separately under federal law. (The offenses and penalties established under ITADA are summarized in

Appendix 1.) This law also required the Federal Trade Commission (FTC) to establish the Identity Theft Data Clearinghouse to collect information about identity theft events from individuals across the nation who believed they were victims.

Maryland Actions

Identity fraud became a crime in Maryland in 1999 by enactment of SB 244/HB 334 of 1999, which became Chs. 331 and 332 of 1999. (The offenses and penalties established under Maryland's identity fraud statute are summarized in Appendix 2.) Maryland created its own "Task Force to Study Identity Theft" in 2005. The task force was required to take a comprehensive look at the impact of identity theft, the roles of state and local governments with regard to data security and what steps could be taken to limit the crime. Among other recommendations, the Task Force recommended legislation, which was enacted, to expand Maryland's identity fraud law to cover the unlawful use of skimmers and reencoders, to increase the maximum imprisonment for felony identity fraud, and to expand the crime of unauthorized use of a computer database to include copying.

The efforts to deter and prevent identity theft were not limited to the creation of new crimes. States and the federal government moved to disconnect SSNs, (long the de facto national identifier for official documents) from documents such as driver's licenses, library cards, student identification cards, health insurance cards, bank account numbers, retail accounts, and other documents (Maryland's law was enacted as Ch. 388 of 2000). Maryland and other states enacted legislation to prohibit the unauthorized publication and dissemination of SSNs (Ch. 521 of 2005 and Ch. 458 of 2006). In the mid-2000s, states also began enacting legislation requiring private businesses and governments to notify individual account or record holders of data breaches involving their financial accounts or personal information. Maryland enacted a security breach law in 2007 (Chs. 531 and 532 of 2007) which imposes a duty on businesses to use reasonable precautions to protect the PII of Maryland residents and to notify Maryland residents in the event that a security breach occurs. (As of July 1, 2014, the notification requirement applies to Executive Branch State agencies and local governments by enactment of Ch. 304 of 2013).

In 2007, Maryland also joined other states in enacting credit freeze legislation (Chs. 307 and 308 of 2007). For a nominal fee, the law authorizes an account holder to impose a credit "freeze" upon the release of information maintained by the three national credit reporting agencies to prevent identity fraud resulting from the unauthorized issuance of new credit lines in the name of the account holder.

Furthermore, Maryland is one of the first states in the country to establish authorization to implement a credit freeze on behalf of a protected individual, namely, a child or other vulnerable individual. Ch. 208 of 2012 was enacted to provide some measure of protection against the growing scourge of the use of SSNs of living or deceased children and other vulnerable individuals for purposes of identity theft. In 2013, Ch. 330 was enacted to require the

Department of Human Resources to request a security freeze from the national consumer reporting agencies for the consumer record of each child placed in foster care. The law takes effect October 1, 2013.

Maryland's Identity Fraud Law

Section 8-301 of the Criminal Law Article is the identity fraud criminal statute for Maryland. The law establishes misdemeanor (less than $1,000) and felony ($1,000 or more) offenses. As of October 1, 2013, a misdemeanor is punishable by maximum penalties of imprisonment for 18 months and/or a fine of $500. A felony is punishable by maximum penalties of imprisonment that range from 10 years to 25 years and/or a fine that ranges from $10,000 to $25,000. A sentence may be imposed separate from and consecutive to, or concurrent with a sentence for a crime based on underlying acts. Other major components of the law include:

- Broad definition of "personal identifying information." The term includes not only a name, date of birth, SSN, or driver's license number, it also includes the mother's maiden name, place of employment, and an employee identification number, among other numbers. As of October 1, 2013, the definition is expanded to include fingerprints and other biometric data, as well as health information and records;

- Prohibiting a person from knowingly, willfully, and with fraudulent intent, possessing, obtaining or helping another to obtain another individual's PII without the consent of that individual for the purpose of using, selling, or transferring the information to get a benefit, credit, good, service or other thing of value. A person may not knowingly and willfully assume the identity of another to avoid identification, apprehension, or prosecution for a crime or with fraudulent intent to get a benefit, credit, service, or other thing of value or to avoid payment of debts and other legal obligations. "Pretexting" is also prohibited, that is, knowingly and willfully claiming to represent another person without that person's knowledge or consent, for the purpose of soliciting, requesting or otherwise inducing another person to divulge PII or a payment device number (PDN);

- No statute of limitations for the misdemeanor offenses. As a result, perpetrators can be arrested and prosecuted at any time after the commission of the offense. Under State law, felony offenses generally do not have a statute of limitations;

- In addition to the use of PII, prohibiting the knowing and willful possession and/or use of skimmers and reencoders with fraudulent intent, for the unauthorized use, sale or transfer of PII or a PDN;

- Making the intent to manufacture, distribute, or dispense PII a felony. A violation committed pursuant to a scheme or continuing course of conduct may be considered as one offense. The value of goods and services may be aggregated to determine whether the violation is a misdemeanor or felony; and

- The investigation of identity fraud offenses without regard to State or local jurisdictional boundaries, subject to notification requirements and oversight by the Maryland State Police. Accordingly, law enforcement officers may investigate an identity fraud crime if the complaining witness resides in Maryland or if an act related to the crime occurred in Maryland.

Other Laws

Along with the comprehensive approach to Maryland's identity fraud law, other criminal offenses are relevant to identity theft. Depending on the circumstances, prosecutors may charge a number of different offenses in an identity theft situation. Charges such as theft, counterfeiting, misrepresentation, unauthorized access and/or copying of computer databases, and receiving property stolen by credit card or PDN are just some of the offenses with elements related to those required to prove the crime of identity fraud.

Identity Theft – The Changing Landscape

As noted earlier, in one form or another, confiscation and misuse of PII has long been an element of financial crimes. The striking difference between misuse of PII ten or twenty years ago (for example) and in 2013 is the speed with which information can be found and then altered to serve a criminal purpose. An identity thief who starts out with one victim can, with the press of a button, escalate his or her crime to include many more people. Another significant element, of course, is the reduced need to confront the victim.

Less Privacy and More Technology – A Perfect Storm for Identity Theft

Technological advances have reduced people's expectations for privacy. Email is supposed to be private; however, email sent on an unsecured or inadequately secured network can be captured with the right technology and read by someone looking to harvest data. What should be a perfectly safe activity, like sending an electronic greeting card to a friend or passing along a funny email with a photo or video attachment, is now synonymous with the danger of inviting computer viruses, trojans, worms, and keystroke loggers, which, in turn, help to facilitate identity theft. The same applies to instant or text messages. It is convenient and has become customary for many people to record their thoughts and feelings and pictures of life events on the Internet. Hundreds of millions of people engage in micro-blogging through the "Twitter" network, a system that allows users to leave their thoughts, (limited to 140 characters, known as "tweets"). Twitter and other applications like "Foursquare" are used to "check in," (in other words, specify a person's location) at various places.

Having all this information on the Internet does not matter a great deal unless it can be found. Advances in search technology, however, have made finding all this information relatively easy. Google, Inc. is known for pioneering data-driven and comprehensive search

results – so much so that it is common to hear people discussing the need to "google" someone. People do "google," too. They google potential employers and employees, family members, dates, spouses, business partners, and more often than not, they find all kinds of personal information. The more recent innovations in search focus on making it even more "personal." That means search results are tied to specific locations and activities – the more specific, potentially, the more profitable.

"Sharing" used to be something you did with family and a few close friends, not a euphemism for a presence on the world stage. The advent of social networks has made "sharing" an activity that is done on the Internet – potentially making personal information available to thousands or millions of people all over the world. As Google is the icon for search, the application "Facebook" has become the icon for Internet sharing, with over one billion members worldwide. There are other Internet-based networks (examples include LinkedIn, Classmates.com, and Google+) that encourage people to provide and share information, but Facebook is, by far, the most well-known and used. It is such a ubiquitous presence that it has become customary for prospective employers to request access to the Facebook pages of people before hiring them. The more people use these types of programs to "check in," the more information becomes available. For example, an investigative report about identity theft on the television show "*Dateline*" documented how a reporter was able to pick a random person from a Facebook profile. Using only the information that this person divulged about herself in the application, the reporter was able to track this person down and find her at work. The person who was found was surprised at how innocuous information about her habits could be analyzed to determine exactly who she was and where she would be at a given time.

So many entities – government, retailers, service providers, etc. make it their business to collect and maintain information about the people with whom they come into contact. Completing business transactions at a store or online often means agreeing to the storage and the sale of personal information within a corporate network and, perhaps, extending that authorization to "trusted" business partners (whoever they may be) unless the person makes the effort to specifically request "not" to be included in such dissemination. As a result, people are dependent on the custodians of all this information to maintain it, disseminate it and dispose of it in a socially responsible manner. If the people who help run the governments, corporations, social networks, and others who are the custodians of these large databases do not maintain the data they keep in a secure manner, or disseminate or dispose of it carelessly or, worse yet, in a criminal manner, then the people whose information is captured by these databases become at risk for identity theft.

Even those people who studiously avoid an Internet presence and ownership of computers, who would never purchase anything through electronic means or join any type of online social network, may still be at risk. At some point, the transactions that even these people engage in are maintained on a database somewhere. The people who personally go to the bank to deposit their paychecks are still dependent on the security of the bank's database to keep their information safe. It is difficult to get through shopping these days without being asked – at least once – for a zip code or an email address – even if the shopper is paying in cash. It is easier and

far more convenient to submit to the tracking and data collection that occurs more and more as a cost of completing basic retail transactions. While those who are in charge of the numerous databases that collect information must constantly watch for incursions and attempts to steal that information, the thieves have only to pick the one right target at the right time to potentially find data on hundreds, thousands, even millions of people.

In the early days of the Internet, and when awareness of the problems created by identity theft was just becoming known, it was far more likely that a thief could be traced directly to a personal interaction that the victim and the thief had at some point. Maybe the person submitted a mortgage application and the "helpful" administrative assistant decided to copy the SSN from the application and apply for credit in that person's name. Maybe the identity thief was a family member who "borrowed" the victim's good name and credit to buy some presents to celebrate an anniversary or birthday. These types of victimizations certainly still occur. In fact, they represent a large share of what local police and State's Attorneys (in the five jurisdictions discussed in this report) address in typical identity theft scenarios. However, they also come across thieves who create complex schemes to harvest large amounts of data by increasingly sophisticated means under a more opaque veneer of anonymity. Today's identity thief may be a face in a country thousands of miles away, or the face next door.

Some Recent Identity Theft and Fraud Schemes

Over the last decade, several identity theft schemes have developed and been executed by identity thieves. These schemes, unlike the more traditional schemes of the 20th century, involve an increased use of technology and often resemble the structure of organized crime rings. Each scheme has presented a unique challenge to the investigating law enforcement officers, requiring officers to communicate with other jurisdictions to discover the cross-jurisdictional, ongoing patterns of criminal behavior. Interviews with the five jurisdictions revealed some common identity theft schemes. For example: (1) buying gift cards with stolen credit cards; (2) felony lane gangs; (3) fraudulent home equity lines of credit; (4) homeless persons used to set up new bank accounts; and (5) work from home involving reshipping packages.

Buying Gift Cards with Stolen Credit Cards Scheme

Although the scheme of buying gift cards with stolen credit cards may seem to lack complexity, the scheme has presented a variety of challenges for identity theft investigation and prosecution. This scheme involves an identity thief using a stolen credit card to purchase gift cards at grocery stores, discount stores, retail pharmacies, or specialty retail stores. Because the identity thief does not have to present identification at many of these establishments, the thief may purchase several high-dollar gift cards on the stolen credit card. Once the gift cards are purchased, identifying and apprehending the identity thief becomes extremely difficult for two reasons. First, retailers do not trace or keep records of gift card numbers or gift card purchases. This means that once a gift card has been purchased, there is no way for law enforcement to identify who subsequently uses the gift card or where the gift is used. Second, gift cards have a

full dollar value that many times does not expire. As a result, gift cards are easy to sell and transfer between several different people. The lack of recordkeeping regarding gift cards coupled with the value of gift cards makes participants in this scheme extremely difficult to prosecute. It also makes this scheme likely to become a part of a larger ring of organized crime that may involve the mass purchase of stolen credit cards.

Felony Lane Gang Scheme

The felony lane gang scheme received its name because participants in the scheme use the outer-most, drive-thru lane of a bank when assuming a victim's identity and withdrawing money. The core of the scheme revolves around a thief stealing an individual's checkbook, typically from a car or a purse that is located at a gym, park, church, or community center. After stealing the checkbook, the thief then arranges for an individual, often a prostitute or homeless person, to pose as the victim and withdraw funds from the victim's bank account. The fraudulent bank withdrawal typically succeeds because of the inability of the bank teller to see the face of the individual attempting to withdraw money and the individual's use of wigs and other disguises. Even following the initial bank transaction, a victim remains at risk because the thief will often try to open up other bank accounts and lines of credit using the victim's identification. Known by many law enforcement agencies as "mules" or "runners," the individuals who pose as the victims often do not know the chief organizers of the felony lane gang scheme. The use of disguises by scheme participants and their lack of knowledge of the entire scheme have hindered law enforcement's ability to apprehend organizers of the felony lane gang scheme.

Fraudulent Home Equity Lines of Credit Scheme

Another identity theft scheme that has emerged over the last decade involves home equity lines of credit. This scheme is similar to the buying gift cards with stolen credit cards scheme because the identity thief relies on the lack of identification needed to take over the victim's finances. Specifically, the identity thief knows that many home equity lines of credit may be opened up online. The identity thief begins by obtaining an individual's basic information by buying it on the Internet or finding some of the information in public records. After the thief has some of the pertinent information of the victim, such as the victim's address, date of birth, telephone number, and home address, the thief will obtain the rest of the information needed to open up a home equity line of credit by (1) locating the information on the Internet or (2) pretending to be a utility company, bank, or other institution and soliciting the victim for the missing information. Once the identity thief has obtained all of the necessary information, including the equity of the victim's home, the thief then opens up a line of credit in person, or online (more likely). The thief is then able to access the funds by requesting a wire transfer of funds to the thief's account or withdrawing the funds at a bank. Victims of this identity theft scheme are at risk of losing tens of thousands of dollars and significant equity in their homes.

Homeless Persons and New Bank Accounts Scheme

Identity thieves have targeted many vulnerable populations to assist in their schemes, including homeless individuals. Organizers of the homeless individuals and new bank accounts scheme send scouts out to locations where homeless people may gather, such as churches, soup kitchens, or parks. The scouts then convince them to open up new bank accounts in exchange for a small fixed amount of money, such as $25. After a homeless person agrees to participate, the scout transports the person to the bank to open up a bank account. After the person has opened up the bank account, using his or her identity or the identity of someone else, the scout collects the new account information and pays the person in cash. Unbeknownst to the person, the scout then gives the account information to the organizer of the scheme. The organizer of the scheme uses the accounts to deposit fraudulent checks and withdraw the money before the checks are flagged by the bank. Because of the number of different people involved in the scheme, investigating and prosecuting the organizers of homeless individuals and new bank account schemes has been difficult.

Reshipping Work from Home Scheme

In this work from home identity theft scheme, people respond to an online job posting that indicates a person may work from home and receive income. A person, unaware that the advertisement is to entice people to participate in an identity theft scheme, responds to the posting. Organizers of the identity theft scheme then tell the person that he or she only needs to receive packages at home and reship the packages to new addresses by using new labels. Frequently, the person must reship the package overseas. Believing only that the packages need to be reshipped because of postal service difficulties, the person then begins receiving, relabeling, and shipping the packages.

The identity thieves compensate the person, as promised, and he or she continues to reship packages. The person, however, remains unaware that he or she is continuing to ship merchandise that has been purchased using stolen PII or stolen credit card information. Typically, the person does not become aware that the reshipping is a part of an identity theft scheme until a law enforcement officer contacts him or her and requests that the person immediately stop participating in the reshipping scheme. Unless the person continues reshipping packages, the person is usually not charged with an identity theft crime. People are particularly susceptible to this scheme because of the genuine appearance of the initial job posting, the ability to work from home, and the person's belief that he or she is being compensated for legitimate work. Similar unpaid reshipping schemes, which involve a person reshipping packages because of a request for help from an online friend or companion, also exist and present similar challenges for law enforcement.

Each of these schemes highlights ways that identity thieves have been able to use technology and the ability to transfer and deposit money easily to develop new organized crime schemes over the past decade. Identity thieves are able to continue executing these schemes

because the schemes often involve different people, many of whom are unaware that they are participating in organized identity theft. Understanding the complexity of identity theft schemes provides useful context when examining the resources law enforcement officials and prosecutors have and use to address identity theft.

Other Identity Theft Trends

Criminals have been extraordinarily resourceful in finding ways to harvest PII for new uses. Credit card fraud has long been the top type of identity theft complaint nationally and in Maryland, until 2011, when fraud for government benefits became the top type of complaint (See **Exhibit 5**.) Criminals are using PII, however, not just to steal money but to steal health care, prescription drugs, citizenship status, tax refunds, unemployment benefits, and even driving privileges. A relatively recent disturbing trend is the commission of identity fraud to avoid sex offender registration requirements.

Resources of Five Maryland Jurisdictions Used to Address Identity Theft

The complexity and frequency of identity theft crimes often means that investigating and prosecuting the crimes is costly – both in time and tangible resources – to the entities tasked with addressing the issue. Based on interviews with law enforcement and prosecutors from each of Maryland's five major jurisdictions, the resources available vary by jurisdiction. Overall, law enforcement personnel, although able to investigate many identity theft crimes, have limited resources that can both decrease the number of cases investigated and the effectiveness of the investigations. On the other hand, prosecutors, who also have limited resources, appear to be able to manage their caseloads more easily.

Law Enforcement Resources

Number of Detectives

As of 2012, each of the five police departments interviewed has at least two detectives assigned to investigate economic or financial crimes. Detectives assigned to each department's economic or financial crimes section must field citizen complaints, investigate allegations of identity theft or other financial crimes, collaborate with the local State's Attorney's office, and testify as witnesses in cases that go to trial. In comparison to other types of criminal investigation units, however, resources available to each of the jurisdiction's economic or financial crimes unit vary, but appear limited. In particular, the number of detectives assigned to investigate economic or financial crimes is generally fewer than the number of detectives assigned to investigate other types of crimes. Many law enforcement personnel expressed that the number of personnel assigned to investigate economic or financial crimes is a result of such investigations being a low priority for departments, especially in comparison to the investigation of violent crimes. Reasons for the low priority of economic or financial crimes varied, including

the number of other types of crimes, the types of sentences that judges issue for economic crimes, and concerns about public safety. The police departments interviewed generally agreed that an increase in the number of detectives assigned to investigate economic and financial crimes would assist units in investigating more identity theft crimes and decreasing detective caseloads. One department even noted that the number of detectives assigned to investigate economic or financial crimes could quadruple, and yet there would still be a need for additional detectives.

Lack of Administrative Support

In addition to jurisdictions having a limited number of detectives assigned to investigate identity theft crimes, as of 2012, three out of five jurisdictions (Anne Arundel County, Baltimore City, and Prince George's County) also noted that detectives assigned to investigate identity theft crimes have no paid administrative support. As a practical matter, this means that detectives must answer phones and prepare and type all correspondence and court documents, including cover letters, warrants, and police reports. Having to perform such tasks, which could be completed by paid administrative support, detracts from detectives' ability to investigate in the field or work on an investigation without interruptions. Detectives in jurisdictions lacking such administrative support stated that having a paid administrative staffer, even if only part-time, would assist in investigation of identity theft crimes.

Limited Patrol Officer and Detective Training

As noted above, many of the more recent identity theft schemes are complex, involving new technology, multiple individuals, and multiple jurisdictions. The constantly changing landscape of identity theft means that investigating techniques also need to change. Discussions with the five jurisdictions revealed that patrol officers, and even some detectives, lack training in being able to recognize identity theft tools such as reencoders and fraudulent identification cards. Ultimately, this means that patrol officers are not always able to apprehend an identity thief because they do not recognize those tools when they encounter suspects while on patrol. In addition, lack of training may hinder economic or financial crimes detectives from using investigation best practices. Multiple jurisdictions noted that limited budgets or access to funds have prevented economic or financial crimes units from being able to participate fully in investigative training or participate in organizations that provide resources for the investigation of economic or financial crimes. To overcome budget restrictions, some detectives have paid out-of-pocket to attend conferences and training events. Paying for patrol officers and detectives to attend trainings and conferences can be expensive and, therefore, not always feasible on a limited government budget.

Outdated Computer Equipment

The technology available to economic or financial crimes units varies by jurisdiction, but, as of 2012, at least one jurisdiction is using computer operating systems and equipment that are a decade old. Outdated equipment has presented such a problem for some detectives that they

have purchased their own equipment and brought it into the office. Law enforcement personnel explained the ramifications of using outdated computer equipment and technology: the inability to receive investigative documents electronically from banks and retailers, the incapacity to investigate certain types of identity theft crimes involving computers, and an overall decrease in investigation efficiency. According to one interviewee, identity theft criminals remain ahead of detectives in the area of technology, making it more difficult for law enforcement to apprehend the identity thief.

State's Attorney Resources

Interviews with the State's Attorney's offices of the five major jurisdictions' indicated that identity theft prosecutions were manageable, although additional funding to hire more personnel would be helpful. Three different factors appeared to affect the ability of State's Attorney's offices to prosecute identity theft cases using existing resources.

Origination of Identity Theft Complaints

Identity theft investigation and prosecution typically begins with local police departments, not State's Attorney's offices. Victims of identity theft, including individuals, retailers, and banking institutions, often contact their local law enforcement agency to make a complaint and provide information regarding alleged incidents. Consequently, State's Attorney's offices do not directly receive a majority of identity theft complaints, the preliminary investigation of which can be quite time consuming. The cases they receive are usually cases in which the identity thief has not only been identified, but already apprehended. This does not mean that State's Attorney's offices do not ever investigate an identity theft crime and subsequently prosecute it. Rather, it means that State's Attorney's offices handle a low volume of initial complaints which helps to make their caseloads more manageable.

Prosecutorial Discretion

After local prosecutors receive cases from law enforcement or investigate a case from a victim, they may choose whether or not to move forward with the case. At least one jurisdiction noted that it does not prosecute cases below a certain dollar threshold. Other jurisdictions assess whether the prosecutor will have enough evidence to be able to prove that a suspect actually committed an identity theft crime before moving forward with prosecution. This prosecutorial discretion, although not always done with the intent to reduce caseloads, allows for State's Attorney's offices to maintain a manageable caseload based on their available resources.

Jurisdictional Issues

Not only do State's Attorney's offices have prosecutorial discretion, but they also have jurisdictional issues that may decrease their caseloads. Two different situations arise regarding jurisdiction that may avert the prosecution of an identity theft case. First, a prosecutor may have an identity theft case that involves a defendant who committed a series of identity theft crimes

throughout the State. Each local State's Attorney's office may initiate prosecution of the defendant because the victim resided in the prosecutor's jurisdiction. Strategically, however, State's Attorneys of different jurisdictions collaborate with each other to get a defendant to plead guilty. Once a defendant pleads guilty in one jurisdiction, the State's Attorney of another jurisdiction frequently does not need to move forward with prosecution.

The second situation regarding jurisdiction occurs when there are multiple defendants who reside in different states or one defendant who committed a crime in several states. When this situation occurs, local prosecutors are often unable to move forward with the prosecution unless the United States Attorney's Office assists with the case. There is little incentive for an individual local prosecutor in this situation to keep the case active without such assistance. These jurisdictional issues, although not under the control of local prosecutors, can result in a decreased caseload and therefore allow local prosecutors to address identity theft cases with existing resources.

Relationships and Communications: An Important Advantage

Despite the limited human and technological resources available to local police departments and prosecutors, local police departments and prosecutors have managed to apprehend numerous identity thieves. Meetings with area work groups, the five jurisdictions' law enforcement officers and prosecutors, and other interested entities such as the Office of Attorney General revealed the magnitude of cross-departmental, cross-jurisdictional relationships. Each of the interested parties in identity theft investigation and prosecution – banks, retailers, prosecutors, and law enforcement – collaborate with each other on a weekly basis to exchange information to identify and apprehend identity thieves and prevent further losses. Such collaboration allows the entities to pool resources together, share best practices, and address organized identity theft rings that span multiple jurisdictions.

Exhibit 1 lists the role of different entities involved in the investigation and prosecution of identity theft in Maryland. It is a non-exhaustive list intended to exemplify how law enforcement relationships in the identity theft area expand far beyond the standard relationship between a local police department and local State's Attorney's office.

Exhibit 1
Entities Involved in Identity Theft Investigation and Prosecution

Entity	Role
Bank Security Officers	• Contact law enforcement about potential cases • Maintain "evidence," including surveillance footage • Notify other banks about possible suspicious behavior or identity theft patterns or schemes
Federal Bureau of Investigation	• Investigates cyber crimes, including identity theft • Investigates white collar crimes
Federal Trade Commission	• Receives complaints of identity theft • Collects and maintains statistics regarding identity theft crimes • Provides resources for consumer and businesses on how to prevent identity theft and take action if it has occurred • Provides resources for law enforcement regarding identity theft investigations
Immigrations and Customs Enforcement - Homeland Security Investigations	• Investigates financial crimes, including identity theft • Collects, analyzes, and shares strategic and tactical data to assist in investigations
Internal Revenue Service	• Investigates identity theft crimes involving employment or tax returns
Local Police Departments	• Field complaints from citizens and write police reports • Investigate identity theft to forward case to a State's Attorney's Office or the United States Attorneys' Office • Assist in federal investigations (e.g. execute a search warrant)
Local State's Attorney's Offices	• Investigate economic crimes • Charge suspects with identity theft, credit card fraud, theft, etc. • Attempt to get a guilty plea or conviction • Make sentencing recommendations
Maryland State Police	• Investigates computer crimes, which include a few identity theft crimes each year • Advises victims on how to protect identity and directs them to resources

Entity	**Role**
Motor Vehicle Administration	• Provides case support for all law enforcement agencies • Investigates suspected incidences of identity theft or false documentation regarding driver's licenses and identification cards
Office of Attorney General	• Helps victims address their problems by directing them to resources or issuing an identity theft passport (that is, a document that certifies the bearer was an identity theft victim, to facilitate reconstruction of financial records)
Office of Inspector General	• Investigates alleged violations of fraud or criminal and civil laws by federal departments and their employees
Retailers	• Employ loss prevention officers who are trained to observe, identify, and prevent thefts • Contact law enforcement about potential cases
Social Security Administration	• Issues SSNs • Investigates the misuse of SSNs
United States Attorney's Offices	• Investigate economic crimes • Charge suspects with violations of federal law relating to identity theft • Attempt to get a guilty plea or conviction • Make sentencing recommendations
U. S. Marshals Service	• Manages and sells assets of identity theft seized and forfeited by federal law enforcement agencies nationwide
United States Postal Inspection Service	• Investigates postal offenses and civil matters relating to the Postal Service, including the investigation of the unlawful confiscation and diversion of the U.S. mail
United States Secret Service	• Investigates identity crimes such as access device fraud, identity theft, false identification fraud, bank fraud, check fraud and related crimes like counterfeiting, to safeguard the nation's financial infrastructure and payment systems

Source: Department of Legislative Services

Informal and Formal Interactions

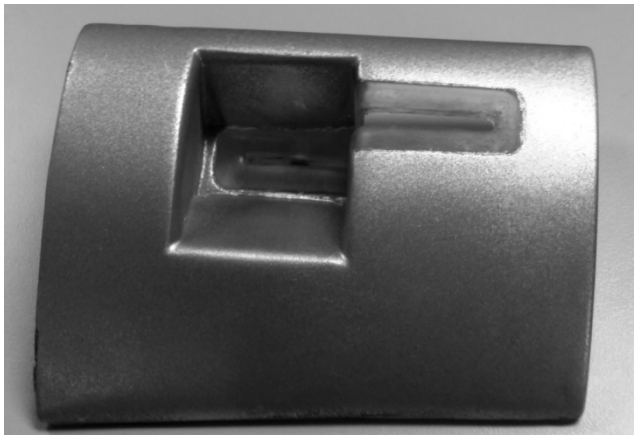
Across the State, those involved in the prevention of crimes relating to identity theft have formed numerous informal and formal groups. The participants of these groups vary. Some

groups, such as the Maryland Association of Bank Security (MABS) primarily include investigators employed by financial institutions, while other groups, such as the Baltimore City Economic Crimes Working Group, include federal and local prosecutors as well as representatives from law enforcement, retailers, and banking institutions. Regardless of the membership of each of these groups, they each focus on two things: identifying ongoing patterns of criminal behavior and sharing resources to identify, stop and prevent those ongoing patterns of criminal behavior.

What it means to "share resources" changes depending on the situation. For example, federal law enforcement agents do not have the authority to make certain misdemeanor arrests or execute State search warrants. Because of federal agents' limited authority in the State, they must rely on the relationships that they have built with local law enforcement agencies, many of which have been formed during these informal and formal interactions. Similarly, local police departments must also rely on federal law enforcement agencies to investigate their more complex, organized identity theft crimes. At least two of the police departments interviewed have an officer who is deputized as a federal agent and serves on a federal task force. Authorizing local police officers to become deputized allows local law police departments to understand and participate in the structure in which federal agencies tackle identity theft and related crimes. It also allows the local police departments to have a close relationship with an officer who has federal authority. Through the relationships formed at work group meetings, trainings, and task forces, federal or local law enforcement agencies may receive assistance identifying an identity theft suspect or gaining access to key information, such as security video footage.

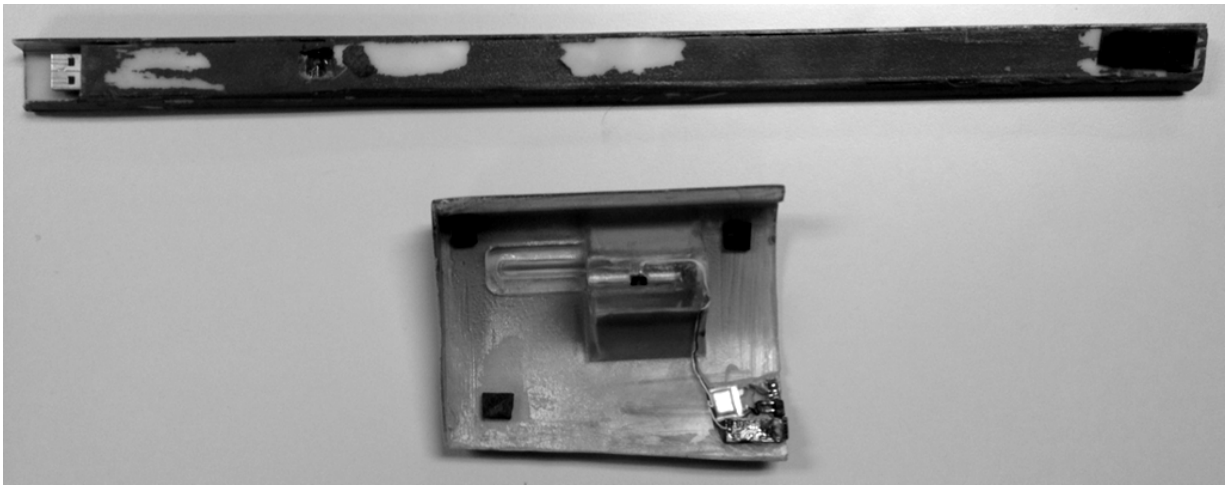
Another example of sharing resources involves intelligence or knowledge regarding a specific scheme or pattern of criminal behavior. During the November 2012 meeting of the Identity Theft Work Group for the District of Maryland, coordinated by the United States Attorney's Office for the District of Maryland, representatives from PNC Bank brought an actual skimmer and pen camera that a branch had removed from one of its automated teller machines in Maryland. Before passing the skimmer and pen camera around to meeting attendees, PNC representatives explained how they were able to remove the device before any credit card numbers were copied. In addition, they explained how they were attempting to identify the suspect who attached the skimmer to the machine. **Exhibit 2** depicts the front of the skimmer that was attached to the machine, **Exhibit 3** depicts the back of the device which contained the computer processor and data information collector and the back of the bar containing the camera, and **Exhibit 4** depicts the bar that contained the pen camera device.

Exhibit 2
Front of Skimming Device



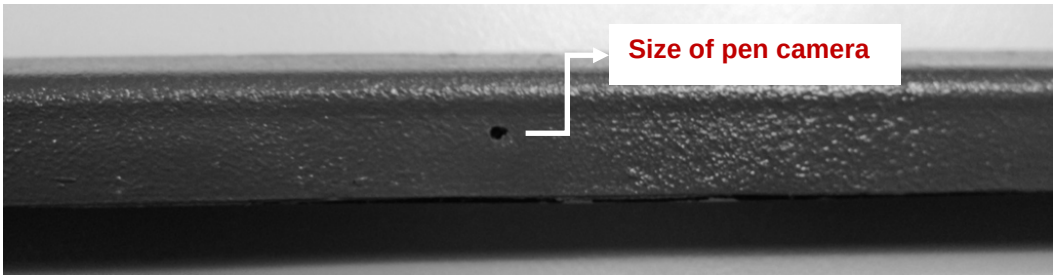
Source: PNC Bank

Exhibit 3
Back of Bar with Pen Camera and Back of Skimming Device



Source: PNC Bank

Exhibit 4
Front of Bar with Pen Camera.



Source: PNC Bank

Showing the actual skimmer to meeting attendees alerted attendees to the newest technology that identity theft suspects are using to conceal skimming devices. As a result, attendees may be able to identity such devices more easily and remove the devices from machines before customers' PII is confiscated.

Role of Financial Institutions and Retailers

Investigators for banks and retailers are often key allies of law enforcement when it comes to finding identity thieves. The identity thief who steals PDNs to acquire something of value often needs to interact (or have someone on his or her behalf to interact) with retailers to convert the stolen information into merchandise or services or interact with a financial institution to convert the stolen information into cash.

Retailers and financial institutions are also in a unique position to be victimized by identity thieves. When a consumer is victimized by identity fraud, it is unlikely that he or she will be required to absorb the cost of the fraudulent charges since checking and savings account funds are fully restored, at some point. Retailers who complete fraudulent purchases have to pay for those items handed over to thieves. Credit card issuers and financial institutions that do not intercept fraudulent transactions experience financial losses from the restoration of accounts. On the other hand, retailers and financial institutions have resources that the average consumer does not have – constant video surveillance, for example, security personnel and employees who are required to check identification and report or deny suspicious transactions. However, banks and retailers have goals that are sometimes at cross-purposes with law enforcement. These entities exist to maximize profits in the most expedient way possible – generally that means serving customers and making it as easy as possible for customers to complete transactions. If retailers and financial institutions were made absolutely secure against identity fraud, it would likely be difficult (if not impossible) to efficiently serve legitimate customers, thereby reducing the profits necessary to stay in business. Also, a favorable reputation in the marketplace, bolstered by

customer goodwill and excellent public relations, is very helpful to these entities. A key component of this goodwill is being regarded as a safe and secure placed to conduct business. As a result, retailers and financial institutions are generally loathe to publicize the successful perpetration of identity fraud on their customers.

This is not to imply that banks and financial institutions do not participate in apprehending identity thieves. They do, but the effort is dictated by the entity's policies and priorities and resources, which are not unlimited. Except for those schemes involving thousands or millions of dollars, it is often cheaper (and definitely easier) for financial institutions to make individual customers whole and for retailers to absorb the loss of merchandise than it is to divert valuable and limited resources away from sales and services. At any given time, the losses affecting financial institutions and large retailers are small in comparison to the potential for lost business and profits if too many resources are diverted to holding relatively petty thieves accountable and away from the far more lucrative business of acquiring customers, managing profits and meeting shareholder expectations. For small scale retailers and financial institutions, the question of where to put scarce resources is even more critical.

Overall, federal and State prosecutors and law enforcement officers willingly provide each other assistance, understanding that they may have a future case and need assistance from another entity. They share information with each other and encourage each other to join organizations such as the International Association of Financial Crimes Investigators (IAFCI) and the National White Collar Crime Center (NW3C). They also forward cases to each other based on jurisdictional restrictions and feasibility to apprehend the suspect. Although the agencies may not always be able assist, they attempt to direct each other in the appropriate direction. The relationships and collaborations between interested entities are not just helpful to the investigation and prosecution of identity theft crimes, but invaluable.

Pursuing Identity Thieves

A continuing theme in discussions with law enforcement personnel is that the crime of identity theft requires the investment of a great deal of work for not necessarily a great return on investment. For the last 10 years, the top consumer complaint documented by the FTC has been identity theft. Since the FTC began collecting the incidences of identity theft complaints, Maryland has been one of the states with a high frequency of identity theft complaints, Maryland has always been among the top 13 states, and, more recently, among the top 10 states. Since 2002, Maryland's rank with regard to complaints has never gone below 13th (2004) and has generally hovered between 9th and 11th. Generally, that means 4,500 to over 6,000 incidences of identity theft affecting Maryland residents are reported to the FTC every year. However, the majority of these cases do not result in the arrests of any suspect. The number of cases that do result in the arrest of a suspect and a finding of guilt or innocence is only a fraction of those self-reported complaints.

Exhibit 5 shows, over an 11-year period, the national number of identity theft complaints reported by individuals to the FTC, the number of complaints reported from Maryland, Maryland's rank among the 50 states and the District of Columbia, the number of complaints per capita, and the most reported type of identity theft crime.

Exhibit 6 shows the number of identity theft convictions from the circuit courts and the number incarcerated in Maryland for 2002 through 2011, the most recent year for which this information is available. The numbers shown do not represent all convictions and incarcerations but are limited to only those misdemeanors and felonies charged as identity fraud that are processed in the circuit courts and are tracked and disposed of under the guidelines of the Maryland State Commission on Criminal Sentencing Policy (MSCCSP).

Exhibits 7, 8, and **9** show identity fraud cases processed in the District Court for which disposition data is available. The District Court processes a majority of the identity fraud cases charged under the State identity fraud statute. The data is available for fiscal 2003 through 2012 and is separated by the specific identity fraud charge that was brought in the case before the District Court.

Exhibit 5

Identity Theft Complaints – National and Maryland

2002-2012

Year	National Complaint Totals	Top Type of ID Theft Complaint – National	Maryland Complaint Totals	Maryland Rank	Maryland Complaints Per Capita*	Top Type of ID Theft Complaint – Maryland
2002	161,977	credit card fraud	3,497	9	66.0	credit card fraud
2003	215,240	credit card fraud	4,124	11	74.9	credit card fraud
2004	246,909	credit card fraud	4,612	13	83.0	credit card fraud
2005	255,687	credit card fraud	4,848	11	86.6	credit card fraud
2006	246,214	credit card fraud	4,656	11	82.9	credit card fraud
2007	259,314	credit card fraud	4,821	10	85.8	credit card fraud
2008	314,594	credit card fraud	5,421	11	96.1	credit card fraud
2009	278,385	credit card fraud	5,232	11	91.8	credit card fraud
2010	251,105	credit card fraud	4,784	9	82.9	credit card fraud
2011	279,156	govt docs/benefits	4,980	9	86.3	govt docs/benefits
2012	369,132	govt docs/benefits	6,178	9	105.0	govt docs/benefits

Numbers revised by FTC – 2008 through 2011
Source: FTC Consumer Sentinel Network Reports 2002 through 2012
* Ranking is based on the number of complaints per 100,000 people.

Exhibit 6

Circuit Court Sentences – Identity Fraud*

2002-2011

Offense	Cases with Valid Data	% Incarcerated	*Average Sentence Length* Total Sentence	Total Sentence Less Suspended
Possess, obtain PII or willfully assume the identity of another for benefit less than $500	43	51.2% (N=22)	13.5 months	7.8 months
Possess, obtain PII or willfully assume the identity of another for benefit for $500 or more	129	61.2% (N=79)	55.0 months	19.5 months
Intent to manufacture, distribute or dispense PII	20	55% (N=11)	37.6 months	17.6 months
Use of re-encoder or skimmer – benefit less than $500	0			
Use of re-encoder or skimmer – benefit $500 or more	0			
Falsely represent to induce disclosure of PII (pretexting)	0			

*Pertains only to cases for which filing and disposition information was available. Other cases with theft or similar charges may have been processed in the circuit court that are not reflected in the exhibit.

Source: Maryland State Commission on Criminal Sentencing Policy

Exhibit 7

Unauthorized Use/Possession of PII With Fraudulent Intent to Obtain Benefit/Value

Criminal Law § 8-301(b)
Fiscal 2003-2012

Offense	**2003**	**2004**	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**Total**
Dismissal	2	4	0	1	2	0	0	1	4	2	**17**
Not Guilty or Judgment by Acquittal	2	3	1	0	1	6	1	4	7	5	**30**
Nolle Prosequi	46	88	67	69	66	103	73	112	204	233	**1,061**
Stet	14	26	14	23	20	30	23	34	48	79	**311**
Probation Before Judgment	0	6	8	5	2	4	1	2	3	2	**33**
Guilty	8	19	16	20	15	5	10	17	21	12	**143**
Other	0	1	0	0	1	1	0	0	0	2	**5**
Total Dispositions	**72**	**147**	**106**	**118**	**107**	**149**	**108**	**170**	**287**	**336**	**1,600**

Source: District Court

Exhibit 8
Assume Identity of Another to Avoid Prosecution
Criminal Law § 8-301(c)(1)
Fiscal 2003-2012

	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	Totals
Offense											
Dismissal	2	0	1	1	0	2	6	4	0	3	**19**
Not Guilty or Judgment by Acquittal	0	1	2	3	2	4	6	3	1	3	**25**
Nolle Prosequi	16	76	95	88	79	112	155	181	192	196	**1,190**
Stet	1	27	21	28	51	42	28	44	52	60	**354**
Probation Before Judgment	1	3	7	1	6	9	5	10	8	11	**61**
Guilty	7	46	63	42	36	34	52	77	74	81	**512**
Other	0	0	1	1	3	0	1	0	0	2	**8**
Total Dispositions	**27**	**153**	**190**	**164**	**177**	**203**	**253**	**319**	**327**	**356**	**2,169**

Source: District Court

Exhibit 9

Assume Identity of Another to Obtain Benefit/Avoid Debt

Criminal Law § 8-301(c)(2)
Fiscal 2003-2012

Offense	**2003**	**2004**	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**Totals**
Dismissal	4	2	1	0	2	3	1	2	2	4	**21**
Not Guilty or Judgment by Acquittal	5	1	2	1	3	6	2	8	10	4	**42**
Nolle Prosequi	39	35	110	99	114	150	127	196	288	265	**1,423**
Stet	11	22	41	33	37	41	78	78	98	104	**543**
Probation Before Judgment	2	1	3	4	2	5	3	5	2	4	**31**
Guilty	10	8	16	18	18	25	23	20	33	20	**191**
Other	0	1	2	2	3	0	1	1	3	2	**15**
Total Dispositions	**71**	**70**	**175**	**157**	**179**	**230**	**235**	**310**	**436**	**403**	**2,266**

Source: District Court

In Exhibits 7, 8, and 9, the term "*nolle prosequi*" indicates cases in which the State's Attorney declined to prosecute the defendant. The State may reinstate the charges at a later date. This disposition may be used if the State's Attorney believes that the evidence is insufficient to continue with the case or because additional evidence may be presented at a later time that may result in other charges or a plea bargain. The State's Attorney may also use the *nolle prosequi* charge as leverage if the defendant has useful information or can provide sworn testimony in a case. The term "*stet*" indicates a docket of cases that are stayed or held in abeyance. A case may be "stetted" for an indefinite or specific period of time. A case may be referred to the *stet* docket if the court determines that while there may be insufficient evidence to issue a verdict, a defendant without a prior criminal record may get the benefit of a *stet*, which means that he she will not have a criminal record as a result of that case. Accordingly, a judge may "stet" the case and tell the defendant that if he or she is brought before the court on the same or a similar charge, the original charge and case will also be reinstated and subject to trial.

For the identity fraud charges shown in Exhibits 7 through 9, the majority of dispositions is either *nolle prosequi* or *stet.* Relatively few cases are dismissed outright or disposed of with a verdict of guilty or not guilty. Over the ten year period shown in Exhibit 7 in which the disposition of 1,600 cases is documented, only 16 cases (or 1 percent) were dismissed outright, according to records kept by the District Court. Only 30 cases (or 1.8%) received a verdict of not guilty or judgment by acquittal and 33 cases (or 2%) were disposed of by Probation Before Judgment (PBJ). On the other hand, 1,061 cases (or 66.3%) were disposed of by *nolle prosequi* and 311 cases (or 19.4%) were stetted. Accordingly, 85.8% of cases with the charge of use or possession of PII with fraudulent intent to obtain a benefit or thing of value were either designated *nolle prosequi* or stetted. Over the same ten year period, 143 cases (or 8.9%) were disposed of with a guilty verdict.

Similar findings are reflected in Exhibit 8, which addresses cases with the charge of assuming the identity of another to avoid prosecution. Of the 2,169 District Court cases for which data is available over the ten year period, 1,190 (or 54.9%) were disposed of by *nolle prosequi* and 354 (or 16.3%) were stetted. This reflects a total of 71.2% of cases with that charge that were handled in the District Court. Only a total of 61 cases (or 2.8%) were disposed of by PBJ and only 25 cases (or 1.2%) were disposed of with a verdict of not guilty or judgment by acquittal during the same period. Those cases dismissed outright were only 19 (or less than 1%) of all cases over the same period. On the other hand, there were 512 guilty dispositions, reflecting a total of 23.6% of all dispositions for that charge over the ten year period.

Over the ten years reflected in Exhibits 7 through 9, the largest number of cases (2,266) dealt with the charge of assuming the identity of another to either obtain a benefit or avoid the payment of a debt, as shown in Exhibit 9. Of those cases, most were disposed of by *nolle prosequi* (1,423) or they were stetted (523) for a total of 86.7% of cases subject to either of these dispositions. Over the same ten year period, only 42 cases (or 1.9%) were disposed of with a not guilty or judgment by acquittal verdict and only 21 (or less than 1%) were dismissed outright. A total of 31 cases (or 1.3%) were disposed of by PBJ and 191 cases (or 8.4%) were disposed of with a guilty verdict.

The District Court also disposed of cases involving the charges of (1) unauthorized use of a reencoder (§ 8-301(d)(1) of the Criminal Law Article); (2) unauthorized use of a skimmer (§ 8-301(d)(2) of the Criminal Law Article); (3) unauthorized possession of a reencoder or skimmer (§ 8-301(e) of the Criminal Law Article); and (4) false representation to induce disclosure of PII or "pretexting" (§ 8-301(f) of the Criminal Law Article). The offense of pretexting was not established until 2007, through enactment of Ch. 447 of 2007. From fiscal 2008 through 2012, 18 cases with the pretexting charge were processed by the District Court. Over that five-year period, 12 of the 18 cases had a disposition of *nolle prosequi* and 4 cases were placed on the *stet* docket. One case had a finding of guilty and the remaining case had a PBJ disposition.

The offenses of the unauthorized use or unauthorized possession of reencoders or skimmers were not established until October 1, 2008, as a result of enactment of Chs. 354 and 355 of 2008. For the charges of (1) unauthorized use of a reencoder; or (2) unauthorized use of a skimmer, a total of 8 cases were processed by the District Court from fiscal 2009 through 2012. All cases were designated *nolle prosequi*. Six cases for the unauthorized possession of a reencoder or skimmer were processed by the District Court during the same period. In fiscal 2010, there was a verdict of guilty in one case and one case had a PBJ disposition. Three of the six cases were designated *nolle prosequi* during the period and one case in fiscal 2012 was placed on the *stet* docket.

It should be noted that all five police departments and State's Attorney's offices mentioned that a significant number of criminal offenses that could be charged as identity fraud are often charged as other criminal offenses. The reasons for this are varied. It may be easier to charge an offense such as theft or counterfeiting. It may be easier to leverage a guilty plea from a suspect with a different charge, or it may be easier to round up witnesses with a different charge. The number of cases that could be charged as identity fraud, but are not, is unknown. Also, prosecutors noted that most cases – perhaps as many as 90%, are disposed of by plea bargain and may not necessarily be reflected in Exhibit 6 or Exhibits 7 through 9. Nevertheless, the gap between the number of complaints reported from Maryland and the number of convictions tracked by the MSCCSP in the circuit court and the number of dispositions in the District Court is illustrative. For example, from 2002 to 2011, a total of 46,975 identity theft complaints in Maryland were forwarded to FTC. In that same period in the circuit courts, 43 misdemeanor identity fraud convictions meeting State sentencing guidelines were documented, 129 felony identity theft convictions and 20 convictions for intent to manufacture, distribute or dispense PII, including single and multiple counts. The number reported incarcerated statewide as a result of the convictions meeting sentencing guidelines for misdemeanor identity fraud was 22; the number incarcerated for felony identity fraud was 79; and the number incarcerated for intent to manufacture, distribute or dispense PII over the last 10 years was 20. For that same period in the District Court, the available data indicate there is less than a 20 percent chance that a verdict of guilty or not guilty will be rendered in an identity fraud case. Instead, it is far more likely that the case will be designated *nolle prosequi* or placed on the *stet* docket.

What Exhibits 5 through 9 tend to validate are what members of the law enforcement community confirmed anecdotally – that most people who commit identity fraud are not identified, let alone arrested and charged. If a suspect is identified, law enforcement and prosecutors still face a significant array of obstacles in successfully charging a suspect so that he or she can be bound over for trial and a verdict rendered.

Challenges with Apprehending Identity Thieves

Elusive Victims and Witnesses

It is sometimes difficult to persuade the individual whose account was compromised to testify at a criminal trial. Credit card issuers routinely remove unauthorized charges from compromised accounts, close compromised accounts, and open new ones. The federal Fair Credit Billing Act limits the amount that an individual credit card account holder is required to pay to $50 per card. Most credit card issuers, however, routinely restore credit from fraudulent activity without requiring the account holder to pay any portion of the amount stolen. For checking and savings accounts that are compromised, especially those involving a debit card, the federal Electronic Funds Transfer Act does not require the same level of protection that is accorded to unauthorized credit card charges. Generally, only losses reported within two business days after discovery are limited to $50. However, it has become customary for banks and other financial institutions to credit compromised savings and checking accounts for losses due to identity fraud without making the account holder pay any portion of the charge, if the loss is reported within a reasonable amount of time. If an individual files an affidavit affirming that the account was compromised and submits a police report (or even a police report case number) to the financial institution, the financial institution is likely to restore the stolen funds.

Once the stolen funds are restored to the individual victim's account, that person is likely to be reluctant to take more time to testify against a suspected identity thief – especially since the restoration of funds does not mean the victim still does not have to spend significant time and even money to repair and secure personal and financial records. Generally, the individual just wants his or her credit restored or the money returned, and his or her financial standing restored. By the time a trial date is set, the victim may have already spent a lot of time straightening out financial records and is understandably reluctant to spend even more time to testify at trial.

Even if an individual victim is motivated to testify against a suspect, he or she is likely to become quickly discouraged by the routine delays in the judicial process. A number of law enforcement personnel cite the almost routine request for a continuance, once a case is scheduled for a hearing. The first request for a continuance is likely to be granted. If the case is charged as a misdemeanor and is scheduled for hearing before a District Court judge, further delays may result from prayers for jury trial. (A defendant is entitled to a jury trial upon request if the crime with which he or she is charged has a penalty of at least 90 days imprisonment). Once a jury trial prayer is granted, the case has to be added to the trial docket of the circuit court, resulting in additional delays. If a case is originally presented in the circuit court and an initial continuance

request is granted, crowded trial dockets could mean a delay of months before the case can be heard.

When the Maryland Task Force to Study Identity Theft was convening in 2007, almost all law enforcement and prosecution representatives who testified encouraged the task force to recommend that identity fraud be added to the list of offenses for which an affidavit, sworn to by a lawful credit cardholder, may be introduced as evidence that the credit card or its number was taken, used or possessed without authorization. Pursuant to a task force recommendation, the law was amended to add identity fraud to the other criminal offenses for which these affidavits are authorized (See § 8-214.1 of the Criminal Law Article). The affidavit is intended to obviate the need for the presence of the actual account holder, whose testimony would likely be limited to confirming that the credit charges in question were not authorized.

In interviews with the prosecutors of the five Maryland jurisdictions, the general consensus was that this authorization has had little practical benefit. Due to the Constitutional requirement that the accused be allowed to confront accusing witnesses, an affidavit can only suffice for personal testimony if the defense consents. In nearly every case, however, defense will request the presence of the witness. Requiring the presence of all witnesses is generally regarded as the minimum that defense counsel can do to render effective assistance to the defendant. Accordingly, local prosecutors proceed as if the defense will always request the presence of the account holder/victim.

Although the defense counsel will likely always demand the presence of the account holder/victim, in identity fraud cases, ironically, the testimony of the account holder/victim is often not very helpful. The victim rarely knows how his or her account was breached, let alone details about any scheme that led to the fraud or theft. The account holder/victim generally only knows, and can only reliably testify, that specified charges occurred without his or her knowledge and they were not authorized. Prosecutors are considering using technology to try to address the problem of witness availability. For example, using videoconferencing technology to transmit a live video feed of the witness could alleviate some of the inconvenience of testifying for the witness, without unduly compromising the right of the accused to confront those who testify against him or her.

A related issue with regard to witness availability has to do with business records. Generally, not only does the account holder need to be present to testify that unauthorized charges occurred, but a representative from the business or financial entity must also be present to verify the authenticity of the business records. The Maryland Task Force to Study Identity Theft recommended in 2007 that the rules of evidence be amended to allow the admissibility of personal or business records if the account holder testifies as to their authenticity in a judicial or administrative proceeding. The account holder is testifying under oath anyway, and the additional testimony of a financial or business entity generally adds little to the probity of the evidence. The existing requirement for authentication of business records by a business can be a potential source for trial delays, according to prosecutors. To date, the Maryland General

Assembly has not passed legislation that would allow account holders to authenticate their business records.

Challenges Across Jurisdictions

Another aspect of the crime of identity fraud which erects sometimes insurmountable obstacles for law enforcement is the ease with which the crime may be perpetrated across jurisdictional boundaries spanning not only other states but other countries and even continents. When Maryland's identity fraud law was enacted in 1999, only the law enforcement personnel who had jurisdiction over either the scene of the crime or the residence of the victim could investigate an alleged identity theft crime. In 2002, the State's identity fraud law was expanded to authorize law enforcement agencies to pursue identity thieves throughout the state, without regard to in-state jurisdictional demarcations, subject to oversight by the Maryland State Police. In spite of this broad authority, State and local law enforcement agencies are still hampered by limited resources.

None of the five local police departments that were interviewed for this paper could assert that significant resources were available to pursue perpetrators located out-of-state (unless they were in nearby jurisdictions such as Washington, DC, Delaware, Virginia and Pennsylvania) or to collaborate with victims who were located out-of-state (especially if they resided west of the Mississippi River) but happened to be in Maryland when victimized. The local police departments interviewed for this paper presumably have more in the way of resources to pursue out-of-state crimes than other Maryland jurisdictions since they are the five largest in the State. Of course, police departments and local State's Attorneys must also balance the desire to apprehend identity thieves with the resources available to accomplish that task. The same police departments and prosecutors that are pursuing identity thieves must also allocate significant resources to capture murderers, rapists, robbers, etc. Significant resources could be deployed to apprehend a non-violent identity thief in Illinois, for example, who victimized someone in Maryland who is reluctant to testify because he or she already had lost funds or credit restored; or those limited resources could be used to track down a violent felon who has victimized people who remain motivated to do what needs to be done to be sure that the criminal is held accountable, including testifying at trial. Law enforcement departments may have the resources to do one or the other, but not both, very well. As a result, resources are likely to be deployed where the greatest return on investment can be realized. Most would agree that limited enforcement resources need to be used for violent felons first.

Arrest and Detention Considerations

Arresting a Suspect

In Maryland, local police departments need authority to arrest a suspect and acquire the information, documents, and other physical evidence needed to prosecute a case. Once a law

enforcement officer has identified an identity thief, the officer must submit the case information so that charges can be filed. For cases that can be prosecuted in the District Court, the case information is presented, in most cases, to a District Court Commissioner so that a determination can be made as to whether sufficient probable cause exists to issue an arrest warrant. The commissioner reviews the officer's description of the case and determines whether probable cause has been established (which supports the issuance of an arrest or search warrant) or whether the facts of the case support the issuance of a summons. The issuance of an arrest warrant, for example, authorizes the officer to pursue and detain the suspect. A summons, on the other hand, can be delivered in person, but is likely to be delivered by mail. If a commissioner determines that only a summons is justified to follow up on a potential case, then, for the officer that means that the case facts are not strong enough to justify an arrest warrant. The officer can continue to develop the case and wait for a response to the summons, spend additional resources to develop the case and resubmit the case to a District Court Commissioner, or allow that case to take a lower priority in favor of cases that would more readily qualify for the issuance of an arrest warrant. In circuit court, arrest warrants may be issued by a circuit court judge, through indictment by a grand jury, or the filing of a criminal information by a State's Attorney. Of course, the police have the power to arrest without a warrant upon witnessing a crime in progress or in other specified circumstances.

After Arrest and Before Trial

Those interviewed highlighted a significant difference in the federal and state arenas regarding the standards governing when and how arrested identity fraud suspects are detained before trial. In discussions with prosecutors in the five jurisdictions that are discussed in this paper, anecdotal evidence suggests that when identity theft suspects appear for bail determination, they are likely to be released on personal recognizance until the trial date. The primary determination for authorizing release on bail or personal recognizance before trial are whether (1) the suspect is a flight risk; and (2) the suspect is likely to be a danger to the alleged victim and the community if the suspect is not detained while awaiting trial. If the answer to both of these queries is "no," the suspect should be released. Most identity theft suspects arraigned at the State level are considered non-violent and if the suspect has community ties and/or employment, is a first-time offender, or an offender with a relatively limited history of criminal activity (excluding traffic violations) then the suspect is not considered to be a flight risk. Anecdotal evidence also indicates that outside of the requirement that the offender post bond (if bail is set) and stay in the jurisdiction, it is rare for a judge to impose other conditions of bail, such as a requirement that the suspect refrain from using computers, printers, embossers, cellphones and other "tools of the trade" typically used by identity thieves.

In the federal arena, the U.S. Attorney's Office for the District of Maryland reports that identity theft suspects are rarely released on personal recognizance and are frequently held pending trial as they are generally regarded as a flight risk. This is because identity theft suspects are presumed to have the technical expertise and the tools (such as fake credit cards and other fake documents) to successfully represent themselves as someone else to avoid prosecution.

Sentencing Outcomes

Those law enforcement personnel interviewed in both the State and federal arenas reported that differences in the way identity theft offenders are treated are also apparent with sentencing outcomes. At the State level, State's Attorneys in the four of the five jurisdictions interviewed for this paper noted that there are often difficulties in getting judges to impose a sentence that requires a period of incarceration. For first-time offenders at the State level, the imposition of probation before judgment (PBJ) is not unusual. Also routine is the transfer of this type of case to the *stet* docket (that is, a case and its charges are held in abeyance for a set period of time, and, if there is no further offense, the case is dropped). In the relatively infrequent event that an identity theft suspect is held until trial, when the suspect is found guilty, any imprisonment sentence is likely to be limited to time served. If an imprisonment sentence is imposed, most, if not all of the sentence is likely to be suspended. It is common for prosecutors to also designate identity fraud cases as *nolle prosequi* (that is, the prosecutor declines to prosecute for the time being). If it looks as if the case could lead to a more complex scheme or additional perpetrators, the prosecutor has the discretion to recharge the suspect at a later date. Maryland prosecutors and law enforcement officers indicated that judges tended to focus less on imprisonment of offenders and more on the expressed remorse of the offender and his or her willingness and ability to make restitution to their victims.

Of the five jurisdictions interviewed, prosecutors and law enforcement officers in Baltimore County indicated that more severe sentences, including imprisonment, were likely to be handed down for identity thieves. The law enforcement officers and prosecutors attribute these more severe penalties to the relatively high priority accorded economic crimes in the county, especially identity fraud. They report this has resulted in a relatively higher priority attached to these crimes by the Baltimore County judicial bench.

In the federal arena, sentencing outcomes were reported to be more severe and frequently include imprisonment of at least two years. In the first place, the cases handled at the federal level involve significantly higher dollar amounts and more complexity. A federal identity theft case could involve interlocking schemes that traverse several states and include international elements. As a result, when convictions occur, longer imprisonment terms are more likely to be imposed. In the second place, although restitution is routinely ordered in federal cases, the institutional expectation is that the offender will not be able to comply with a restitution order, as he or she has already spent the assets acquired by the scheme. Especially for schemes where many thousands of dollars are stolen, it is also likely that other holdings of the offender were subject to search, seizure, and forfeiture, (seizure and forfeiture of asserts is not authorized in Maryland) so those assets would not be available to the offender to make restitution. Due to the dollar amounts, the wide-ranging impact of the schemes investigated at the federal level, and the complexity of these schemes, federal prosecutors emphasize the need for imprisonment when making sentencing recommendations to the judge. For those offenders found guilty of aggravated identity theft at the federal level, sentencing guidelines require the imposition of a mandatory minimum sentence of two years imprisonment.

Stopping and Preventing Identity Theft: Possible Approaches

As the investigation and prosecution of identity theft in Maryland has continued to evolve, those investigating and prosecuting these crimes have been identifying additional approaches or changes that could assist them with this issue. Interviewees consistently mentioned six different approaches that could help prevent identity theft in Maryland: (1) forfeiture and seizure of assets; (2) increased public awareness; (3) increased industry cooperation; (4) increased technological resources; (5) improved victim and witness participation; and (6) greater use of available legal resources.

Assets Forfeiture and Seizure

Recommended by the Task Force to Study Identity Theft in 2007, asset forfeiture and seizure authorizes a court to order forfeiture of all property obtained from the crime by a criminal convicted of identity theft. Under the most recent asset forfeiture and seizure bill introduced (House Bill 1316 of 2011), a law enforcement agency would have been able to seize specified property on process issued by a court of competent jurisdiction. Property could be seized without a warrant if the seizure was incident to an arrest, or search under a search warrant, or if the seizure was made with probable cause to believe that the property was used or was intended to be used for the purpose of a financial crime. Property or an interest in property would not have been subject to forfeiture if the owner established by a preponderance of the evidence that the violation was committed without the owner's actual knowledge. Under Maryland law, the forfeiture procedure is only authorized for controlled dangerous substance, gambling, gun, explosives, mortgage fraud and, as of October 1, 2013, human trafficking violations.

During interviews with the five jurisdictions' law enforcement agencies, officers provided several examples of cases where identity theft defendants were able to keep the proceeds or property obtained by perpetrating identity theft. A few of the cases involved defendants stealing money and investing the money into their personal homes. Local law enforcement agencies, as well as State's Attorney's offices, expressed support for an asset forfeiture and seizure law. Because financial crime defendants rarely pay restitution ordered by the court, asset forfeiture and seizure could be an approach used to make victims whole and possibly deter potential identity theft offenders.

Increased Public Awareness

Many victims of identity theft are unaware of the prevalence of identity theft, how to prevent identity theft, and what actions to take if their identities are stolen. A number of police officers and prosecutors agreed that at least some identity theft could be prevented with better consumer education and vigilance. Interviewees recommended an increase in public outreach and education regarding methods to protect PII, including properly destroying documents and mail and making secure purchases on the Internet. Providing more public workshops and forums

to discuss identity theft may eliminate, according to interviewees, some instances of identity theft and reduce the negative impact of identity theft if it occurs.

Increased Industry Cooperation

An additional approach to preventing and stopping identity theft in Maryland involves convincing retailers and banks to modify their systems to allow for the thorough investigation of identity theft. Retailers and banks operate computer and security systems that, although beneficial to their institutions, are not always beneficial to law enforcement and prosecutors who are attempting to apprehend identity thieves. For example, the buying gift cards with stolen credit cards scheme relies almost exclusively on retailers (1) failing to track the card numbers of purchased gift cards; and (2) allowing gift cards to be purchased using credit cards. These two gift card practices, not tracking gift card serial numbers and authorizing the purchase of gift cards with credit cards, may help retailers provide a customer experience that is quick and easy. Modifying these practices, however, could allow law enforcement to access more information regarding certain identity theft crimes and fully investigate claims of identity theft and financial fraud. While certain retailers have altered their policies regarding gift cards by prohibiting the purchase of gift cards using credit cards, other retailers have not amended their practices. Retailers and banks' other systems and practices include (1) storing security camera footage in proprietary video formats so that the videos are not viewable by law enforcement; and (2) withholding compromised account holders' contact information. Such practices have an enormous impact on the investigation and prosecution of identity theft. Creating incentives for retailers and banks to modify such systems and practices may increase the effectiveness and efficiency of identity theft investigations and prosecution.

Increased Technological Resources

As noted, at least one of the major local law enforcement agencies interviewed does not have the technology needed to investigate identity theft crime rings, many of which are complex and involve various types of electronic equipment. Presumably, smaller local police departments that were not interviewed have even less technological resources available to investigate identity theft crimes because of fewer incidences of identity theft and smaller budgets. Therefore, increasing the amount of technological resources available to law enforcement may help Maryland advance in its investigation and prosecution of identity theft.

Improving Victim and Witness Participation

As noted, the use of videoconferencing technology could be helpful with increasing the availability of victims and witnesses for identity fraud trials, without unconstitutionally compromising the right of a defendant to confront and cross-examine witnesses. Such technology is readily available and has become significantly easier to acquire due to the portability of devices and the reduced costs of implementing this function. Also, as noted, there was wide agreement that being able to authenticate personal and business records without

corroborating testimony from representatives of business entities could help speed the consideration and closure of identity fraud cases.

Greater Use of Available Legal Resources

A significant positive change in the fight to prevent identity theft in the last ten years is the increased awareness about the crime and its destructive effects. Also, additional legal tools are available to police and prosecutors, although these additional tools (such as creation of the pretexting offense and the offense of unauthorized possession or use of skimmers or reencoders, for example) are not always widely known or appreciated, even among prosecutors. There may be ways to creatively use the charging authority already available to hold more identity fraud criminals accountable. This already occurs, at least to some extent, when prosecutors charge a number of offenses which have elements similar to identity fraud, to increase the leverage on suspects.

Conclusion

Investigating and prosecuting identity theft cases is extremely challenging and can be rewarding for investigators and prosecutors. At the same time, it can be an extremely frustrating endeavor. Law enforcement officers and prosecutors – whether at the federal or State levels – cite the tremendous amount of resources required to put together a case against an identity thief. Painstaking research may be required to determine how schemes are designed. A very detailed understanding of how money moves in a financial environment; how merchandise moves in a retail environment; and how merchandise, credit and other financial instruments are converted to cash is also required. Often cited by those who were interviewed is the frustration that comes from the development of a strong case that may only result in a *nolle prosequi* at the State level or maybe a two year prison sentence at the federal level – in other words, not a big payoff in terms of the penalties that could have a deterrent effect on this crime.

An interesting aspect of the crime of identity theft is the way criminals respond – almost mutating – in response to changing circumstances. In 2008, Maryland enacted a law making the possession and use of skimmers and reencoders a crime. Criminals have responded by finding and using cameras, and skimmer and reencoder devices that are significantly harder to detect. They have also responded by focusing more on database breaches that can yield thousands of records of individuals that can be sold and resold or used over a period of months or years.

At the federal level especially, law enforcement officials have noticed the increasing organizational sophistication employed to pull off some of the more complex identity theft schemes. Indeed, elements of organized crime have made incursions into the identity theft business. Some crime elements structure their organizations similarly to terrorist cell networks. Along with the trend toward more organized networks of criminals is also a trend toward escalating violence. At the same time, technological advances have made it almost easy for a

thief on a different continent to target an unsuspecting person in Maryland and wreak havoc on his or her financial life.

While it has proven difficult for State and federal criminal justice organizations to pivot as quickly as the criminals seem to be able to with regard to creating new and ever more inventive identity fraud schemes, progress has been made and continues to be made against this crime. Overall, law enforcement organizations have become more adept at using the same technology so often used by criminals and could benefit from receiving additional resources. The use of technology to improve education and outreach is necessary so that all the stakeholders involved in preventing this crime – the consumers, the retailers, the banks, the investigators, prosecutors, judges, and juries – can increase their understanding of how this crime is perpetrated and the truly devastating impacts it can have. The five jurisdictions that were interviewed for this paper have developed relationships through task forces and workgroups established at the regional and federal levels. The sharing of information that occurs under these circumstances has become invaluable in uncovering identity theft schemes and identifying the criminals who perpetrate them.

Appendix I. Federal Statute *(summary)*
Identity Theft Assumption and Deterrence Act (ITADA)
18 U.S.C. §§ 1028 and 1028A

Selected Defined Terms	• "Authentication Feature" means any hologram, watermark, certification, symbol, code, image, sequence of numbers or letters, or other feature that either individually or in combination with another feature is used by the issuing authority on an ID document, document-making implement, or means of Identification (ID) to determine if the document is counterfeit, altered, or otherwise falsified;
	• "Document-Making Implement" means any implement, impression, template, computer file, electronic device, or computer hardware or software, that is specifically configured or primarily used for making an ID document, a false ID document, or another document-making implement;
	• "ID Document" means a document made or issued by or under (1) the authority of the U.S. government; (2) a state or political subdivision of a State; (3) a sponsoring entity of a nationally significant special event; (4) a foreign government or political subdivision of a foreign government; or (5) an international governmental or quasi-governmental organization which, when completed with information about a particular individual, is of a type intended or commonly accepted for ID of individuals;
	• "False ID Document" means a document of a type intended or commonly accepted to ID individuals that –
	  • Is not issued by or under (1) a governmental authority; (2) a sponsoring entity of a nationally significant special event; or (3) an international governmental or quasi-governmental organization;
	  • Appears to be issued by or under the authority of a government, a sponsoring entity of a nationally significant special event, or international governmental or quasi-governmental organization;
	• "Means of ID" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual including an –
	  • Name, SSN, date of birth, official State or government issued driver's license or ID number, alien registration, government passport number, employer or taxpayer ID number;
	  • Unique biometric data such as fingerprint, voice print, retina or iris image, or other unique physical representation;
	  • Unique electronic ID number, address, or routing code; or
	  • Telecommunication ID information or access device, as specified;
	• "Personal ID Card" means an ID document issued by a state or local government solely for the purpose of ID.

Offense	It is prohibited, under a specified circumstance, to knowingly – • And without lawful authority produce an ID document, authentication feature, or false identification document; • Transfer an ID document, authentication feature, or a false ID document knowing that the document or feature was stolen or produced without lawful authority; • Possess an ID with intent to unlawfully use or transfer five or more ID documents, (other than those lawfully issued for use of possessor) authentication features, or false ID documents; • Possess an ID document (other than one lawfully issued to the possessor) or authentication feature with intent that the document or feature be used to defraud the U.S.; • Produce, transfer or possess a document-making implement or authentication feature with intent that the implement or feature be used to produce a false ID document or another document-making implement or feature that will be so used; • Produce an ID document or authentication feature that appears to be a document or feature of the U.S. or a sponsoring entity of a nationally significant special event, that is stolen or produced without lawful authority, knowing that the document or feature was stolen or produced without lawful authority; • Transfer or possess or use without lawful authority a means of ID of another person with intent to commit, or aid or abet, or in connection with any unlawful activity that violates federal law or is a felony under state or local law; or • Traffic in false or actual authentication features for use in a false ID document, document-making implement or means of ID.
Application	The referenced specified circumstance is – • The ID document, authentication feature or false ID document is or appears to be, issued by or under U.S. authority, or the sponsoring entity of a nationally significant special event, or that the document making is designed or suited for making an ID document authentication feature or false ID document; or • Knowing possession of an ID document (that is not issued lawfully to the possessor) authentication feature, or false ID document with the intent that the document or feature be sued to defraud the U.S.; or either • The prohibited production, transfer, possession or use is in or affects interstate or foreign commerce including electronic transfer; or • The means of ID, ID document, false ID document or document-making implement is transported in the mail in the course of production, transfer, possession or use that is prohibited.

Penalties	Forfeiture to the U.S. of any personal property used or intended to be used to commit the offense; and Maximum penalties of 15 years imprisonment and/or a fine of $250,000 if the offense is – • Production or transfer of an ID document, authentication feature, or false ID document that is or appears to be issued by or under U.S. authority; or • A birth certificate, driver's license, or personal ID card; • The production or transfer of more than five ID documents, authentication features, or false ID documents; • The knowing production, transfer or possession of a document making implement, or authentication feature with intent that the implement or feature be used to produce a false ID document or another document-making implement or feature that will be used as prohibited; or • The knowing transfer, or possession or use without lawful authority of a means of ID of another person to commit or aid or abet, or in connection with, any unlawful activity that violates federal law or is a felony under state or local law if, as a result of the offense, the violator committing the offense obtains anything of value aggregating to $1,000 or more during any one-year period. Maximum penalties of 5 years imprisonment and/or a fine of $250,000 if the offense is – • Any other production, transfer or use of a means of ID, an ID document, authentication feature or a false ID document; or • Knowing possession of an ID with intent to unlawfully use or transfer five or more ID documents, authentication features, (other than those lawfully issued for use of possessor) or false ID documents; or • Knowing transfer or possession or use without lawful authority a means of ID of another person with intent to commit or aid or abet or in connection with, any unlawful activity that violates federal law or is a felony under State or local law. Maximum penalties of 20 years imprisonment and/or a fine of $250,000 if the offense is committed to – • Facilitate a drug-trafficking crime; • In connection with a crime of violence; or • After a prior conviction under ITADA becomes final. Maximum penalties of 30 years imprisonment and/or a fine of $250,000 if the offense is committed to facilitate an act of domestic terrorism. Maximum penalties of one year imprisonment and/or a fine of $250,000 in any other case.

Aggravated ID Theft/Penalties	The knowing transfer, possession or use, without lawful authority of a means of ID of another person during and in relation to, any felony violation, as specified, must be sentenced to two years imprisonment in addition to the punishment imposed for the underlying felony; The knowing transfer, possession, or use, without lawful authority of a means of ID of another person or a false ID document, during and in relation to a federal crime of terrorism, as specified, must be sentenced to five years imprisonment in addition to the punishment imposed for the underlying felony; and The offender may not be placed on probation.

Source: United States Code, Cornell University

Appendix II. Maryland Statute *(summary)**
Identity Fraud
§ 8-301 of the Criminal Law Article

Selected Defined Terms	• "Payment Device Number" (PDN) means a code, account number, or other means of account access, other than a check, draft, or similar paper instrument, that can be used to obtain money, goods, services, or anything of value, or for purposes of initiating a transfer of funds; • "PII" includes a name, address, telephone number, driver's license number, SSN, place of employment, employee ID number, *health insurance ID number*, *medical ID number*, mother's maiden name, bank or other financial account number, date of birth, personal ID number, *unique biometric data, including fingerprint, voice print, retina or iris image or other unique physical representation, digital signature,* credit card number, or other PDN; • "Reencoder" means an electronic device that places encoded personal ID information or a PDN from a magnetic strip or stripe of a different credit card or any electronic medium that allows such a transaction to occur; • "Skimming device" means a scanner skimmer, reader, or any other electronic device used to access, read, scan, obtain, memorize or store PII or a PDN encoded on a magnetic strip or stripe of a credit card.
Offense	A person may not knowingly and willfully **–** • And with fraudulent intent possess, obtain, or help another to possess or obtain any PII of an individual, without the consent of the individual to sell, transfer the information to get a benefit, credit, good, service, or other thing of value, *or to access health information or health care* in the name of the individual; • Assume the identity of another, including a fictitious person • To avoid ID, apprehension or prosecution for a crime; or • With fraudulent intent to: • Get a benefit, credit, good, service or other thing of value; • *Access health information or health care*; or • Avoid payment of a debt or other legal obligation; • And with fraudulent intent to obtain a benefit, credit, good or service or other thing of value *or to access health information or health care*, use a reencoder or skimming device; • And with fraudulent intent, possess, obtain, or help another possess or obtain a reencoder device or a skimming device for the unauthorized use, sale, or transfer of PII or a PDN; • Claim to represent another person without the knowledge or consent of that person, with intent to solicit, request, or take any other action to induce another person to provide PII or a PDN (pretexting).

Penalties	A person who violates the law (except for the offenses of (1) possession or obtaining or helping another to possess or obtain a reencoder or skimmer; and (2) pretexting) where the benefit, credit, good service, *health information or health care* or other thing of value has – • a value of $500 or greater *($1,000 to less than $10,000)* is guilty of a felony and on conviction is subject to maximum penalties of 15 *(10)* years imprisonment and/or a fine of $25,000 (*$10,000);* • *a value of $10,000 to less than $100,000 is guilty of a felony and is subject to maximum penalties of 15 years imprisonment and/or a fine of $15,000;* • *a value of $100,000 or greater is guilty of a felony* and is subject maximum penalties of 15 *(25)* years imprisonment *and/or a fine of $15,000;* A person who violates the law (except for the offenses of (1) possession or obtaining or helping another to possess or obtain a reencoder or skimmer; and (2) pretexting) where the benefit, credit, good service, *health information or health care* or other thing of value has – • a value of less than $500 *(less than $1,000)* is guilty of a misdemeanor and on conviction is subject to maximum penalties of 18 months imprisonment and/or a fine of $5,000 *($500)*; A person who violates the law (applies only to (1) knowingly and willfully assuming the identity of another to avoid ID, apprehension, or prosecution for a crime; (2) possession or obtaining or helping another to possess or obtain a reencoder or skimmer; and (3) pretexting) is guilty of a misdemeanor and on conviction is subject to maximum penalties of 18 months imprisonment and/or a fine of $5,000 *($500)*; A person who violates the law under circumstances that reasonably indicate an intent to manufacture, distribute, or dispense another's PII without consent is guilty of a felony and is subject to maximum penalties of 15 years imprisonment and/or a fine of $25,000.

*****Italicized content indicates provisions that become effective as October 1, 2013.

Source: Maryland Annotated Code

Source Documents

Primary Sources

Officers from the Police Departments of:

- Anne Arundel County
- Baltimore City
- Baltimore County
- Montgomery County
- Prince George's County

Prosecutors from the State's Attorney's Offices of:

- Anne Arundel County
- Baltimore City
- Baltimore County
- Montgomery County
- Prince George's County

Maryland Association of Bank Security

Maryland Motor Vehicle Administration

Office of Attorney General

Office of Public Defender

Prosecutors from the U.S. Department of Justice, Office of the U.S. Attorney, District of Maryland

Maryland District Court

Maryland State Commission on Criminal Sentencing Policy

Other Sources

American Guard Services

Board of Governors of the Federal Reserve System. *Regulation E: Electronic Fund Transfers Compliance Guide to Small Entities.* October 2011

Duncan, Ian. *Man Calls Self 'Schmuck' After Ordering Fraud Witness Murder*. Baltimore Sun, October 2012

Federal Bureau of Investigation

Federal Deposit Insurance Corporation.
Consumer News. Spring 1998
Debit vs. Credit Cards: How They Stack Up. Fall 2009

Federal Trade Commission
Consumer Sentinel Reports. 2002 Through 2012
Fair Credit Billing – Facts for Consumers. April 2009
FTC Obtains Court Order Halting International Scheme Responsible for More Than Ten Million Dollars in Unauthorized Charges on Consumers' Credit and Debit Cards. June 2010
Prepared Statement, *Identity Theft* before the Subcommittee on Technology, Terrorism and Government Information, Committee on the Judiciary, U.S. Senate, March 2000

Federal Bureau of Investigation. *2009 Mortgage Fraud Report 'Year in Review'*. 2009

Fine, Tamera. Office of the U.S. Attorney, District of Maryland, U.S. Department of Justice. Presentation on *Maryland Identity Theft Grade Card.* November 2012

Fox-Baltimore News. *Felony Lane Gang Strikes Again.* November 2012

General Accounting Office
Cyber Threats Facilitate Ability to Commit Economic Espionage. June 2012
Identity Theft – Available Data Indicate Growth in prevalence and Cost. February 2002
Identity Fraud – Information on Prevalence, Cost and Internet Impact is Limited. May 1998

Hernandez, Arelis. *Felony Lane Gang Targeting Shoppers, Church-goers.* Orlando Sentinel, August 2012

Immigration and Customs Enforcement – Homeland Security Investigations

Lippe, Adam, Office of Baltimore County State's Attorney. Presentation on *How to Talk to Law Enforcement and Why They Should Listen.* November 2012

Maryland General Assembly. *Task Force to Study Identity Theft – Final Report.* December 2007

Maryland State's Attorneys' Association

MacDonald, Jay. *ID Thieves Target Home Equity Line.* www.bankrate.com, November 2008

McGuinn, Colleen, Office of Howard County State's Attorney. Presentation on *Identity Theft.* November 2012

National Broadcasting Corporation. *Dateline – To Catch an ID Thief.* 2007

Office of the Attorney General. *Guidelines for Businesses to Comply with the Maryland Personal Information Protection Act.* 2012

Palmer, Walter E. and Richardson, Chris, ASIS Foundation. *Organized Retail Crime: Assessing the Risk and Developing Effective Strategies.* 2012

Satterfield, Jamie. *Last Defendant in Bank Fraud Scheme Using Homeless People Pleads Guilty.* www.knoxnews.com, June 2012

Social Security Administration, Office of Inspector General

U.S. Department of Education, Office of Inspector General

U.S. Internal Revenue Service

U.S. Marshal's Service

U.S. Postal Inspection Service

U.S. Secret Service

Wall Street Journal. *Spearphishing Fraud Hooks More Victims.* August 2012.

www.Wikipedia.com. *Internet* (History of), November 2012

www.USA.gov. *Credit Card Billing Disputes.* October 2012

Zimmer, Beau. *"Felony Lane Gang" Continues to Target Women across Florida.* Tampa Bay Florida News 10, October 2012