Identity Theft and Fraud: Who, What, Why, and Steps to Stopping the Epidemic

Prepared by the NECCC Technologies for Early Identity Management Work Group

NATIONAL ELECTRONIC COMMERCE COORDINATING COUNCIL

NECCC
2401 Regency Road
Suite 302
Lexington, KY 40503
(859) 276-1147
www.ec3.org

Made in the United States of America.

NECCC is a consortium of national organizations and public and private sector leaders identifying best practices for strategic change within government.

Alliance partners are:

National Association of State Auditors, Comptrollers and Treasurers
National Association of Secretaries of State
National Institute of Governmental Purchasing

NECCC also works in partnership with these affiliate organizations:

Association of Government Accountants
Information Technology Association of America
National Automated Clearing House Association
National Association of Government Archives and Records Administrators
National Association of State Treasurers

Table of Contents

Prologue

For the policy community, appreciating the elemental nuances of the evolution of the vast information technology network over the past 50 years presents challenges of vocabulary, technical complexity and simple perception. The societal shift to an “information economy” is well documented, but its meaning is poorly understood by policy makers, even in the flagship nation that spawned much of the information revolution.

The “Greenspan” effect on productivity may someday be revealed to lie at the heart of the absence of recessions in the U.S. economy for over a decade. Efficiency multipliers and other economists’ indexes are off the charts. Since the first PCs were exported from the U.S. in the 1980s, we have witnessed a succession in evolutions of manufactured technologies moving from proprietary wealth generators for their inventors and manufacturers to commodity tools without which, no economic activity can occur. U.S. producers carpet-bombed the planet first with PCs, then system components, then operating systems, then peripherals, then network architecture. At each stage, the technology began as largely proprietary and costly. At each stage of global network evolution, the technology migrated to being standardized, low-cost—essentially, a commodity.

We are now witnessing that migration from proprietary status to commodity in the area of security technologies. In the post-9/11 era, the concept of security is more readily appreciated in any discussion. For technology networks, not only has extrinsic risk heightened sensitivities about network security; systemic dependencies of many critical infrastructures has also raised appreciation of the value of security. No one planned that U.S. economic activity would become dependent on global, public information networks when the phenomenon began to evolve a decade ago. But the fact of the matter is that what were largely independent, disconnected private institutional networks in the commercial and government financial community in the 1980s now depend on the availability of the public Internet to execute their functions.

The U.S. economy is measured at almost $11 trillion dollars. Almost $3 trillion is cleared over the Federal Reserve’s private, secure Fed Wire network each day. And while that network is capable of isolation from the public network, normal bank transactions, ACH clearances, securities settlements and the full execution of the economy’s activities depends on such sites as NYSE.net, BankofAmerica.com and Treasury.gov being up, available and secure. When that is not true, when the full secure interdependent set of public and private network systems is not available, the U.S. economy will begin to grind to a halt at the rate of $100 billion dollars per hour.

Payrolls will not be met, shipments not paid for, production lines not run; an “economic nuclear winter” is only a few hours of inactivity away.

Among the technologies most essential to a secure network environment is *authentication*; the act of being able to identify a device, system or party to a network transaction to engender sufficient trust to engage in that transaction as one would in a paper world with a known entity. Authentication comes in many forms and flavors; it is traditionally comprised of the “shared secret” between two parties of something you have; something you know or something you are. Public key cryptography and biometric devices represent the dominant modes of electronic authentication deployed today; sometimes these are deployed in combination. Other methods exist.

Over the last decade, the early entrant vendors into electronic authentication markets relied largely on proprietary implementations of their technologies to secure customer loyalty and generate revenue. Increasingly, however, the global growth of electronic interchanges—e-commerce, e-government, electronic messaging—have produced a demand for interoperable security tools. And interoperable systems of authentication have begun to evolve to meet that demand. Previously proprietary vendors have stimulated ad hoc “standards” efforts; the concept of “federated identity” systems has emerged as a method of assuring the ability of individuals to secure authentication credentials from one issuing party and have them be accepted by an entirely unrelated, different transactional partner. While the commoditization of these leading edge system elements may rapidly reduce the unit revenue for vendors, the explosive growth in the number of consumers seeking the tools more than offsets—indeed, in market size eclipses — the revenue expectations of many security vendors.

Since late 2004, an additional phenomenon layered on top of the commoditization of authentication has influenced the security policy and market space; that is the explosive growth in incidents of lapses in data custody by entities—including commercial “data brokers”—who have a nominal duty of care over the personally identifiable information which they store on their systems. These widely reported episodes of data custody “breach” have spawned hysterical press reports, disproportionate legislative proposals and a flurry of demand for retail security products and services.

Unfortunately, they have not spawned a migration of data custodian behavior and widespread deployment of state-of-the art network and storage security tools.

One major purpose of the NECCC ID Theft and Fraud Work Group is to raise a clarion call across broad constituencies of data users and custodians to encourage the prompt deployment of appropriate, “best-in-breed” security technologies, policies and practices.

The stakes are simply too great to ignore. The “networked economy” is often today described in life-sciences terms. “Insults” to software are “viruses.” The entire space is referred to often as an “ecosystem.” In such an ecosystem, there will inevitably be swamps. And it is in the dark, dank corners of the network ecosystem, where the gators and cottonmouths of spam, phishing, ID theft and other abuses occur. Such unpleasant neighborhoods might be tolerable in the otherwise valuable and robust ecosystem, but for the fact that a connection is rapidly emerging between these annoying, inhospitable locales. Indeed, the terrorists and state-sponsored adversaries who wish Western democracies ill are increasingly being identified as organized sources of phishing, ID abuse and other retail consumer-targeted crimes. These organizations are utilizing the revenue gleaned from these bad acts to fund more fundamental, systemic threats.

While “good hygiene” alone will not prevent cyber attacks that could bring down the U.S. economy, each secured portal of entry unavailable to a worm, virus or Trojan denies a cyber terrorist one more platform to launch electronic exploits and represents an incremental step in the direction of a more secure environment. When good hygiene is the norm, and phishing, spam and ID abuses rare or non-existent, attacks against the network infrastructure will be more difficult, less prevalent and more easily repelled.

It is the objective of this work group to make the case for changed behaviors that support a more secure electronic ecosystem:

- Increased investment in R&D for security tools by government and industry.
- Increased deployment of available, best-in-breed tools by all network participants.
- Special care in securing Personally Identifiable Information, or PII, by data custodians.
- Responsible deployment of basic system hygiene by all consumer-network users.
- Incentives from the policy community to support these practices.

With these goals in mind, we present *Identity Theft and Fraud: Who, What, Why, and Steps to Stopping the Epidemic*.

Identity Theft and Fraud: Who, What, Why and Steps to Stopping the Epidemic

Who is Affected by Identity Theft and Fraud?

All U.S. citizens.

Identity theft and fraud affect every one of us in the United States. Since the beginning of 2000, 30,000,000 to 50,000,000 or more U.S. citizens have been victims of identity theft and fraud. Those affected come from every sector and demographic of U.S. society. The Federal Trade Commission, in a study performed by Synovate in 2003[i], found that 4.6% of survey respondents, an estimated 10,000,000 citizens, had discovered some form of ID theft or fraud during the previous year. In the same study, 12.7% of respondents, an estimated 27,000,000+ adult citizens, had discovered ID theft and fraud. The estimated cost of these crimes during the year prior to the study is over $50 billion, most of which is born by business and government. In addition to direct monetary costs, an additional 300 million hours were spent by citizens resolving the problems associated with these crimes. There are millions of additional hours of government and business personnel used to address these crimes rather than directed to other productive uses.

This personal identity information can also be used for non-financial crimes. “The most common such use reported was to present the victim’s name and identifying information when someone was stopped by law enforcement authorities or was charged with a crime.” (Federal Trade Commission report by Synovate) The terrorists acting in the 9/11 attacks used and shared a variety of fraudulent and criminally obtained documents. Our national and local security and safety are continually compromised as a result of identity theft and fraud.

Identity theft and fraud is a crime that is often not discovered for months after the event. The rate of occurrence of these crimes appears to have increased dramatically during the past several years. The figures included above are estimates of discovered crimes. Given the lag time of discovery and the increasing rate of the crimes, the actual incidence of the crime is likely to be significantly higher.

Identity theft and fraud is a crime that keeps on giving. Discovering, reporting and responding to a particular incident of ID theft and fraud does not mean that the ordeal has ended. Stolen or defrauded personal information is often sold and used repeatedly by numerous offenders creating

the potential for continuing offenses against victims. There is an active and vibrant market for stolen personal information, which will lead to further spreading of stolen identity information.

Identity theft and fraud is a crime that imposes a “tax” on each of us. Every product, service, loan and transaction includes an additional cost resulting from ID theft and fraud. These costs can appear directly, as in higher credit card rates, or indirectly, as in higher operating costs that appear in the final cost of credit, products or transactions.

The other “who” question is, “Who is committing ID theft and fraud?” There are lots of people. At this time the crime is a high profit venture, easily entered with relatively little chance of being caught, prosecuted or heavily penalized. There are individuals who steal a wallet or purse, gangs who copy PII from credit cards and IDs for their use or resale, there are loose confederations that share criminal techniques and provide a market for PII on the Internet. There are highly organized, highly financed, and highly skilled criminal operations, and there are foreign state or country operated enterprises attacking systems for tactical or strategic advantage.

What is identity theft and fraud? Identity theft and fraud can take a variety of forms, but in general involves the stealing or defrauding of personal identifying information such as

Web Threats Keep Users Away

By Matt Hines

October 26, 2005

New research released by Consumer Reports WebWatch finds that U.S. Internet users are cutting back on the hours they spend online, shunning e-commerce and refusing to give out personal information as a result of the rising tide of Web-based crimes related to identity theft.

According to the WebWatch report, released Wednesday, 80 percent of all American Web surfers are at least somewhat concerned about the threat of identity theft posed by engaging in online activities.

As a result of those concerns, at least 30 percent of the 1,500 people interviewed for the survey said they have reduced the amount of time they access the Internet.

In addition to going online less frequently, 53 percent of the respondents told WebWatch that fears of ID theft have stopped them from giving out their personal information to Web sites and online marketers, while 25 percent said they are no longer purchasing items from e-commerce sites.

In a nod to related information security concerns, some 54 percent of the respondents who still buy items online said they now read Web sites' privacy policies before doing business with a company, and 29 percent said they have merely cut down on the amount of Web shopping they engage in.

New York-based WebWatch, a grant-funded project of the nonprofit Consumers Union, said that consumers have dramatically shifted their views of online activity over the last several years, becoming far more conservative about what constitutes safe online behavior.

Compared to the group's 2002 study on the same topic, researchers said that people are placing far more importance on issues of security and privacy when choosing which sites they visit or do business with. (from e.week.com, October 26, 2005)

social security numbers, credit card numbers, drivers license numbers and the accompanying personal information or documents that are commonly used to validate identity and thus establish accounts and perform transactions.

A few years ago, identity theft and fraud was mostly a retail crime. A pocket might be picked and a wallet stolen or a credit card slip stolen or copied. A fraudulent account would be established by a visit to a bank or business. During the past few decades our transactional infrastructure has evolved to electronic. For good or ill most of our government and business transactions of all types are to some extent performed through an electronic infrastructure. The evolution to this electronic infrastructure has been accompanied by an evolution of criminals and their tactics. ID theft and fraud have become significantly “wholesale” electronic crimes. While there are still significant “retail” thefts of personal information, the large numbers of thefts of personal information occur “wholesale” electronically in which hundreds to millions of records are stolen, processed and marketed electronically by and to skilled, organized criminals. Accounts can be established remotely using compromised information from anywhere on the globe with an electronic connection. In a popular cartoon one dog at a desktop computer tells his friend, another dog, “On the Internet, no one knows you’re a dog.” Additionally, almost no one can tell where your doghouse resides, whether you are a wolf hound or a sheep dog or whether you are Rover pretending to be Fido.

The following scenarios have been selected as vehicles to explore a variety of aspects of Identity theft and fraud. When possible, actual situations or events are used. The scenarios will provide an event of identity theft or fraud, effects of that event, and actual and potential responses. It is expected that these scenarios will be used to stimulate the thinking and creativity of readers to develop a body of information and solutions to help fight this criminal epidemic that threatens us all.

Why Identity Theft is Increasing in Prevalence

Identity theft and fraud, as noted by the Synovate report previously mentioned in this paper, is increasing in prevalence and magnitude. A recent report[ii] displays how a single individual can compromise the PII of several millions of American citizens, in what the Department of Justice termed, “what may be the largest cases of intrusion of personal data to date.”

When dealing with criminals who are as clever as any in the security industry and as slimy as the aforementioned cottonmouth, legislation needs to be adjusted and created to address the facts of

criminal activity as they exist. Legislation currently seeks to thwart would-be criminals by acting as a deterrent to the actual crime of identity theft prior to the attempt to undermine the system, but this may well be inadequate.

Legislation in the United States, takes the form of several laws such as the Identity Theft and Assumption Deterrence Act of 1998, making the act of identity theft a felony, and the Identity Theft Penalty Enhancement Act, further enhancing legislation to include aggravated identity theft. There are many other laws aimed toward the credit reporting industry and the maintenance and regulation of the data it maintains; however, these continue to be opt-out facilities, favoring corporate rights to maintain data over consumer rights. None of these laws address the problem posed by "data-brokers." The states likewise have enacted laws on the subject of identity theft and consumer fraud that vary in severity and coverage from state to state. Considering all of these laws, they may still be inadequate to sufficiently eradicate the problem.

In 2002, the European Union (EU) enacted its Directive 2002/58/EC[iii], which relates directly to consumer rights to data ownership, placing the onus for gaining consumer consent (op-in) on the company and placing ultimate control of the flow of personal information on the consumer. The legislation includes such articles as limiting Web-bugs and cookies that a company might willingly install without consumer consent. This is very much a proactive system of organizing the flow of information from an individual, rather than utilizing felony charges as the only identity theft/fraud deterrence mechanism. The EU continues to utilize after-the-fact legislation[iv] to apply redress to the act of theft of consumer data.

The fact that the EU places squarely the onus of management of consumer data in the hands of the consumer is critical to our understanding of the course that needs to be undertaken. The United States can ill-afford another 9/11; with many terrorist attacks linked[v] to instances of identity theft, we need to act decisively to impede this agenda. This issue not only has links to terrorist activity, it also affects every American citizen. Consider one victim of identity theft, dealing with the effects and the ongoing battle that is the aftermath of a preventable crime.

No static document can provide viable long-term system or personal security solutions. Specific advice is at best effective for a short period of time after publication and often not even that. Practitioners of these crimes adapt extremely rapidly, daily and even hourly. The securing of PII must be seen as an ongoing process, not a destination. Until the risk/value equation of personal information is changed, there will be lots of criminals and organizations evolving attack mechanisms faster than any individual organization on its own can adapt. The following scenarios and initiative descriptions are meant to provide starting points for understanding the events that

lead to PII compromise, the effects of that theft or fraud and concepts to apply in addressing ID theft and fraud.

Case Studies

Statement of Nicole Robinson, Maryland

I am a victim of ID theft. One Friday evening in early April 2000, I was contacted by a fraud investigator of a national jewelry chain. He informed me that an individual had opened an instant credit account for $3,200 and bought two watches and a ring in a mall in San Antonio a day before using my social security number. The criminal had returned that day and attempted to purchase more merchandise–which the sales person thought was suspicious. The sales people told her that their computers were down and then alerted their fraud department and the San Antonio police.

On Monday, I contacted the three credit reporting agencies to see if there were any accounts that were opened recently, but there were no new accounts showing on my reports on that day. There were a lot of inquiries. I contacted my mortgage lender to alert them to the fact that there was a woman in Texas using my identity to obtain credit. They confirmed that a woman had provided my information in connection with an application for a personal loan with them in the amount of $1,800. They contacted her to tell her she was approved for the loan. She was arrested by the San Antonio police when she left the loan office with the loan check she obtained using my identity.

After she was arrested, they asked her where she obtained my social security number and date of birth. She told them that she worked for a business that maintained HMO databases. She searched that information to get my social security number and date of birth. She was charged with "making a false statement to obtain goods." She was released a few days later after she, her pastor, and parents assured a judge that she would not do this again. A few days after her release she applied for a mortgage using my social security number.

When I finally received my credit reports in the mail, there were several changes. I saw that she had made up middle names for my middle initial. She had provided a fictitious maiden name, several different addresses in Texas and several different dates of birth. Her use of my social security number severely delayed my ability to receive copies of my credit reports. Every time she made a new application for credit, the credit reporting agencies updated my credit reports with information that was provided by her. When I called the credit reporting agencies, I could not get access to my reports because the correct information had been changed to reflect the multiple fictitious addresses, names and dates of birth she was using.

On one application, she provided my social security number with the last two numbers transposed, and a bogus Texas address, and she was still approved for the item she sought. When the bills for the item were returned from the fake address, the creditor reviewed my credit report again and sent several of her delinquent bills to my home in Maryland. When I contacted them by phone, they were rude and did not want to believe the account was fraudulent, then refused to send me an affidavit of fraud. Shortly after I contacted them, they located the woman in San Antonio and repossessed the item from a warehouse. The business never acknowledged the account as fraudulent, but I no longer receive bills and the information has not resurfaced on my credit reports.

In the following months, I would discover that she also applied and was approved for computers, large appliances, clothing, household goods, a cellular phone and a $1,600 vacuum cleaner. Some items were obtained even after fraud alerts had been placed on my credit reports. In June of 2000, two months after her arrest, she shopped for a car with my identity. She eventually purchased a 2000 Mitsubishi automobile from a San Antonio dealership. Although it took me until January 2001 to verify that the car was not purchased using my identity, Geico insured the car for her in June 2000 using my identity. When I contacted Geico in June 2000 to obtain the VIN number of the vehicle, they refused to give it to me citing their policy on protecting the privacy of their policyholders. I thought that was ironic, since technically the policy they issued was to me. She was able to obtain $36,000 worth of goods and services in a three-month period.

I spent days talking to police in Texas in an effort to convince them that I was allowed by Texas law to file a report and to have her charged with theft of my identity. I had to pay for the collect call from the San Antonio Police Department to file the police report. I tried to contact the district attorney's office to see what I could do to have her charged and no one ever responded to my messages.

This crime affected my ability to refinance my home, obtain a line of credit at my bank, and get cellular phone service. It even affected accounts that I had prior to the crime. I subsequently had two lines of credit, both with zero balances and in good standing, closed because the businesses suspected that they too were fraudulent. I was told that I would have to reapply if I wanted the accounts re-opened. Most importantly this crime continues to give me constant anxiety.

When I was starting to believe that this was over, I received a collection notice in her name at my home in Maryland on April 4, 2001, more than a year after she assumed my identity. When I contacted the collection agency to tell them that they had the wrong person, I was told that the social security number that she provided for the loan was not mine. The gentleman at the collection agency told me that they had a bad address in San Antonio, so information was given to their research department and they came up with my address in Maryland. I asked him what service was connecting my address with this woman who was committing felonies in Texas, and he would not provide that information. I contacted him three times and he did not return my calls. His company transferred the account to a different collection agency that sent me a third letter. After four calls to the new collection agency, they finally agreed to stop sending me letters.

In July 2001, 15 months after her arrest, the criminal in my case was arrested and charged with two felonies in connection with stealing my identity. As of today, she has not gone to trial or pled guilty to the charges because her attorney says she is too sick to go to trial.

In February 2002, I received two collection letters at my home in the thief’s name for an account that she opened using a social security number that was not mine. When I called the collection agency, I was told that they used a skip trace report that had my address on it. They used her social security number for the skip trace and it came up with aliases that she had used, one of them was me, my property address and mortgage information and my social security number. Once again the collection agency refused to give me the name of the company that ran the skip trace report.

At the end of 2003, I ordered copies of my credit reports and discovered that I have been intertwined with my perpetrator. I have the master SSN and all of her debt has now been attributed to me whether my SSN was used or not. With one credit reporting agency, there were four credit reports bearing my SSN. At another the credit report I received was 54 pages long, it had 171 accounts, 140 of which were in collections. I also discovered

that my perpetrator, even after she was arrested, reactivated a dormant store account of mine in 2002. That account is now in collections. My perpetrator made over ten more applications for credit after she was sentenced in early 2003 for stealing my identity. I received a collection notice in January of 2004 for a check that she wrote on a closed account in 1999. The collection agency harassed me for three weeks even though I told them that I was a victim of this woman and that as a result our credit had been merged. The collector didn't believe me. He chose to believe that the skip trace report that he had was the truth, and I was a liar. He even called back to tell me that I would pay this bad check and that he had my SSN (the last four digits he recited to me). Even after I sent him a copy of the bill of indictment against my perpetrator, he placed the bad check on all my credit reports as a collection account the next month.

At the end of 2003 and beginning of 2004, I was able to clear one of the two erroneous credit reports over the phone. Equifax, however was much more difficult. I had to contact people higher up in the company to try to get my report disconnected from hers. In April of 2004, a mortgage broker ran my credit and told me that Equifax was reporting additional information on my credit report. She said that there was a "Nicole Robinson 01" and "Nicole Robinson 02" the information reporting under the "02" did not belong to me. I decided that I was in a no win situation.

I ordered my credit reports again at the end of 2004 in hopes of obtaining a mortgage in 2005. I had to dispute the bad check that she had written and that the collection agency was reporting as belonging to me. There was also a Sprint account showing on my credit report that was not mine as well. I disputed all this information with all three credit reporting agencies. This time there were no hugely egregious mix ups on my credit reports.

In February 2005, my credit was run through a mortgage broker. He sent me an e-mail saying that he could get me approved for a mortgage if I could prove that the bad accounts that were reporting were fraudulent. Since I had just seen my credit reports, I had no idea what he was talking about. He cut and pasted from the report he received using my SSN. The report was filled with delinquent accounts, hospital bills and bad checks. Equifax was no longer sending me the information, but they were sending the information to the creditors.

I made some calls to the Federal Trade Commission because at that point I had done all that a consumer could do to rectify erroneous credit reports. I called an acquaintance of mine who had a direct connection to a person at Equifax. I contacted her to get my credit report unlinked from my perpetrator. She told me that she had fixed the problem. I didn't reapply for credit immediately. My credit was run by another mortgage broker on June 1, 2005. I was again linked to my perpetrator and unable to get approved for a mortgage.

I have suffered and continue to suffer significantly at the hands of my impostor and the credit reporting agencies. I dread the thought of seeing my credit report or applying for credit. From day to day, I don't know what collection agency will contact me for debts that are not mine. I feel that my identity will never again belong solely to me. My thief is allowed to use it for fraudulent purposes with impunity. I will suffer and pay the costs forever.

A touching story to be sure, one that is told all too frequently in the lives of Americans. How much of this could be averted if stricter controls were put in place on the third-party that maintained the HMO databases in this scenario? No one can really say, but, what is certain, as long as we continue to passively allow PII data to be sold, rented, and otherwise shifted from unknown locale to unknown locale, we will continue to face these very types of stories. Even with tight controls in

place, we may find ourselves at the mercy of those who would do us harm, in the next scenario we'll take a look at how this can happen from the inside.

The Insider Threat

This scenario assumes the implementation of Personal Identity Verification (PIV) I/II in an Identity Management System (IMS), as prescribed by FIPS 201 and makes the assumption that the FIPS 199 impact-level is designated "high" for existing systems due to the confidentiality component. The theft of any amount of PII is assumed to be undertaken by a system authorized individual.

> A system-authorized individual misuses information due to predetermined human malefactor logic. This misuse has negative impact on an individual whose PII data is stored in the system, up to and including the misuse of their biometric data. The IMS auditing system records the intrusion by the authorized individual, but because the individual is authorized to use the system and the data, auditing is moot until an out-of-scope force like the victim or other third party recognizes the intrusion as such (witness Nicole in the previous case study).

There is any number of factors that lead to the realization of this type of scenario occurring at every stage of operation. During the system development stage, by designing a system that creates a single store for all PII data in a homogenous system, the designer lends the system to the potential for insider intrusion, notwithstanding the potential exposure from outside sources. This creates a single point of failure for access to the PII of an individual. At this stage, by further designing a system based solely on workflow processes and not considering the lower-level data exposes the system to incidents. During the operation and maintenance stages of the system life, access controls are in place with these controls focusing primarily on those *without* authorized access, that is, inspecting the system for failed attempts and generally reviewing the system from an "outside the box" or network- and system-centric point of view. Auditing is in place for the system, which for normal authorized access may not flag the incident as suspect until after the outside force recognizes the incident, creating a reactive versus a proactive auditing environment. Workflow processes, while addressing the ability of a single authorized person to create the PIV vehicle, by such actions as limiting creation through delegation of activities, say nothing of the ability to access the data after the fact. During the system retirement stage, the systems must be fully cleansed of PII data. These and certainly many more factors lead to the situation described in the scenario section above.

Most information systems contain information about both the users and third parties subject to the system, but the information that can be maintained by this type of IMS is truly frightening. From an impact perspective, it opens those subject to the system up to considerably larger sets of

potentialities for ID theft and misuse. For all intents and purposes, an insider could effectively change the identity of an individual by misusing their access to PII contained in this type of system. The impact could be devastating both in terms of financial and non-financial ramifications suffered by the victim. Financial impact could be as simple as opening a single account for making a single purchase. It could be as extreme as destroying the credit history of the victim and in many cases, will lead to trafficking[vi] the affected individuals entire PII storehouse for nefarious purposes. That biometric data is also included simply raises the level to which the loss of said data could have negative impacts on the affected individual. How could an individual ever effectively "prove" who they are if, for instance, the database has been compromised and they appear to have several and/or differing biometric footprints? From U.S. Senate Subcommittee testimony[vii] on identity theft in 2000, there was mention of an individual who had to go to the extent of providing fingerprints to prove his identity *after* spending 10 days in jail based on a search of his SSN that returned a warrant; this was the result of fraudulent use of his SSN. There exists now more than ever the possibility of misidentification based on fraudulent or invalid data. How much more compounded will the possibility for this type of misuse become when multiple facets of an individual's PII becomes subject to a single system or, through a system of systems in a federated environment? Other non-financial impacts include the emotional impact of having an identity stolen, the general lack of support found for ID theft victims, and the possibility of loss of self as a result of ID theft (i.e., job loss, credit destruction, etc.).

Of course this does not mean that the federal credentialing system and other such systems are inherently insecure. This does mean that particular attention needs to be paid to the preventive measures that should be undertaken as the system is developed, and throughout the life of the system. The preventive measures that could have been implemented in our case and should be considered both at design time and throughout the system life cycle of every such system will be bulleted here for each high-level causative factor. These should provide beginning discussion points for further securing the system from internal and external threats.

System Design

- System distribution
    - Biometric data in system1
    - Name data is system2
    - Other "Required" data in system3
- System communications
    - Query/Response systems for valid/invalid
    - Provide access only when required

- System business logic
    - PIV issuance allows action A
    - Address change allows action B
    - Action B requires approval of section C

Access Controls

- Tie access to specific functions (PIV issuance, change of address, etc.)
    - All other accesses flagged
    - Systemic/non-systemic workflows
- System access at different levels
    - View access on system1
    - No access on system2
    - Query/Response access on system3
- Limit admin functions
    - To the data
        - ALL accesses must be investigated
    - To the system
        - Only available from 8-5
        - Only available from Office 3A
        - Workflow requires 2 people in room
    - Different system, different admin
        - Don’t consolidate admin in a single person

Auditing Controls

- Record all accesses to ensure valid functions
    - Review heuristically from code
- Audit all admin access
    - For appropriate function
    - Cross-reference with different system accesses
- Audit the auditors

Business Controls

- Build separation of duties into system and business
    - Systemic workflows to regulate access to data for specific reasons
    - Business workflows to regulate who/how/why
    - Continually review workflows for incompatible activities at a single desktop

Legislation

- FIPS should specify the separation of data elements
    - No biometric data stored with name
    - No name data stored with SSN
    - Don't keep SSN unless mandated
- Identity Theft and Assumption Deterrence Act
- Reach must be expanded to include more protections for the victim
    - Credit card companies report raising interest rates based on credit ratings (whether fraudulent or not) and dealings with other creditors[viii]
- 48 States and Guam have some form of legislation[ix]
    - District of Columbia does not
    - Colorado does not
    - Vermont does not

Existing systems clearly cannot be re-built to encompass all of the measure suggested previously. Systems can however, be secured through the application of access controls, auditing controls, and business controls to the existing system. Incorporating access control to data elements at the user level helps to provide the granularity that should be found at the system level. If the system is modifiable, the existing system should be retrofit to limit access to certain data elements by certain users, thereby limiting the amount of information that any one user can gain benefit. Gaining any further benefit would require collaboration, which should not be easy to acquire (considering the quality of your workforce). If modification at the system or user level is not feasible, then business controls should be put in place that enforces the access controls that the system cannot enforce. These business controls can further build out the separation of duties to include the separation of access to certain data elements necessary to performing specific job functions. Java or html based front-ends can be built fairly easily to assist in obfuscating data from viewing, with or without an enterprise service bus or other service oriented architecture in place. While this is less than ideal, with proper auditing in place, it should suffice for bringing the system into an improved and more secure state. Proper auditing controls include all items listed in the Auditing Controls section of this document such as auditing all accesses to sensitive data for proper use, auditing all admin accesses to sensitive data and data stores, and of course, auditing the auditors to ensure that no collaboration has occurred at that level. Most modern systems have at a minimum a rudimentary auditing system integrated while most government systems go far beyond.

If the statistics for ID theft in general are any indication, this has the potential to be an enormous problem. But as it stands, statistics for ID theft by insiders are currently very sparse. This may be

due to the simple disconnect that exists between the time the data is actually stolen and when a person recognizes that ID theft has occurred (normally after trying to purchase something on new credit or review of credit report), which could be a considerable timeframe. This is a known problem that needs to be addressed along with developing statistics. Fending off this potential problem begins with the legislation that authorizes agencies to collect and maintain certain data. When legislation specifies that biometric (or any) data be collected but neglects to denote *how* the data should be stored as a dataset does a great disservice. To make a novel comparison, as a general rule, object-oriented programming defines both the data and the methods that can be applied to the data. Legislation regarding initiating data collection and maintenance should define the data to be collected, the methods that can be applied to that data (i.e., public information, private information, individual information, etc.), *and* how that data should be stored (i.e., as separate elements in a single system, as separate elements in separate systems, etc.). With good legislation, the agencies charged with implementing the legislation have less flexibility for interpretation of what "best practice" might dictate; the rules will be clear.

Agencies can now implement forward-thinking technologies and processes in their people-centric applications, where PII information will be stored. Best practices for credit card applications dictate not keeping credit card information after the transaction has been completed. This best practice applies equally to PII contained within a single system; keep the minimum amount of information required. Build a culture around separation of data elements. If it is harder for a single person to gain access to multiple pieces of PII, the safety of our consumer data will benefit.

In a recent case at the Department of Motor Vehicles California[x], there was a loss of driver information that resulted in the arrest of four employees. The employees created and sold false drivers licenses, identification cards, and vehicle registration documents. The arrests came after a 20-month investigation with internal affairs officers and federal agents. The striking fact about this case is the DMV has very strict controls in place to combat this type of fraud, even maintaining its own internal affairs officers that are sworn officers in the state. The systemic and business controls were in place, much like they are at any government institution. The one common factor that cuts across all government institutions is the hardest factor to control, people. Social engineering will be the lynchpin to succeeding in the battle for maintaining control of our systems. Employees entrusted with the confidentiality, integrity, and protection of citizen data must be inculcated with driving principles that necessarily present themselves as a resultant of being stewards of the citizen data.

Insider theft is a considerable problem; however, there are other areas of concern where citizens might find their PII compromised. In our truly mobile society, we carelessly utilize our cellular

telephones and PDAs and laptop computers to transfer information and data to any number of destinations. To continue the ecosystem analogy, it is imperative for us to communicate almost instantaneously with our work unit, our family, and others in our sphere of influence to be effective, not unlike gazelles communicating the impending leap of a plains lion. Consider the commuter in his daily ritual of getting to and from the office while continuing to be a producer in our society.

The Capitol Corridor Initiative

The Capitol Corridor Inter-City trains travel from Auburn, Sacramento, Santa Clara and San Jose in California's Silicon Valley. The trains are running trials that will evaluate technology and business models for trial WiFi and mobile Internet, working with the State of California, Department of Transportation, Rail Division, which has made arrangements with the California Center for Innovative Transportation (CCIT), an applied transportation technology research institution affiliated with the University of California Berkeley. The project is a collaboration between the French technology center of excellence, INRETS, GLOCOL, and the University of California at Berkeley.

The effort is to lead trials to provide secure wireless Internet services on a long-term exclusive basis. The example helps establish a protocol for sharing data and survey results with each vendor that respects the sensitivities of each vendor.

Wireless fidelity or Wi-Fi communication and mobile IP is being used for trials for commuter Internet services for mobile environments. Research Framework by Glocol introduces mobile IP, an open standard, defined by the Internet Engineering Task Force (IETF), which is becoming dominant today as it allows a user to keep the same IP address, stay connected, and maintain ongoing applications while roaming between IP networks. Mobile IP is scalable for the Internet because it is based on IP; any media that can support IP can support mobile IP. Mobility and networks while-in-motion are becoming dominant themes for the mobile Industry.

In IP networks, routing is based on stationary IP addresses. A payment device on a network is reachable through normal IP routing by the IP address it is assigned on the network. A payment device sitting on a network inside a moving medium such as an automobile, bus or train, as it roams away from its home network, is no longer reachable by using normal IP routing. This results in the active sessions of the payment device being terminated. Mobile IP enables users to keep the same IP address while traveling to a different network, ensuring that a roaming individual can continue communication without sessions or connections being dropped.

The security of transportation systems has taken on new dimensions since 9/11. New threats on the security and the safety of transportation systems, particularly trains and their users have come to light in recent years and present tremendous technical and operational challenges to wide open and expansive systems such as railroads. But new advances in information technology, particularly in the areas of sensing, data management and computing, and communications offer many opportunities to meet these challenges. One such opportunity is the growing interest in and market for the use of wireless technologies such as WiFi to provide Internet access on the various elements of the railroad system.

The objective of this scenario and simulation is to create a plan of pilot deployment to utilize wireless technologies while creating a trusted environment for secure transit operators:

- Capture the scene of security violation for post-incident investigation.
- Prevent wireless theft of data, wireless and radio-based hacking (e.g., wireless access security).
- Evaluate the wireless technologies as part of the viable communication mechanism for emergency response where land phone is inoperable.
- Implement a viable mechanism to alert train conductor of any adverse safety/security violation
- Improve passenger safety and make precautionary measures for any kind of fraud on train.

The simulation scenario describes an exercise to model and create a mobile network environment simulation within the Berkeley campus to demonstrate mobile networks using mobile IP protocol on mobile router and provide a platform to simulate trackside/wayside research tests before undertaking the test demonstrations at actual rail environment for physical testing on trains. The simulation tests also helped to demonstrate various mobility issues inside a mobile network and protocols for route optimization and to prepare a reference architecture for future trackside/wayside and terrestrial networks for rail and road, while demonstrating basic core requirements for real-time homeland security infrastructure deployment needs such as video surveillance.

Evaluations of on-board trial are a key component to understanding the process. During the course of the trial, the trial service providers may provide detailed specifications and customer valuation in a commercial (for fee) application setting.

The effort is intended to provide secure wireless Internet services on a long term exclusive basis. The example helps establish a protocol for sharing data and survey results with each vendor that respects the sensitivities of each vendor. Following are fundamental trusted performance attributes identified as core features of any wireless Internet service provider requirements:

Protected Commuter Communications

- E-mail, instant messaging
- Voice/fax

Protected E-Payment

- Online purchasing and e-payment
- Pay-for-content
- Pay-for-service
- Electronic ticketing

Information Protection

- Privacy
- Digital rights management
- LOB database locator

Network Access

- VPN and wireless access to home network
- Client integrity checking
- Protected logon

Information Access Control

- Documents and records
- Rail application information access
- Secure Web access for trusted operations like e-payment

As the mobile environment becomes ubiquitous, so the need to protect PII will also become paramount. As our communications environment continues its evolution to a more cohesive state, it will be incumbent upon us, the custodians of data, to maintain a clear delineation of what is acceptable use and a clear demarcation of what will not be tolerated from ourselves, our systems, and those that would do harm to our customers, the citizens we serve.

Stopping the Epidemic

Stopping the epidemic will be no small task, but like an unwanted virus in an ecosystem, it must be eradicated if life is to continue as normal. We have discussed some specific examples of how

and where ID theft and fraud occur and the affects on the individual of identity theft. We will now turn our attention to providing concrete efforts that can be undertaken to combat the situation.

Legislation

- Support giving consumers more control over their PII data, turning our consumer society from an opt-out society into an opt-in society.
- Support increasing privacy protection legislation to regulate all consumer entities that maintain any amount of PII information.
- Support stiffer penalties for those subverting identity theft regulation.
- Track existing and proposed legislation (e.g., the Identity Theft Protection Act of 2005 S.1408).

Government

- Inform citizens what data will be collected and why (e.g. legislation).
- Inform citizens how data will be used by the agency.
- Inform citizens how they will be contacted in the event of unauthorized disclosure of information.
- Perform privacy impact assessments yearly.
    - Post results to your consumers.
- Perform business process assessment.
    - Enable the discovery of potential insider enabling gaps.
    - Determine where the paper trail stops.
    - Use results to streamline business and close gaps.
- Develop a culture.
    - That supports us as custodians of citizen data.
    - That is offended by the concept of ID theft and fraud.
    - Where auditing is welcomed.

Systems and Networks

- Perform design-time consumer privacy impact.
- Perform design-time risk and impact assessments for all system and network components.
- Build business process separation into systems (Need-to-know).
- Exploit security measures (encryption, data separation, etc.).
- Deploy and maintain meaningful tools (NIDS, AntiVirus, etc.).
- Utilize current best practice (NIST FIPS, CERT, etc.).
- Utilize current best knowledge (CERT-NVD, etc.).

- Utilize federal guidance[xi] on cyberspace and physical security.
- Use multi-factor authentication that utilizes definitive sources.
- Utilize incident response teams for both hardware/software systems and business process failures.

Epilogue

Identity crimes are not recent innovations, nor did they spring up with the creation of the Internet or electronic information systems, but the quantity and quality of these crimes have changed with the development of the electronically interconnected world. Interlinking and interdependence of information systems, whether or not intentional, has occurred, continues to occur and will likely go on for some time to come. There is dramatic value to be had from the interoperability of systems. There are, however, potentially drastic unintended consequences for the unaware or unwary. Stopping the infection or invasion should not be conceived as a destination point. It is not a project that when completed can be forgotten. Success in repelling the infections and invasions requires the building and maintenance of a healthy infrastructure, which is comparable to the effort required to maintain a healthy body. It is not enough to eat a bowl of broccoli and jog a couple of miles and consider your health requirements covered. Maintaining personal health requires continual work, doing some things, not doing others, eating less or more of certain categories of food, getting help from others, planning for risks and insuring against disasters.

Not that long ago, information was stored in warehouses in filing cabinets. If it was important or valuable enough information there were guards and locks on the doors to prevent the information from being taken. Electronic storehouses replaced many of those paper warehouses, but the criminals still had to get into the buildings and then the electronic systems to access the information inside. As the electronic ecosystem has developed we built channels straight into the hearts of the electronic systems and opened many of them up to the denizens of the swamps of the virtual world. These channels provide access to creatures from anywhere in the physical world. Similar to past invasions of zebra mussels, snakehead fish or killer bees, creatures given access to foreign environs can cause tremendous damage.

If you believe that your system has not yet been compromised there is a high likelihood that your system has not yet been discovered, you don't present a tempting enough target yet, or you have missed a break-in. As in the physical world, the creatures will always find ways in faster than any of us can develop ways to keep them out. There are a host of dedicated, resourceful and often resource-rich vermin continually searching for gaps to crawl through, gnawing away at the electronic infrastructure to get to the goodies inside. Almost no organization can repel such a

siege alone. It takes full-time dedication to remain current on rapidly adapting intruders. There are a number of new groups that provide the latest pest eradication techniques, tools and documentation all of which should be required study material for anyone trying to maintain systems holding personal information.

Filling in the channels and disconnecting from the virtual world is not an acceptable option for most of us who have come to appreciate the benefits derived from electronic services and systems. In many cases there is no viable alternative to replace the infrastructure we have built which would provide us with the benefits we have come to expect and rely upon from e-commerce and e-government. To maintain those benefits will require effort on part of every beneficiary to avoid surrendering our way of life to those who would take it away from us.

Acknowledgements

Michael Aisenberg, Director of Government Relations, Verisign Inc.
Robert Bunty, IT Policy Consultant, Commonwealth of Pennsylvania
Dan Greenwood, Director, MIT E-Commerce Architecture Prgm., MIT
Denise Hendricks, E-Services and Support, Department of Motor Vehicles, State of California
Greg Martin, Information Systems Supervisor, State of Delaware
Harsh Verma, Principal and Director, GLOCOL Inc.
Steve Spoonamore, CEO, Cybrinth Inc.
Lori Wetzel Morris, United States Notary Association
Dan Combs, President, Global Identity Solutions
Bill Reinhard, Assistant State Controller, State of Nevada
Sjon Woodlyn, Infrastructure Branch, Department of Motor Vehicles, State of California

Bibliography

[i] http://www.ftc.gov/os/2003/09/synovatereport.pdf
[ii] http://www.usdoj.gov/opa/pr/2004/July/04_crm_501.html
[iii] http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML
[iv] http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:52004DC0346:EN:HTML
[v] http://www.fbi.gov/congress/congress02/idtheft.htm
[vi] http://www.usdoj.gov/usao/nj/publicaffairs/NJ_Press/files/pdffiles/fire1028.rel.pdf
[vii] Identity Theft: How it Happens, Its Impact on Victims, and Legislative Solutions – http://www.privacyrights.org/AR/id_theft.htm
[viii] Consumer Action 2005 Credit Card Survey
[ix] http://www.consumer.gov/idtheft/federallaws.html - criminalstate
[x] http://www.dmv.ca.gov/pubs/newsrel/2005-07.htm
[xi] http://www.whitehouse.gov/pcipb/