



ISSUE #16 – 2nd Quarter 2006

- Children - Targets of ID Theft
- Workplace Privacy & Security

Children - Targets of ID Theft

Identity thieves are increasingly targeting children for abuse and gain because children have social security numbers that are usually not used or monitored (i.e. children usually do not have credit or a job). Sometimes the thieves are the parents or other relatives. In other cases, it is a stranger knowingly targeting children, due to the likelihood the fraud will not be detected right away. In the past three years, the number of FTC complaints of identity theft involving victims younger than 18 has doubled.

Since children usually have no credit history, many people believe their social security numbers are safe and that fraudulent accounts cannot be opened in the child's name. However, these clean records can be ideal targets for an identity thief.

In reality, all a thief needs is your child's social security number to apply for a new credit card at which point the thief may actually establish some good credit in your child's name. However, establishing good credit allows the thief to obtain higher credit limits, which are eventually 'max'd out' with the purchase of goods and services and then abandoned when the large bills start to arrive. You may discover your child has fraudulent accounts in his/ her name when bills arrive or collectors call. In other cases, you or your child would only find out years later when he/ she starts trying to establish credit, seemingly for the first time, only to find out there is a negative credit history.

To illustrate another example of child identity theft, Identity Fraud, Inc. recently had a case where a young disabled son of a member had his social security number stolen and used for employment and other frauds. When the child was twelve years old, a collector caught up to the child (via his parents). Upon investigating, the thief had used the stolen social security number for six years, while earning an average of \$46,000 per year. After engaging in further frauds, the thief resorted to a different social security number leaving the child (his parents and IFI) to resolve the case.

To make sure your child is not a victim of identity theft, you can follow the same prevention steps recommended to you for fraud prevention. Request copies of your child's credit report from the three main credit reporting agencies (Equifax, Experian, and TransUnion) by calling them at the numbers provided below or by visiting www.annualcreditreport.com. If there is no credit report on file for your child, it is likely that your child is not a victim, but it is a good idea to keep checking as often as you do check for yourself. If there is a credit report in your child's name, contact the credit bureaus and start a dispute process reminding them that your child was a minor at the time the account was opened and that your child is the victim of identity theft. You can also place fraud alerts on your child's credit files to prevent further fraud from occurring.

To request copies of your child's credit report and to place fraud alerts, call:

Equifax: 1-800-525-6285
Experian: 1-888-397-3742
TransUnion: 1-800-680-7289

Because anyone can become a victim of identity theft, both young and old, individuals having great credit or bad credit, it's important to protect yourself and those that are close to you, e.g. children and parents. Identity Fraud, Inc. does provide the Family Plan to protect you, your spouse or domestic partner, and dependents to the age of 23 and provides its 'Family Extension' options to cover parents, grandparents, brothers and/or sisters.

Did you know?

Protect Yourself from Scams

Jury Duty Scam: You receive a call stating you have missed jury duty, yet you never received a notice to appear. The caller may request personal information to verify your identity. Treat these calls as you would any other unsolicited call and don't give any personal information. You can always call the clerk's office and check if you missed jury duty or if you were a victim of a scam.

At Home Job Opportunities/ Cashier's Check Fraud: If it sounds too good to be true, it usually is. In this scam, victims are sent a cashier's check and are requested to cash the check, remit the funds back to the sender, but keep a healthy fee for the services rendered. By the time the financial institution realizes the check was fraudulent, the thief has the money and the victim is held responsible for the full amount of the fraudulent deposit. (Reminder: You are responsible for the funds you deposit!)

Workplace Privacy & Security

If you are like most of us that are still working for a living, you need to consider your workplace environment for privacy and identity theft issues. In respect of identity theft, the prevention practices you should be doing at home are the same prevention practices you should incorporate at work. For example, when you leave your work area, be mindful of leaving your purse or other personal belongings at your work station. If you use the work mail-room to send out personal bills, etc., consider the alternative of dropping them in a post office box outside the office. There are many examples of thefts of personal belongings and mail in the workplace, especially if it's a busy one.



While you look out for your personal effects at work, you also need to consider any work related items that are in your possession. Do you have a company credit card? Do you review the statements? Unfortunately, poor habits or diligence can cost the business considerably if fraud occurs on the business accounts. Individuals and businesses have different protections under law, and businesses remain quite exposed.

Similarly, be familiar with company policies and procedures. You likely have access to sensitive information, which makes your password very valuable. And just like you can fall victim to clever and attractive looking scams at home, the same techniques are used to target the business. When people call or email you, don't necessarily trust them. A call from the I.T. department may not be a call from the I.T. department. Take a name, check their number and call them back.

Other common techniques like shredding sensitive information, having computer security protection, and being aware of your exposures are all important while at work, and in many cases, required by law. In fact, by being observant, you might uncover insider frauds that are occurring. According to the 2005 Computer Security Institute / FBI annual computer crime survey, nearly half of incidents occur from within an organization. Don't hesitate to notify your superiors if you think fraud is occurring and try not to fear retribution, as current "whistleblower" laws help to make sure you are protected.

Privacy

In reality, you have very little privacy or privacy rights at work. Because you are working for your employer and using your employers phones, computers, etc., you will likely have your activity monitored. Indeed, according to the American Management Association and its 2005 survey, 76% of companies surveyed indicate they monitor the web site activity of their employees. Phone calls, emails, web sites, video surveillance, essentially any activity at work can and is being monitored. According to the report, 80% of employers convey to their employees that monitoring (of computers) is being conducted.

While nearly all people desire privacy and believe in the right to privacy, it's difficult to argue with the employer's right to monitor activity and incorporate safeguards to prevent loss. When a simple email message can be spread to the world, slander individuals or groups, and cause liability to the employer, the extent of the potential damage can be catastrophic. Further, any emails you send, web sites you visit or activities you engage are usually maintained in databases that can be referenced in lawsuits against the employer, used to support employee terminations, or other meaningful actions.

To review the AMA survey, please visit http://www.amanet.org/research/pdfs/EMS_summary05.pdf.

In order to protect yourself and your employer, it's important to adhere to the policies and procedures in your workplace. If none exist, it may not be a bad idea to suggest that they are created or to clarify the employers' position. Deviating from good practices can create some worst case loss scenarios, for example, your employer could face serious liability for a slanderous email you send, or copyright infringement for web site materials you copied and distributed without authority. Similarly, you could accidentally expose your password allowing access to sensitive customer information, or you might simply be terminated for visiting an inappropriate web site. The list of exposures is quite long and continues to grow as we use the Internet and electronics in increasing amounts. So remember, be mindful of information privacy and security issues, both yours and others. After all, it is the age we live in now.
