

SmartGuard Newsletter

Data Security Breach

A Never Ending Tool for Identity Thieves

Has your personal information ever been stolen during a data security breach? Are you sure? Prior to rash of well publicized incidents beginning in 2005 (Choice Point, Lexis/Nexus, Ameritrade and others) that have brought the issue to the forefront of both our minds and those of our legislators, security breaches were rarely reported and victims often went un-notified. Because so many of us are unaware that our personal information has been compromised, we aren't actively taking the steps necessary to protect our identity.

Fortunately, most states now have laws and guidelines in place that require companies/institutions to notify consumers when their personal information has been compromised, but just knowing your information has been stolen won't keep your identity from being assumed. Without consistently monitoring the use of your personal information, these security breaches can create long-term problems, both financial and non-financial. Big problems.

As a result of a data breach, identity thieves essentially "hit the jackpot", hacking into and stealing large databases of consumers personal information that can ultimately be used to assume a victim's identity. In the last two years alone, over 100 million consumers have had their personal information compromised during a security breach. Sometimes attempts to use the information will come quickly, but more often this information will be warehoused or sold for future use.

When the criminal decides it's time to dip into his database and assume your identity the first thing he will likely do is attempt to change the address associated with your personal information. If successful, he can take advantage of your credit and employment history, opening new accounts you will be responsible for paying, obtaining jobs that leave you on the hook for income tax, and even committing sometimes violent crimes using your identity meaning you could be the one sitting in jail until the situation is straightened out.

It takes the typical identity theft victim over 350 hours and 44 months to rectify the situation. Victims may endure un-reimbursable costs, persistent hassle and permanent damage to their credit.

With the seemingly endless internal and external opportunity (hacking, lost laptops, stealing file folders, internet, email, spyware, etc.) for criminals to get their hands on large quantities of consumer information, it seems as though we'll continue to be victimized by data security breaches long-term. Notification by the company or institution involved will help alert us to the potential for a problem, but to truly be protected from identity assumption, we need to take matters into our own hands.

You can't stop the criminals from attempting to assume your identity, but by staying abreast of changes to your personal information that you didn't initiate, you'll minimize the time and cost associated with correcting a full blown identity assumption.

Related News

Report: Connecticut Workers' Private Data Was On-Line for Years

Census Bureau Admits Privacy Breach

Experts Warn of Identity Theft Risk

Identity Restoration

If your identity is ever assumed by a criminal, we will aid in the recovery process in two ways. We can either assist you in the resolution process, or completely do it for you.

If you simply want assistance, we provide a step-by-step instruction manual detailing the resolution process, including guidance for avoiding future complications, and a toll-free victim assistance number for access to specialists trained in identity theft recovery.

This service allows you to correct identity theft problems themselves, without the assistance or expense of an attorney. You may also choose to have us assume and reorganize the recovery process on your behalf. In this case, we can further minimize the time and hassle involved.