Internet Identity Theft

“A Tragedy for Victims”

A White Paper from the Technology Working Group, eBusiness Division, SIIA
Project Author: Tom Arnold, Chief Technical Officer, CyberSource Corporation

SIIA

Table of Contents

1. The Consumer Tragedy

This paper is not for the faint of heart. Those who would rather ignore the “dark side” of the Internet might be well advised to stop reading, pack a light bag and disappear into the Australian outback.

Identity theft is a crime where one person masquerades under the identity of another. This does not involve just the stealing of a credit card number, theft of a check, or the fabrication of false documents. This is also not an act that is limited only to the age of technology even though identity theft was not considered a crime in and of itself until 1998. Prior to that, the theft of an identity was considered a tool used in the commission of some other crime. However, improvements in computing and telecommunication technologies in the late 1990’s fueled a resurgence of Identity thefts allowing criminals to hide more efficiently.

In the past, a criminal would have to appear at a bank or lending institution to apply for an account increasing the risk of being captured. However with instant credit accounts on the Internet, the likelihood of a criminal being captured is greatly reduced and the immediate rewards for a thief of identities increased as well. A smart crook working on the Internet may turn a tax-free gain of as much as US$50,000 per week. Compare this to the bank robber who passes a note to a teller and, if he’s lucky, walks off with $1,000. The media plays up the crime of bank robbery and the criminal is hunted, prosecuted as a menace to society, convicted, and put away for years. The identity thief on the other hand committed only fraud, a *white collar crime* if and when he’s captured, the *fraudster* will use his victim’s funds to pay for defense, and may serve less than one year (if at all) in prison.

In January 2000, the US Fair Trade Commission estimated approximately 21,000 identities were stolen, a sobering statistic. The remainder of this section will offer two US case studies: traditional identity theft from the pre-Internet era and Internet identity theft. The following sections will cover the characteristics of Internet Identity theft, common methods of prevention and detection, the role of privacy and security policies in the private sector, a discussion of public policy, and close with an issue analysis of the case outlined below. The names in the cases have been changed to protect the victims.

Although the cases and legal policy discussions presented in this paper describe the situation in the United States, the subject and occurrence of Internet identity theft is a global issue. E-businesses, consumers, policymakers and law enforcement agencies need to be aware of the threat and understand how to prevent, detect and respond to this crime.

1.1 Traditional Identity Theft Case

Mary Jane Smith is a manager in the accounts payable department of hospital in northern Rhode Island. She and her family members have a health insurance plan that covers treatment at the same hospital. Mrs. Smith’s husband is stricken by a heart attack and rushed to the hospital where he is admitted and treated for a full week. But her husband’s condition deteriorates and he eventually dies. After settling the family affairs, Mrs. Smith moves to Ohio to live with her sister.

Four months pass and Mrs. Smith is contacted by a collection agency. She is asked why she has never made a payment on the new vehicle she purchased in Austin, Texas. Mrs. Smith denies she has ever purchased such a vehicle and states that she does not even have any credit accounts open as she cleared all debts after her husband’s death. The collection agency is adamant that she owes on the debt. They verify her social security number, past street address in Rhode Island, and date of birth. Mrs. Smith remains firm that she never purchased the vehicle and has never been to Austin, Texas.

At the conclusion of the call, Mrs. Smith pulls a credit report on herself and discovers that over $180,000 in charges had been made on accounts that she never opened.

The original phone call from the collection agency took place in 1994. Subsequently, Mrs. Smith had to battle 14 collection agencies and deal with all four credit reporting agencies on repeated occasions, as charges and accounts would be put back on her history within a month after they were removed. She attempted to file police reports, but was told that she was not the victim of any specific crime. Instead, she was told that the credit institution or merchant was the actual victim and would have to file the report. She then filed a report with the US Secret Service.

After a lengthy investigation, agents identified and arrested a suspect, who was subsequently convicted of the crime of fraud. As it turns out, the suspect was a clerical staff member working for Mrs. Smith at the Rhode Island hospital. The suspect stole private information about Mrs. Smith and her husband from medical records maintained by the hospital. Armed with this information, the suspect masqueraded as Mrs. Smith (even though the real Mrs. Smith was nearly 35 years older than the suspect) and opened the first credit account where a $2,000 diamond ring was purchased. The suspect left her job and moved to Austin, Texas at approximately the same time that the real Mrs. Smith moved to Ohio. At some point, the suspect obtained a Texas driver's license in the name of Mrs. Smith then purchased a Jeep Cherokee from a local car dealer. This was followed by the opening of 3 different cash lines of credit and the purchase of numerous disposable items, including computer products and jewelry which were all sold for cash.

In this case, the suspect initiated all fraudulent credit transactions in person, having to present herself and identification documents in person to sales staff at the merchant stores. Additionally, the suspect had to move quickly to run up credit charges so as to maximize gain and avoid identification. In each case, she preyed on merchants who offered quick credit under liberal terms. All revolving credit accounts were private-label card accounts, limited to use in a specific store, and it took over four months before the first creditor referred the delinquent account to collections. The collection agency quickly discovered that the address that had been used to open the accounts was bogus. Using the social security number, the agency then searched the credit bureau database and discovered the address and phone number for a Mrs. Smith in Cleveland, Ohio. They then made contact with the real Mrs. Smith and demanded payment.

1.2 Internet Identity Theft Case

This case occurred in late 1999 and will be the primary case followed through the rest of this white paper.

In October 1999, a list of current and retired command officers in the US armed services was posted on a public Web site. The posting was based on a publicly available document from the US Congressional Record. For over the last 25 years, the US military has used the Social Security Number as the *serial* number for soldiers, sailors and marines.

The clever criminal takes a copy of the list, goes to several other Web sites and applies for online credit, both at stores offering instant credit and those offering major brand instant revolving online accounts, like issuing an instant Visa™ account. One of the identities from the list is that of Retired Lt. Colonel James Jones who still lives in Baltimore, Maryland.

At some point in time, the criminal had to arrange addresses to receive the stolen funds and goods. It's believed that he used addresses from private mailboxes located throughout the North Eastern United States. According to Lt. Col. Jones, the suspect ran up charges for products including numerous computer systems, consumer electronics, and video game equipment. The suspect also took cash advances on the accounts. All transactions were placed over the Internet.

After the suspect attempted to make another cash advance, the bank decided to try and contact Lt. Col. Jones. In this situation, the account had been opened with a bogus address and phone number. Upon discovery the bank ran a credit report on the social security number and located another phone number for Jones at which time they contacted him. Lt. Col. Jones ran a credit report on himself and discovered that the suspect had run over $50,000 of charges using the stolen identity. Jones contacted law enforcement authorities in Baltimore, who subsequently contacted the US Secret Service.

At this time the suspect has not been located and continues to open new charge accounts online. During this period, numerous lenders have written off this bad debt, forging traditional collection agencies and sending negative reports to the credit bureaus. These actions have served to destroy the reputation and credit worthiness of Lt. Colonel Jones and his wife. They have been denied credit, been told that they could only purchase a car with cash, and invested constant agonizing hours of work to clear their report.

2. Understanding Internet Identity Theft

There is little difference between the cases described, except in the second example the suspect remains hidden from detection as a virtual entity on a public network. Although the suspect's methods and taxonomy of identity theft are similar, the technology of the Internet allows the suspect to move quickly, opening new accounts, striking merchant sites with rapid attacks, creating new victims in the number of merchants and volume of transactions that can be posted, and then disappearing into another identity. In this section, we take a look at some of the common factors related to stealing and using identities.

2.1 Common Factors

2.1.1 Identities are Stolen to Commit Other Crimes

In all cases, the theft of an identity is to commit some other form of crime. The criminal may commit fraud, sell the identities to others who commit fraud, generate new illegal forms of personal identity (like a birth certificate, driver's license, or even a passport), use the identity to acquire new access points to the Internet, and/or more.

2.1.2 The Victim Doesn't Know

Using the Internet, the victim of an identity theft may not even know how or when their identity was stolen. Until the suspect trips over some systemic control (as in the case of a velocity check) or bill collectors locate and contact the victim, the crime remains concealed.

2.1.3 Greed Drives Identity Theft

In any fraud there can be many victims, but the fraudster plays to the greed of someone or some entity. The following section introduces types of associated crimes, like account takeover and account creation.

As described in the prior cases, *account creation* preys on the greed and willingness of the bank or merchant to issue an instant account. All too often, these entities understand the potential risk and will quickly write-off losses when faced with a non-paying customer. In the case of Lt. Col. Jones, the lender even restored the identity and increased the credit line after apparently being notified by the suspect of a change of billing address. After three more months, the account was again closed and written off.

In the case of *account takeover* (not described in the cases, but a form of identity theft), the greed or desire of a merchant or another person to close a business transaction drives the fraud. This may include a company who is willing to risk fraud for the sake of increasing sales revenue. Or, a company who has a large backlog of products to sell and is *offering bargain basement pricing to move the good*s.

Another form of greed is the lender's failure to run complete credit checks before issuing a new account. The instant credit accounts issued on the Internet are completed and set up in a few minutes. Given the speed with which "instant" credit is approved, it is clearly not possible that a complete review of a credit file could have taken place. One can only surmise the lender's intense desire to open new accounts contributes to this problem.

2.1.4 Authentic, Bogus Addresses

In each account creation case, the billing address was a valid address and serviced by the US Postal Service. It just wasn't the address of the suspect. In some cases, the address was a private mail service or mail forwarding address. Goods and services that had to be shipped were sent to the same address as listed in the billing address. The use of large, upscale hotel addresses is also common.

2.2 Types of Associated Crimes

There are several types of crimes associated with Internet identity theft. These are some of the more common ones.

2.2.1 New Account Creation

New account creation involves stealing sufficient identifying information about an individual in order to open new credit accounts. The information needed to create new accounts can be gathered from a variety of sources including trash bins, legitimate files (as in the case of Mrs. Smith) or even public records (as in the case of Lt. Col. Jones).

2.2.2 Account Takeover

Account takeover involves assuming the identity from a single account and using the account to make purchases. The theft of the account information can be accomplished in many forms. In some cases, a criminal needing to increase his stock of cases may even use a prior stolen identity to help steal more. Here are some of the common tools and venues:

- Use of chat-room information from a public list. The new term *link capture* describes the tool and method for doing this. In this case, the criminal makes a posting that includes a hot link to a site that is outside the domain of the chat-room. This site is actually a Web page where the victim is asked to enter information on a form. The look and feel of the page may mimic the original chat-room or a service screen exactly. However in reality, the graphic content of the page will have been stolen from the site and reproduced to look the same.
- Site cloning, this is a variant of the chat-room method where a merchant Web site will have been cloned and will mimic the completion of a e-commerce purchase transaction, including the response of a email receipt. The only problem is that the product will never arrive.
- False merchant site is another variant on the *link capture*. In this situation, the suspect is running a merchant site, usually an adult site, which accepts credit cards for access or even accepts credit cards as proof of age. In all of these cases, the consumer’s actual account is never charged (at least not on this site). Once the identities are gathered, the suspect makes purchases on *real* merchant sites, or acquires cash advances on the accounts by possibly using the identities on an Internet casino site.
- Hacking and cracking into a merchant database with the intent of stealing credit card accounts is another problem. This is probably the least common form of account takeover on the Internet, because it requires specific technical skills to perform from the outside. The theft of account data from inside a company is more likely and would have the same impact.

There are several more situations including trash bin diving, stealing account information from telephone services, and removal of credit card data from fax machines to name a few.

2.2.3 Fraudulent Transactions

On the Internet, fraudulent transactions are the most common crime committed with stolen identities. Whether a credit card account has been taken over or a stolen identity was used to create a new credit account, these accounts are used to attack e-businesses.

In essence, a fraudulent transaction involves an individual filling out an order form as though they were someone else, the merchant accepting the order, and the shipment of goods or services that the suspect can receive. One key difference from a traditional in-store fraud is that the criminal can "hit" a lot of different merchants and do a lot of damage very fast in the virtual world of the Internet. The suspect doesn’t have to drive between merchants, doesn’t have to risk being identified by a sales clerk, doesn't have to be videotaped by surveillance cameras or doesn’t have to speak to a telephone operator to commit their crime.

Compared to robbing a liquor store, this form of fraud is nearly perfect. The chance of capture is small and the crime is considered a non-violent, white-collar economic crime. While fraud is a crime, the perception of it is significantly different the image of some bad guy poking a gun in the nose of a store clerk. Needless to say, unless the loss is significant, one probably won't see these crimes featured on the nightly news.

3. Prevention

Based on today's legal, cultural, and social conditions, this section describes some prevention methods and best practices. Additionally, it is clear that prevention is currently the only viable approach to resolving the problem of stolen identities being used online since post-loss enforcement and property recovery is difficult and sparsely performed due to the limited number of trained Internet fraud investigators. This section gives the reader a set of best practices to consider that may help reduce the risk of loss.

3.1 Consumer

- ❑ Above all, know who and why you are giving information to someone or some entity on the Net.
- ❑ Only provide the minimum amount of information to complete a transaction.
- ❑ Check your credit history and credit report occasionally.
- ❑ Contact authorities if you suspect your identity has been taken. For US consumers, call the Federal Trade Commission (FTC) at 1-877-ID-THEFT, report complaints to the Internet Fraud Complaint Center run by the Federal Bureau of Investigation (FBI) at http://www.ifccfbi.gov, and make a report to your local police.
- ❑ Use only one credit card online and monitor the statement each month, checking for even small discrepancies.
- ❑ Be careful with programs where merchants or entities want to remember your purchase data and allow you to use it again. This means the merchant has to have significant systems and technology to protect this information.
- ❑ Be careful with the use of server-based payment wallets that store your information on someone else's system. Consider the time-value of your credit card account and how long that information has to be securely stored. This service may have to keep that account data secure for 8 years of more.
- ❑ Check merchant privacy policies. Only shop with merchants who have published privacy policies that you agree with. Remember that privacy policies vary widely. A policy that states "This site gives your information to anyone who asks," is just as valid as a policy that states, "This sites never provides information to anyone." Do not assume that just because a site has a privacy policy link that your expectations will be met. The only way to know is to read the policy and make a decision.
- ❑ Only do business with Internet companies that use a secure form to capture private information (such as an account number or credit card number). For example, you can tell if the form is secure if the lock or key symbol on your browser status bar is solid instead of broken or open.
- ❑ Know whom you are giving personal data to and how they intend to use it. To help understand whom you're doing business with, click on either the solid lock or key symbol in your browser window. This will bring up a screen that gives you information about the merchant from the server certificate. If this certificate was issued by an independent certificate authority, they did some form of due diligence on the business. If someone has cloned a site they will not have such a certificate. Or, if the certificate name is someone else, you will know to be suspicious.
- ❑ Avoid instant credit offers.
- ❑ Avoid the temptation of purchasing a product from a merchant or through an auction site where the deal looks *too* good. Yes, this means the consumer must use some sound judgement.

3.2 E-Business

- □ Develop and publish a privacy policy.
- □ Follow your privacy policy. And, above all, insure that your employees are trained about the policy.
- □ Monitor the privacy policy and your compliance. To this extent, appoint a security and privacy coordinator for your organization. Make that person's contact information known. Research and respond to any consumer complaints.
- □ Store only data elements that you absolutely need to have. Maintaining a database with purchase and address information is fine to facilitate one-to-one marketing, but maintaining a database of payment information is not needed. Once the payment is completed, this data should be removed.
- □ Verify that the payment system you implement (even when outsourcing) deletes temporary data files with payment records and that the outsourcing entity has strict security and privacy policies as well.
- □ Make certain server log files do not inadvertently store customer payment information.
- □ Compartmentalization of access to payment systems. All employees don't need to have access to databases or payment application software.
- □ Monitor employees who have access to sensitive data or payment systems. Perform spot-checks and verify that they are working within the scope of their jobs.
- □ Immediately report any security breach or loss of computer systems to police.
- □ Only ask customers for information that is absolutely necessary to complete the transaction.

3.3 Service Institutions (especially Internet-based service institutions)

- □ Have and publish a privacy policy, including appointing a consumer privacy coordinator. This person is responsible for implementation of the policy, monitoring and researching any consumer complaints.
- □ Have a security policy that is clearly documented, understood by employees, monitored and modified as appropriate.
- □ Encrypt sensitive data, like credit card account data, in databases. Encrypting uses cryptographic methods to scramble data so that only an authorized application in possession of a special key can read the data.
- □ Manage encryption keys. This includes all key management best practices, including obsolescence of keys and re-issuance of keys.
- □ Use sufficiently large key lengths and strong enough cryptographic technology to insure integrity of private data over life of storage.
- □ Understand life of storage of sensitive data and implement electronic shredding policy.
- □ Verify that backup tapes and other off-line systems correctly store sensitive data.
- □ Monitor access to sensitive information.
- □ Constant review of security policy compliance and periodic review and update of procedures.
- □ Careful observation of internal staff capable of handling sensitive data.
- □ Management of terminating employees.

3.4 Information and Marketing Companies

This area includes data miners, *spammers*, information brokers and market research companies.

- ❑ As with the E-Business section, businesses in this area must have a strong privacy policy. If your policy is to use, abuse, share or sell information, publish this as your policy and follow it.
- ❑ Designate a privacy coordinator. This person is responsible for implementation of the policy, monitoring and researching any complaints.
- ❑ Remember that companies must adhere to the policies and agreement between the initial business collecting the data and the end-user.
- ❑ Make certain to provide a mechanism for end-users to challenge the use of information by one of these companies. To this extent, some of US companies may be governed by the Fair Credit Reporting Act (FCRA). Those not covered by the FCRA should have some mechanism to collect, investigate and resolve end-user complaints.
- ❑ Encrypt sensitive data, like credit card account data, in databases. Better yet, avoid using or storing this information. If a marketing company receives a data set containing sensitive consumer information, this data should be destroyed or electronically shredded. The sender of the information should be notified not to send such data in the future. A certificate of destruction should be kept on record to respond to any potential challenge by a consumer.
- ❑ Manage encryption keys. This includes all key management best practices, including obsolescence of keys and re-issuance of keys.
- ❑ If you must store private data, use sufficiently large key lengths to insure integrity of private data over life of storage.
- ❑ Understand life of storage of sensitive data and implement electronic shredding policy.
- ❑ Verify that backup tapes and other off-line systems correctly store sensitive data.
- ❑ Monitor access to sensitive information.
- ❑ Constantly review security policy compliance and periodically review and update procedures.
- ❑ Carefully observe internal staff handling sensitive data.
- ❑ Properly manage terminating employees.

4. Role of Privacy and Security Policies

Privacy and security policies are important steps in protecting consumers from fraud. Companies should have both privacy and security policies to ensure that there are clear rules to which the company and its employees adhere and that consumers understand the operations of a company with which they choose to do business.

Developing a good privacy policy helps a company examine and analyze its own information practices. Many times companies find that in the process of writing and implementing a privacy policy they may be able to change how the firm collects data, what data is collected, how data is stored or used and where consumer choices can be introduced. By taking a comprehensive approach to writing a privacy policy, companies are forced to examine their own practices and, in the process, may in fact modify their current practices to be more consumer-friendly. The result is generally a raised awareness within a company about consumer privacy concerns, a greater sensitivity to consumer preferences about personal data and greater attention to the security of personally identifiable data. For businesses, there is the additional benefit of improved consumer perceptions as companies work with their customers to identify their consumers concerns and preferences about privacy.

For consumers, the benefit is a greater sense of trust and security when doing business online or providing personally identifiable information to Web sites. Individuals are far more likely to share information if they are confident that a company respects their preferences, allows them to make some choices about how their personal information is shared and gives them the opportunity at any point to opt-out of further data collection or use.

Governments also benefit from widespread use of privacy policies. Self-regulation is an effective mechanism in protecting privacy of online consumers when combined with a strong, effective and clear underlying legal structure. By adopting the approach that the U.S. has to date pursued, governments do not have to be concerned that outdated privacy laws will retard the growth of electronic commerce while still being able to protect the privacy of their online consumers. The market is a powerful force, and as consumers begin to express their preferences towards data usage, businesses quickly comply. Those that do not, or those that betray their consumers' trust, will quickly be put out of business in a dynamic and interactive environment like the Internet.

4.1 Privacy Policy

4.1.1 Role

A privacy policy should accomplish three things: 1) explain a company's information practices; 2) identify choices that a consumer may have in how his or her data is collected, used or shared; and 3) establish a mechanism for receiving, investigating and resolving complaints.

4.1.2 Typical Example

Some privacy policies are very simple; some are far more complex. Policies vary widely from company to company, and privacy policies reflect that differentiation. Visit http://www.siia.net/govt/toolkit.asp or http://www.truste.com for examples of privacy policies and more information.

4.1.3 Responsibilities

Companies have a responsibility to develop a privacy policy that fully discloses their information practices, communicates these practices in easy-to-understand language to consumers, and clearly identifies what choices a consumer may make about the use of his or her information. Companies also have an obligation to fully implement their privacy policies and ensure that employees fully understand the policy and to work with a third-party group to ensure compliance.

Consumers have a responsibility to look for privacy policies when online. Whether an individual is shopping or just browsing, everyone should read privacy policies and think carefully before sharing any information online with any site. If customers are not comfortable with the privacy policy of a given site, he or she should conduct their business everywhere.

4.2 Security Policy

4.2.1 Role

The role of a security policy is to ensure that a company has established procedures that govern how it secures any sensitive or personal information it may collect. While companies may in fact have a comprehensive approach to security without such a policy, a security policy is an excellent addition to any company's operating procedures. Such an approach provides direction to staff, underscores the company's commitment to solid security practices and is reassuring to consumers.

A security policy should also identify for a company what types of data will be protected and in what manner. For example, will network access be protected only by password? Will all e-mail be encrypted or only messages marked confidential? Will access to sensitive data be available to remote users? The development of such a policy will help a company identify its core assets, identify what types of data must be protected and in what matter as well as which technologies and standards will be deployed throughout the company.

4.2.2 Technologies and Application

The following is a list of technologies that should or may be used in the security of data.

- ❑ Cryptography
- ❑ Certification and Authentication
- ❑ Single-Sign On Technologies and their role in monitoring network assets access
- ❑ Human / individual authentication technology
- ❑ Biometric technologies
- ❑ Anonymity tools

4.2.3 Responsibilities

Companies have a responsibility to develop a security policy that is comprehensive, takes into account all of the types of data stored on and access allowed to its network and leverages technology effectively to protect its assets. The company is also responsible for fully implementing the policy and access policy that fully discloses their information practices, communicates these practices in easy-to-understand language to consumers, and clearly identifies what choices a consumer may make about the use of his or her information. Companies also have an obligation to fully implement their security policies and ensure that employees fully understand the policy and to work with a third-party group to ensure compliance.

4.3 Response to a Breach

Companies need to have clear policies about what to do in cases of a breach. In many cases, what a company does in the time immediately following a breach is critically important. Companies must make sure that they not only shut down future attacks but also make sure that they do not destroy any evidence that may potentially help identify the source of the breach. Companies who have experienced a disclosure of personal information may be under some obligation to notify their customers.

5. Government Action and Public Policy

This section describes current public policy and areas of possible future attention.

5.1 Privacy Legislation

Currently, there is a wide range of privacy legislation pending in Congress. Some of this legislation would be quite restrictive when compared to current practices; other efforts are more targeted at particular types of information. It is unclear whether Congress will step in to regulate customer data this year, especially given the recent conclusion of the safe harbor agreements with the European Union.

5.1.1 Review of Current Public Information

There is a wide variety of information available to the public. This information can be categorized into three different areas. *Public records* include the numerous records, files, databases, indices and other data maintained by local, state and the federal government. These records, which are generally open for public inspection, include driver's license information, real estate records, business records, some professional certifications and licensing data and other types of data collected by an official entity.

Publicly available information includes data that is available to the general public through non-government entities, such as phone books, classified ads and newspaper reports. Finally, *open-source information* is a term that covers a wide variety of information that is generally available to the public, including newspaper archives, magazines, and other periodicals.

Currently, Congress is considering limiting the amount of information that it collects from individuals, especially in the area of driver's licenses and vehicle information.

5.1.2 Review of Current Policies

Currently, there are few laws that govern the use of personally identifiable information. While medical, financial, credit and academic records are generally well-protected by statute and can only be released with the permission of the data subject, other data – including social security numbers, home addresses and other personal information – are not so restricted. Given the rise in identify theft crimes in recent years, Congress is considering whether new legislation is necessary to directly address this growing problem. There are numerous bills currently pending that make identity theft a crime. While it is unlikely that any of these bills will pass this year, their introduction has opened the discussion in Congress about the best way to combat identify theft.

5.2 Safe Harbor

5.2.1 Complete Existing Work

The Safe Harbor negotiations with the European Union (EU) seem to have reached a successful conclusion. The Department of Commerce hopes to sign formal letters with the EU in June 2000. Under the Safe Harbor provisions, US companies will be required to provide notice, disclosure, choice and access to customer information, in addition to a number of specific provisions for particular industries (such as head hunters, financial data and others). Companies will be required to self-certify annually that they are in compliance with the provisions of the Safe Harbor. A master list of companies that have self-certified will be maintained by the Department of Commerce, but the DOC will not "verify" compliance. Companies that are found to have violated the Safe Harbor process may be subject to U.S. enforcement and may have their data flows from the EU suspended.

5.2.2 Establish Provision for Fraud and Identity Detection

5.2.3 Extradition and Prosecution

- ❑ Establish provision for prosecution and extradition of individuals discovered using the identity of another.
- ❑ Establish provision for criminal prosecution and extradition of individuals discovered in possession of multiple identities.
- ❑ Establish provision whereby US entity or any foreign entity in a member country will permit the civil prosecution of company found to have mishandled or failed to correctly store private information.

5.3 Security and Protection of Information

- ❑ Establish criminal penalties for companies who knowingly mishandle or fail to protect private consumer information.
- ❑ Establish civil penalties equal to 10 times damage to consumer for loss of single private data record

5.4 Response to Victim

5.4.1 Reporting and Investigation

- ❑ In the event of a loss as a result of either identity theft or fraud, complaints can be registered to the US Department of Justice, FBI through the Internet Fraud Complaint Center Web site at http://www.ifccfbi.gov.
- ❑ Rapid investigation

5.4.2 New Identity

Coordinate notification and issuance of new identity documents. Consider state, local, and other uses.

6. Analysis of Case

The case of Lt. Colonel James Jones will be used for this analysis.

6.1 General Analysis of Opening Case

The identifying information, specifically the Social Security Number (SSN), was acquired by a criminal from a document published on the public Internet. This document was a part of the US Congressional record in the public domain. Beyond the fact that there is little reason for the complete SSN to be included in the record, this is a publicly available document.

6.2 Commercial Issues

6.2.1 General Business Practice Issues

There are a few issues of interest in this case:

1. Instant credit was approved for the presenter of the identity. Even though the credit line was small, it suggests that online verification of presented information may not be sufficiently strong to verify the identity presented. Some online verification of information beyond the presence of a SSN is needed.
2. Follow up credit verification needs to take into account physical address information as well as all credit bureau header information. If the information seems inconsistent with other data (especially if there are other active credit accounts where the address has not changed), this should raise suspicions.
3. Use of Internet predictive variables to assist in identification and credit scoring is important. If the same set of Internet environment values have opened other accounts using other names, this should highlight a potential problem.
4. Follow-up with applicant via telephone call and verification that telephone number presented is consistent with addresses and Internet environment variables.

6.2.2 Issues Related to Privacy

No apparent business-to-consumer privacy issues are present in this case.

6.2.3 Issues Related to Security

No apparent security issues or breaches of security are apparent in this case.

6.2.4 Issues Related to Databases

Do database systems used to evaluate credit applications store sufficient information about Internet predictive variables and their historical use in order to help identify potential problem? If such a system and information for a system is not readily available, this sort of service can be sourced from an Internet fraud detection company. This type of information needs to be used at both the credit issuance and shopping transactions to detect a potential problem.

6.2.5 Issues Related to Use of Stolen Identity

The Web site where the identity was presented to issue the online credit account (in the case of Lt. Col. Jones, a revolving credit card account), should have performed a detailed analysis of the presented identity and scored the information presented along with prior transactional information, credit bureau information, and specific geographic information, and Internet predictive variables.

Had a system been employed that generated a risk score based on the information presented, data from static databases (like a credit bureau) and data about the Internet connection, the system may have detected (1) the address change in that the new billing address did not match any pre-existing information; (2) a potential miss-match of the address in a situation that the billing address in the credit bureau record was being used to post existing payments; (3) possible Internet velocity issues; and (4) identity changes related to the Internet environment data.

6.3 Public Policy Issues

6.3.1 Issues Related to Privacy

The republication of private information even though that private information may exist in the public domain and be readily accessible may be considered unethical. The entity that republished the congressional record was committing no crime as the content was in the public domain. The problem was that private information was republished in an efficient medium where hackers and legitimate browsers could acquire the data. Jones' SSN number should have been masked from the document.

The same privacy standards and practices required of US businesses needs to be extended to Government entities as well.

6.3.2 Issues Related to Security

The protection of SSN data, even though this is listed as a “military serial number”, must be implemented. This information should be masked or can even be represented as a hashed value. A hash value is the use of a computer algorithm to one-way encrypt (scramble) a data value so that the resulting value is unique yet unrecoverable. In essence, this would have created a surrogate value for an SSN number that could not be recognized by any credit issuing company.

6.3.3 Issues Related to Response

It is unclear what response the involved Government agencies will take to insure this type of security breach will not occur in the future.

7. Conclusion

The issues related to identity theft require a multi-faceted response that involves eBusinesses, consumer education, and public policy. Only through this level of cooperation and action will the issues and victims caused by identity theft be addressed. The response by each is summarized and all were presented earlier in this paper:

- ❑ Business (or any entity on the Net) must prevent the illicit use of an identity and protect private information. Other types of eBusiness, like service bureaus and marketing companies, need to take steps to assure that private information is correctly stored and unavailable for abuse. Additionally, eBusinesses involved with the issuance of online credit or online revolving credit, need to take steps that verify information and use technology to reduce the ability of a stolen identity being used to create a new account.
- ❑ Consumers can’t expect that some “big brother” will watch out for their privacy or verify that information is not used without their authorization. Further, consumers need to know where to report identity theft issues, what action eBusinesses can take, and to what extent business will protect their privacy.
- ❑ Governments need to provide mechanisms for consumers to report crimes to the appropriate law enforcement agencies; provide training and education to law enforcement; and, capture statistical information about the use and abuse of stolen identities and make this information available to both public and private sector groups.

About SIIA

The Software & Information Industry Association is the principal trade association for the software and digital content industry. SIIA provides global services in government relations, business development, corporate education and intellectual property protection to the leading companies that are setting the pace for the digital age. Through the efforts SIIA is building the digital economy. For more information about SIIA and its programs, visit our Web site at www.siia.net.

The Software & Information Industry Association
1730 M St. NW, Suite 700
Washington, DC 20036-4510
USA
Telephone: +1.202.452.1600
Fax: +1.202.223.8756