Global Information Assurance Certification Paper

IDENTITY THEFT: WHAT TO DO IN THE EVENT YOUR IDENTITY IS STOLEN

Ken Reincke

GIAC Security Essentials Certification (GSEC)

Practical Assignment
Version 1.4c – Option 1

March 12, 2005

ABSTRACT

According to the Federal Trade Commission, Identity Theft is the fastest growing crime of our time. Much has been written regarding the best steps to safeguard against becoming a victim and that aspect of the identity theft problem is not addressed here. Instead, we will focus on mitigation and recovery after the fact. In many respects, industry, consumer agencies and law enforcement have been slow to respond to this threat; this has contributed to the problem. We will find that even with great diligence on an individual's part, personal information is sometimes released to others due to lapses on the part of other legitimate users of such information.

The question that must be addressed then, is what legal protections are there for the Identity Theft victim and how does one mitigate the damage and recover from fraudulent use of one's identity? We will first briefly review existing laws that establish the rights of the victim and the responsibilities of creditors and the credit industry. After establishing this legislative baseline, the specific "mitigation and recovery" actions an identify theft victim should take are discussed in detail. This discussion will then review recent developments intended to strengthen the ability of victims to repair their credit histories and pending legislation under consideration. Finally, we will conclude with a few comments regarding where the need for future, yet to be introduced, legislation should focus in order to protect the consumer.

Table of Contents

1.0 Introduction

With increasing frequency, individuals like you and I are finding out that someone, somewhere, has assumed our identity and have proceeded well down the road of racking up bills and ruining our credit. In some cases, this happens through no fault of our own. No matter the due diligence we take to protect our own private information, others in a position to know such information are not so careful.

Take the case of Mr. Chip St. Clair of Rochester Hills, MI. Mr. St Clair's own parents began using his Social Security number to open credit card accounts when he was still a teenager. He has spent seven years trying to clear his credit history[1]. Take also the case of ChoicePoint, a data broker boasting a collection of 17 billion public records. The company, duped by criminals, gave up personal information on 145,000 people in 2004[2]. There is no shortage of examples, even SAIC, a government contractor with an information security practice, has fallen victim:

> Some of the nation's most influential former military and intelligence officials have been informed in recent days that they are at risk of identity theft after a break-in at a major government contractor netted computers containing the Social Security numbers and other personal information about tens of thousands of past and present company employees.
>
> The contractor, employee-owned Science Applications International Corp. of San Diego, handles sensitive government contracts, including many in information security. It has a reputation for hiring Washington's most powerful figures when they leave the government, and its payroll has been studded with former secretaries of defense, CIA directors and White House counterterrorism advisers.
>
> Those former officials -- along with the rest of a 45,000-person workforce in which a significant percentage of employees hold government security clearances -- were informed last week that their private information may have been breached and they need to take steps to protect themselves from fraud.[3]

The problem of identity theft is not a problem going away any time soon. The Federal Trade Commission calls this the fastest growing crime of our time. Not only that, but it's a crime that can consume the time of its victims in trying to clear their name. According to the Privacy Rights Clearinghouse, a nonprofit consumer information and advocacy organization, the average amount of time it took before the victim became aware someone was using their identity to obtain credit was 14 months. *The average time it took to clear up their credit records was 2 years.*[4]

It is not the focus of this paper to rehash how to protect yourself from identity theft; Mr. Surber has already addressed that issue[5]. Besides, as noted above, sometimes even when doing all you can, identity theft still happens. Instead,

this paper will expand on Mr. Surber's comments on mitigation and recovery in the event a criminal is successful in compromising your identity and has proceeded to wreak havoc on your life. We will first quickly review the existing applicable laws, then proceed to discuss actions that should be taken immediately upon discovering compromise of identity and then conclude with a look at pending legislation addressing the issue of identity theft.

2.0 Existing Laws Addressing Identity Theft

Before addressing what to do in the event of identity theft, it is instructive to understand the laws that direct such actions. When armed with a good knowledge of your legal rights, you are in a better position to insist that a reporting agency or bill collector comply with legal requirements. The descriptions presented below are not intended to fully summarize each Act but instead focus on those aspects that pertain to Identity Theft. In some cases these Acts address a much broader subject in total.

2.1 Identity Theft and Assumption Deterrence Act

The Identity Theft and Assumption Deterrence Act of 1998 – was enacted by congress in October 1998 specifically to address the issue of identity theft. The Act amends Federal law to make it illegal for anyone to "knowingly transfer or use, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law"[6].

In general terms, the Act:

1) Makes identity theft a criminal act. It specifies penalties for violations involving fraud associated with another person's means of identification.

2) Requires that the Federal Trade Commission establish procedures to:

   (a) log and acknowledge the receipt of complaints by individuals having reason to believe that one or more of their means of identification have been assumed, stolen, or otherwise unlawfully acquired;

   (b) provide informational materials to such individuals; and

   (c) refer such complaints to the appropriate entities, including national consumer reporting agencies and law enforcement agencies.

The Identity Theft and Assumption Deterrence Act actually covers numerous other related issues but items 1) and 2) above capture the crux of the Act for our purposes. Prior to enactment, acts of identity theft could be prosecuted to the extent actual fraud or, say, monetary or property theft was involved but it wasn't in and of itself illegal to assume another's identity.

The Act also served to require the Federal Trade Commission to provide victim assistance which was almost entirely lacking in the 1998 time frame.

2.2 Fair Credit Reporting Act

The Fair Credit Reporting Act (FCRA)[7,8] is a comprehensive provision addressing far-reaching requirements related to credit, many of which are not directly associated with identity theft. However, the aspects of the FCRA that pertain to identity theft are very important towards mitigating the effects of fraud:

1) It is of utmost importance to monitor your credit report. Your credit score is probably the single most important factor in maintaining the ability to obtain credit and also affecting the extent to which more favorable terms will be offered. The FCRA addresses this by requiring credit reporting agencies to provide you a free copy of your credit report on an annual basis.

2) FCRA gives you the right to notify potential creditors that you may be the victim of identity theft. You can place a fraud alert in your file by notifying the three main consumer reporting agencies:

   - www.equifax.com
   - www.experian.com
   - www.transunion.com

3) If requested in writing, a creditor or other business must give you copies of applications or other business records relating to any transactions resulting from the theft of your identity.

4) If contacted by a debt collector, you have the right to request sufficient information to ascertain the basis for the purported debt.

5) You can request that consumer reporting agencies block from your report any information resulting from identity theft. An important benefit here is that once a debt resulting from ID theft

has been blocked, the creditor may not sell, transfer or place the debt for collection.

2.3 Credit Repair Organizations Act

The increasing incidence of identity theft and associated fraud has provided a new market for credit repair businesses and related organizations. As a result, in keeping with good old American ingenuity, the incidence of fraud in credit repair has also risen. Congress responded by passing the Credit Repair Organizations Act (CROA)[9]. The CROA provides numerous protections to both creditors and the consumer. In general, no person may:

1) make any statement upon which, with the exercise of reasonable care, should be known by the credit repair organization to be untrue or misleading with respect to any consumer's credit standing.

2) make any attempts (or counseling) to alter or conceal adverse information regarding a consumer's credit record.

3) make any untrue or misleading representations of the services provided by the credit repair organization.

4) Engage in any activities or practices that results in the commission, or attempt to commit fraud, in connection with the offering of services of the credit repair organization.

Additionally, credit repair organizations are prohibited from charging for any services before such services are performed and must provide the consumer with a specified disclosure statement. The Act also requires that credit repair contracts must be written and specifies certain requirements for such contracts (including a 3 day right to cancel privilege).

3.0 Identity Theft: Mitigation and Recovery

The horse is out of the barn. Although you have taken precautionary measures, you find out someone has obtained credit in your name. The new car loan you applied for was denied and all the sudden bill collectors are calling demanding payment on accounts you know nothing about. What do you do now?

3.1 Credit Bureaus

The first step is to immediately file reports with the three major credit bureaus (see 2.2.2 above). Be sure and ask that a "fraud alert" be placed in your file. You should also ask that a copy of your credit report be

provided to you immediately. Upon receipt of the credit report review the report to identify any accounts which were opened fraudulently. Immediately report back to the credit bureau, in writing, any accounts or inaccurate information that you note.

There are two types of fraud alerts, initial and extended. An initial report stays on your credit report for 90 days. You should file an initial report even if fraud has not yet occurred but the potential exists such as your wallet or purse being lost or stolen. You can change your alert to an extended alert upon filing an "identity theft affidavit" (discussed in section 3.2 below). The extended alert stays on your record for seven years. One of the main benefits of an extended alert is that the credit bureaus will remove your name from pre-screened credit offers for five years.

3.2 File a Complaint with the Federal Trade Commission

As noted in Section 2.1, the FTC is required to maintain a database of fraudulent activity. This database is made available to law enforcement officials and filing a report provides additional information that may lead to the perpetrators arrest. You can file an online complaint at www.consumer.gov/idtheft.

The FTC also makes available an ID Theft Affidavit[10]. The ID Theft Affidavit was developed by a group of credit grantors, consumer advocates, and attorneys at the Federal Trade Commission. The affidavit makes it easier for fraud victims to report information. The affidavit should be provided anywhere a new account was opened in your name. The information contained in the affidavit will enable creditors to investigate the fraud and decide the outcome of your claim. As a side note, you should know that while many companies accept this affidavit, not all do.

3.3 File a Police Report

Not all jurisdictions will take a report on identity theft but this is changing rapidly due to the increasing number of such crimes. The primary purpose for filing such report is that many banks and creditors will require it to support your claim of fraud.

3.4 Creditors

It is important to immediately contact any creditors where accounts were fraudulently opened in your name. Your credit report will identify such accounts. The ID Theft Affidavit will provide the creditor the necessary information to support your claim. Likewise, it is a good idea to ask existing creditors for new account numbers if there is any possibility such accounts were compromised.

3.5 Social Security Number

If you suspect another individual has obtained your social security number you should immediately report it to the Social Security Administration. The SSA can be contacted at:

www.socialsecuirty.gov or 1-800-772-1213

The Social Security Administration will assist you in obtaining a replacement card if your Social Security card was lost or stolen, provide a new Social Security number in certain circumstances, and help to correct your earnings records.

3.6 Overcoming the Emotional Impact

For the most part, available resources for the identity theft victim focus on the administrative steps or "paperwork" aspects of recovery. Even after following steps such as those related above, most victim accounts tell a story of a long and involved process. Many times fraudulent charges are dropped from a credit report only to appear again later, triggering the recovery process once again. It is not unusual for a victim to become overwhelmed by the feeling of helplessness, anger, betrayal and even embarrassment.

Linda Foley, writing for the Identity Theft Resource Center[11] recommends a multi-factor process for dealing with the emotional aspects of identity theft:

3.6.1 The Moment of Discovery

Be prepared for a roller coaster ride of emotions ranging from denial, to rage to "why me"? You may also become frustrated with the inefficiencies of the governmental organizations and the facelessness of the creditor organizations. Try to be patient with those whose job it is to help.

3.6.2 Start the Healing Process

Recognize that your feelings are valid and normal. Don't berate yourself or waste time being embarrassed. As pointed out above, many times it's not your fault.

3.6.3 Overcoming Feelings of Helplessness

You can't change what has happened but you can control your reaction. Refuse to give in mentally and allow the perpetrator to dictate your actions with irrational behavior. Stay organized,

maintain a record of who you talk to, letters sent, etc. Don't let the situation become all-consuming. Focus on your accomplishments in life both in the past and currently.

3.6.4 Take Time For Yourself

Recovering from identity theft can be time consuming. Reward yourself with time off to relax and exercise.

3.6.5 Consider Professional Help

If you find it difficult to function normally, lose interest in things you used to enjoy and feel unable to cope, its time to talk to a trained professional. It's important also to not wait until its too late. This is a very stressful time and it is not necessary to go it alone.

The above is just a brief summary of Ms. Foley's recommendations. Please see the referenced article for more details.

4.0 Pending Legislation and Recent Developments

So far we have looked at the existing laws addressing identity theft and the consumer protections they provide. We have also addressed the steps that you should take in the event you are a victim of identity theft. Unfortunately, identity theft victims do not believe the existing laws go far enough. In this section we will look at pending legislation intended to further strengthen our ability to fight back against ID theft. Following is a summary of recent State level developments and federal legislation pending as of March 2005. Obviously, because this section addresses pending legislation, the final form of any such legislation is subject to change.

4.1 Senate Bill 29 – Social Security Number Misuse Prevention Act

Senate Bill 29 (S.29)[12] has been introduced into the 109th congress with the title "Social Security Number Misuse Prevention Act". The bill committee summarizes it's findings that Social Security numbers aid fraud, and because the federal government requires every one to have a Social Security number, it is the federal government's responsibility to take action to provide individuals with protection from the display, sale and purchase of social security numbers.

The bill provides the following protections:

1) Limitation on Display- No person (with some exceptions) may display any individual's Social Security number to the general public without the affirmatively expressed consent of the individual.

2) Limitation on Sale or Purchase- Except as otherwise provided in this section, no person may sell or purchase any individual's Social Security number without the affirmatively expressed consent of the individual. In order for consent to exist, the person displaying or seeking to display, selling or attempting to sell, or purchasing or attempting to purchase, an individual's Social Security number shall--

(a) inform the individual of the general purpose for which the number will be used, the types of persons to whom the number may be available, and the scope of transactions permitted by the consent; and

(b) obtain the affirmatively expressed consent (electronically or in writing) of the individual.

3) In General, a commercial entity may not require an individual to provide the individual's Social Security number when purchasing a commercial good or service or deny an individual the good or service for refusing to provide that number except--

(1) for any purpose relating to--

(a) obtaining a consumer report for any purpose permitted under the Fair Credit Reporting Act;

(b) a background check of the individual conducted by a landlord, lessor, employer, voluntary service agency, or other entity as determined by the Attorney General;

(c) law enforcement; or

(d) a Federal, State, or local law requirement; or

(2) if the Social Security number is necessary to verify the identity of the consumer to effect, administer, or enforce the specific transaction requested or authorized by the consumer, or to prevent fraud.

This bill will have implications on the display by government entities of public records but the details are yet to be worked out.

The bill also levies certain criminal penalties for violations of the Act.

4.2 Senate Bill 116 – Privacy Act of 2005

Senate Bill 116 (S.116)[13] has been introduced into the 109th congress with the title "Privacy Act of 2005". Senate Bill 116 addresses the same type issues as SB.29 but in a much broader sense. Rather than limiting

the disclosure of information to social security numbers as SB.29 does, SB.116 makes it unlawful for a commercial entity to collect and disclose "personally identifiable information" to any non-affiliated third party for marketing purposes or to sell such information (without requisite prior authorization).

Prior to release of any such information, the bill requires that:

> (1) notice be given to the individual to whom the information relates; and
>
> (2) an opportunity be given for such individual to restrict the disclosure or sale of such information.

Interestingly SB.116 also provides for the right to "opt-out" of certain marketing activities:

> (1) OPPORTUNITY TO OPT-OUT OF SALE OR MARKETING- The opportunity provided to limit the sale of personally identifiable information to nonaffiliated third parties or the disclosure of such information for marketing purposes, shall be easy to use, accessible and available in the medium the information is collected, or in a medium approved by the individual.
>
> (2) DURATION OF LIMITATION- An individual's limitation on the sale or marketing of personally identifiable information shall be considered permanent, unless otherwise specified by the individual.
>
> (3) REVOCATION OF CONSENT- After an individual grants consent to the use of that individual's personally identifiable information, the individual may revoke the consent at any time, except to the extent that the commercial entity has taken action in reliance thereon. The commercial entity shall provide the individual an opportunity to revoke consent that is easy to use, accessible, and available in the medium the information was or is collected.
>
> (4) NOT APPLICABLE- This section shall not apply to disclosure of personally identifiable information--
>
> > (a) that is necessary to facilitate a transaction specifically requested by the consumer;
> >
> > (b) is used for the sole purpose of facilitating this transaction; and
> >
> > (c) in which the entity receiving or obtaining such information is limited, by contract, to use such formation for the purpose of completing the transaction.

As with SB.29, criminal penalties are imposed and there are implications to disclosure of public records that are yet to be worked out.

4.3 House Resolution 220 – Identity Theft Prevention Act of 2005

House Resolution 220 (H.R. 220)[14] has been introduced into the 109th congress with the title "Identity Theft Protection Act of 2005". H.R. 220 contains provisions under certain circumstances for the re-issuance of social security numbers, limitations on the IRS's use of social security numbers and a prohibition against multiple agencies of the federal government from using the social security number as an identifying number and a prohibition against federal agencies from mandating a uniform standard for identification of individuals that is required to be used by any other federal agency.

4.4 State Initiatives

In addition to federal laws, many states are also passing legislation addressing the issue of identity theft. For example, Michigan has recently passed a package of 11 laws protecting personal information[1]. Included in these new laws are new penalties and prohibitions dealing with identity theft.

One of the new laws sets the maximum penalty for identity theft at five years in prison and a $25,000 fine. Other new laws help victims by allowing them to get a police report on their case and by banning companies from denying them credit. In addition, retailers cannot display more than the last four digits of a credit card account number on a sales receipt or mailing under one of the laws. Another prohibits businesses, schools, local governments and other organizations from using more than four sequential digits of a person's Social Security number as an account or ID number. The new laws will also provide prosecutors more flexibility to pursue identity theft crimes. They now have six years to prosecute identity theft from the time it happens or the offender is identified. The old statute of limitations ran out six years after the crime occurred.

Another interesting trend is the availability of Identity Theft Passports[15]:

> Victims of identity theft in Virginia, Ohio and now Arkansas have a way to make the experience a little less painful, and to get their good names back a bit sooner.
>
> Identity theft passports, which carry the photo and name of the victim and are issued by the state, can help victims prove to creditors, police and their banks that they've had their identities stolen and aren't responsible for crimes committed with their identity.
>
> One victim, Elizabeth Price of Little Rock, ended up in jail after her

> driver's license was used to cash a $900 check. Police didn't know she was a victim of identity theft — the No. 1 fraud complaint across the nation last year — and Price had no way to prove it.
>
> To get a passport, a victim first files a police report, sends it to the attorney general, who, after verifying the identify theft, issues the passport.

Clearly the trend is for the problem of identity theft to be addressed at the State level in addition to legislation implemented at the Federal level.

5.0 What Next?

It is important to question whether or not these recent developments and new legislation goes far enough. After all, the reason there is so much identity theft is because it is easy and rewarding for the criminal.

Anyone with a mail box realizes how competitive the credit industry is. Obviously, credit companies are able to absorb the fraud and still make money. Meanwhile, identity theft victim's lives are in a shambles. According to MSN[16] credit issuers engage in very sloppy practices. Credit applications are approved with incorrect names, addresses, social security numbers, etc. These practices enable the thief to get credit approved in another's name without having accurate information. Even more amazing is that many creditors ignore fraud alerts placed on accounts. Lenders claim that it is less expensive (for them, at least) to deal with the fraud rather than verify every credit application.

This situation will continue until the pain threshold for the creditors is raised to a sufficient level. MSN claims that business lobbies have so far defeated any such measures. This situation will not change until our representatives hear from enough of us.

6.0 Conclusion

The overriding theme evident in determining how to respond to identity theft is that government, businesses and individuals are all playing catch-up in figuring out how to deal with this phenomena. The criminal element is unquestionably ahead of the curve. It seems in many respects that industry and consumer agencies have been slow in getting the word out regarding the existence of this threat and how to deal with it.

Obviously the first step is to protect one's self as best as possible. However, as we noted, sometimes even that is not sufficient. If you find that you have become a victim, it is important to file reports with credit bureaus, consumer agencies and law enforcement. Only by taking these actions will you protect your rights and clear your credit standing.

7.0 Bibliography

1) Associated Press. "New laws to better protect against ID theft take effect", Detroit Free Press, February 28, 2005. URL: http://www.freep.com/news/statewire/sw112325_20050228.htm

2) Staff Writer. "Few companies have to tell when identity thieves strike", USA Today, February 27, 2005. URL: http://www.usatoday.com/news/opinion/2005-02-27-consumer-protection-our_x.htm

3) Griff Witte, "Break-In At SAIC Risks ID Theft; Computers Held Personal Data on Employee-Owners", Washington Post, February 12, 2005.

4) Beth Givens, "Identity Theft: The Growing Problem of Wrongful Criminal Records", Privacy Rights Clearinghouse, June 1, 2000. URL: http://www.privacyrights.org/ar/wcr.htm

5) Greg Surber, "Loosing Yourself: Identity Theft in the Digital Age", September 20, 2001, SANS Reading Room. URL: http://www.sans.org/rr/whitepapers/privacy/686.php

6) National Archives and Records Administration, GPO Access, URL: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_public_laws&docid=f:publ318.105.pdf

7) Federal Trade Commission, "Fair Credit Reporting Act". URL: http://www.ftc.gov/os/statutes/fcra.htm

8) Federal Trade Commission, "Fair Credit Reporting Act". URL: www.ftc.gov/bcp/conline/pubs/credit/cdtsummary.pdf

9) Federal Trade Commission, "Credit Repair Organizations Act". URL: http://www.ftc.gov/os/statutes/croa/croa.htm

10) Federal Trade Commission, "Identity Theft Affidavit". URL: http://www.ftc.gov/bcp/conline/pubs/credit/affidavit.pdf

11) Linda Foley, "Identity Theft – Overcoming the Emotional Impact", Identity Theft Resource Center, Inc., Feb 2003. URL: http://www.idtheftcenter.org/vg108.shtml

12) Thomas Legislative Information on the Internet. URL: http://thomas.loc.gov/cgi-bin/query/F?c109:1:./temp/~c1099Kqzvh:e901

13) Thomas Legislative Information on the Internet. URL: http://thomas.loc.gov/cgi-bin/query/D?c109:41:./temp/~c1099ZLCnK::

14) Thomas Legislative Information on the Internet. URL: http://thomas.loc.gov/cgi-bin/query/D?c109:1:./temp/~c1093dRJOc::

15) Fox News, March 04, 2005. URL: http://www.foxnews.com/printer_friendly_story/0,3566,149484,00.html

16) Liz Pulliam Weston, "How Lenders make Identity Theft Easier". URL: http://moneycentral.msn.com/content/banking/financialprivacy/P48173.asp

: