

A Better Way To Prevent Identity Theft

Robert Pinheiro Consulting LLC

bp@bobpinheiro.com

July, 2005

Thanks to a pioneering California law that requires companies in that state to disclose security breaches involving personal information, we are all learning just how vulnerable personal information about us is to being lost or stolen. The news this year has been filled with stories documenting yet another massive hemorrhage of personal information from the computer files of some bank, business, employer, government agency, or other organization that keeps track of our lives. Names, addresses, social security numbers, birth dates, credit card numbers - it's all out there somewhere, stored in databases that thieves seem to be able to tap into with little difficulty. First it was ChoicePoint, the data aggregator that keeps information about virtually all of us in its files. Personal information, including social security numbers of over 145,000 people, was fraudulently obtained by thieves posing as legitimate businesses. Then Bank of America, LexisNexis, DSW Shoe Warehouse, Time Warner, and others told us that personal information was stolen from them as well.

The biggest concern, besides the loss of privacy that accompanies theft of personal information, is the possibility of identity theft. Although the term identity theft is often used loosely to refer to situations ranging from loss of credit card information to stolen passwords and PIN numbers, in its most dangerous form identity theft is what happens when someone opens a new credit account in your name, using little more than knowledge of your name and social security number. You tend to find out about it when the thief stops paying the bills, and the credit grantor somehow manages to find you and demands payment. By that time, of course, your credit rating may be ruined, since the creditor will likely have reported to the credit bureaus that "you" haven't been paying "your" bills.

Identity theft is enabled by an outdated and blatantly false assumption about our personal information. The assumption is that each person's social security number, birthdate, mother's maiden name, etc. is somehow "secret", and is only known by the person to whom the information refers. So, a person presenting information about you when applying for a new account in your name is assumed to be...you!. It wasn't too long ago we were told that the best defense against identity theft was to shred old documents containing personal information. If the thieves can't get the information, they can't steal your identity, right? While shredding sensitive documents is certainly still a good idea, the recent data theft disclosures show just how little control we have over who can gain access to personal information about us. Credit bureaus, for instance, are generally allowed to sell our credit information to anyone who they believe has a legitimate reason to see it. Since access to personal information, especially credit-related information, enables identity theft, politicians are finally realizing that individuals must be given some meaningful control over how this information is used.

One way to allow people to exercise greater control over who sees their personal information, while at the same time helping to prevent identity theft, is to allow individuals to place a "security freeze" on their credit files. A security freeze would prohibit credit bureaus from sharing your credit-related information with anyone else, with a few exceptions such as existing creditors, unless you

specifically allow it to be available. A few states already permit security freezes, and with the widespread fear of identity theft spurred by the recent bad publicity, several more states have security freeze bills pending. With the passage of the Identity Theft Prevention Act (A4001) by both houses of the New Jersey legislature on June 23, 2005, credit bureaus will be required to allow New Jersey residents (on January 1, 2006) to place a security freeze on their credit files.

One of the great success stories of American business is the “miracle of instant credit.” Because credit bureaus such as Equifax, Experian, and Trans Union collect data about our money-management habits, it’s easy for businesses that extend credit to determine who is a good credit risk. The ability to collect this information and use it to determine creditworthiness is a good thing, and is of benefit to consumers. If your credit history is good, you can go into a store and walk out with a new plasma TV without having to pay cash. So although credit-granting businesses are eager to open accounts for new customers, they do want to ensure that the accounts are being opened for people with good credit histories who can pay their bills. To do this, businesses use the personal information provided by the account applicant to pull the credit file on that person, to make sure his or her credit is good. If it looks good, the application is usually successful and a new account is opened.

The problem is, businesses don’t really know if the person wanting to open a new account is truly the person he or she claims to be. This is especially troublesome when making account applications online, because the applicant is not present and cannot show an ID. In most cases, the credit grantor simply uses the personal information provided by the applicant to access a credit file, under the assumption that the applicant is providing their own personal information. But if a security freeze is in place and the applicant is actually an identity thief, the credit bureau won’t provide any credit information, and the business won’t open the account. If it’s really you applying for the account, and you’ve got a security freeze in place, you’d have to first temporarily lift the freeze in order to allow the credit bureau to provide your credit information to the business.

In theory, identity theft could be prevented if there were some foolproof way to verify the identities of those seeking to open new credit accounts, and if credit grantors actually took the pains to verify those identities. Unfortunately, there’s no bulletproof way to prove your identity to someone who doesn’t know you, especially when you’re not physically present. The best that can be done, in many cases, is to ask about information that only you are supposed to know about, such as your social security number, birth date, mother’s maiden name, etc. Identity thieves realize this, of course, which is why stolen personal information is so valuable to them. So while a security freeze doesn’t prevent identity thieves from being able to steal sensitive personal information, it renders such information useless in allowing the thief to open new credit accounts using someone else’s identity. Thieves who steal personal information also often sell the information to other criminals who use it to open new accounts and commit other financial fraud. Often the information thieves will decide how much the information is worth to other crooks by pretending to be a “legitimate” business and accessing the victim’s credit report. The ability to freeze your credit files will prevent this from happening, providing another stumbling block in the way of identity thieves.

The financial services and retail industries have raised objections to security freezes. They say it will make it harder for people to make impulse purchases, and that it will impede the free flow of credit that empowers so much of the American economy. Perhaps. But that may be a tradeoff that

must be made in order for people to be able to prevent identity theft. Individual consumers ought to be allowed to make the choice about freezing their credit files, with the understanding that they will have to lift the freeze temporarily if they themselves wish to open any new credit accounts. The industry points out that security freezes, where they are currently available, are in use by a relatively small number of people. But that is probably because the credit bureaus don't advertise them. And quite frankly, the way that the credit bureaus have implemented security freezes are far from user-friendly. For instance, under the New Jersey law a credit bureau can take up to five days after a request is made before the freeze is put into effect. If the consumer wants to temporarily remove the freeze prior to applying for a new account, the law allows up to three days before the freeze is removed. So someone using a security freeze has to plan ahead if they want to open a new credit account. In New Jersey, credit bureaus cannot charge consumers to place a freeze, although in other states a fee may be charged. Credit bureaus can charge up to \$5 to temporarily remove a security freeze. And since there are three credit bureaus to deal with, that amount may need to be tripled to ensure that a freeze is temporarily lifted from the appropriate credit bureau.

The financial services industry objects further, saying that consumers already have adequate methods to deal with identity theft, and that security freezes would be too burdensome for everyone to deal with. Better to use a credit monitoring service, they say, which is supposed to tell you if there is any change in your credit report. Or you could frequently check your credit report yourself. Everyone in the country is now entitled to one free credit report per year. Both would tip you off if someone has been messing with your credit. Of course, by the time you become aware of a problem, the damage has already been done, and you'll need to spend countless hours cleaning up the mess.

You could also put a "fraud alert" on your credit file. This is supposed to alert would-be credit-grantors who view your file prior to opening an account in your name that possibly the person applying for the account isn't really you. The credit grantor is then supposed to verify the identity of the person applying for the account. In theory, this is not a bad idea. But many times, business eager to grant credit don't bother to do this. Or they don't even notice that the fraud alert is there. And even if they try to verify the person's identity, there are no generally accepted rules and procedures for doing so. Fraud alerts also expire after 90 days, so they must be constantly renewed unless you can prove that you're already an identity theft victim.

Credit bureaus have traditionally sold their products, namely credit information, to businesses that grant credit to consumers and need to know how creditworthy an applicant is. But in recent years, as awareness of identity theft has increased, credit bureaus have begun to provide services directly to individual consumers. Such services include credit scores, enhanced credit reports and analysis, and "identity theft prevention" services that typically include credit report monitoring and notification, combined with some form of insurance. But the ability to freeze your credit file is only available where it is required by law. The credit bureaus do not voluntarily provide this service to consumers. In fact, the credit bureaus actively discourage the use of security freezes, which is not surprising since a freeze impedes the credit bureau's ability to sell a consumer's credit information. For example, in response to a consumer's question about security freezes versus fraud alerts, Experian's website says the following:

“Our experience, and that of many consumers, indicates a file freeze simply doesn't make sense. As a preventative tool, it is simply far too inconvenient, not to mention time consuming and costly to remove the file freeze regularly, especially when you consider you must freeze and unfreeze your credit file at each of the three national credit reporting agencies.”

Experian would rather that consumers to sign up for their credit monitoring service, which doesn't prevent identity theft, but only alerts consumers of suspicious activity on their credit files. And as Experian reminds us in the above quote, security freezes are cumbersome and costly to place and remove. But there is no reason why credit bureaus could not, if they choose to, create an easy-to-use service that would allow consumers to quickly freeze and unfreeze access to their credit information for a nominal subscription fee. Such a service could be made available for use online, or over the phone.

There are a few possible pitfalls to all this, however. A key assumption is that credit-grantors won't go ahead and open new accounts anyway if they can't get access to a credit file. Another is that thieves won't be able to sabotage the process and somehow unfreeze a victim's credit file. Current implementations of security freezes allow individuals to temporarily remove a freeze by providing a PIN or password. So one possible opening for thieves is to attempt to fool people into revealing this information. Most Internet users today are probably familiar with “phishing” emails that purport to come from a bank or other trusted entity, and that seek to get the recipient to part with sensitive information. It's not hard to envision phishing emails that seek to fool people into revealing information needed to lift a security freeze. This same ability to steal PINs and passwords through phishing emails and other methods has enabled thieves to break into online bank accounts. People who engage in online banking transactions know that they must provide a user ID and password to access their accounts online. But banks are under a certain amount of pressure from the Federal Deposit Insurance Corporation to beef up online banking security by adding another layer of protection, in addition to passwords. Although this second authentication factor could take several forms, one widespread method in use for high-end corporate customers is a physical “token” that generates a different passcode every 60 seconds. If banks begin adopting stronger forms of identity authentication for access to online bank accounts, these same tokens could be leveraged for use in protecting security freezes.

Although no security measure is perfect, security freezes are a step in the right direction for preventing identity theft. As more states begin to enact security freeze laws, the financial services industry will hopefully streamline the process and create a system that allows individuals to easily freeze and unfreeze their credit files. If doing so can significantly reduce identity theft, the effort will be worth it.