SPECIAL REPORT

DATA BREACHES: KNOW THE RISKS

What is a data breach?

You might have heard about millions of taxpayers in South Carolina having their personal data hacked; or the credit card system at Zaxby's exposing customers' credit card data. Or maybe you've heard about a laptop being stolen from a doctor's office; or a USB drive with voter registration information going missing. Some stories even involve paper records being left in a dumpster for anyone to see.

All of these are examples of a data breach -- which simply means that sensitive data has been exposed. It can happen by accident or carelessness; it can be the result of insider theft; or be caused by an outside hacker.

Identity theft is **9.5 times** more likely if you have received a data breach notification

5 Key truths about data breaches

1. You will be the last to know

There is no Federal law governing how quickly a breached organization must let you know your data has been lost, stolen or exposed. In states where legislation exists, there is typically a 60-day "grace period" before they must notify you. In other words, two credit card billing cycles may have gone by before you know you should be paying extra attention to check for fraudulent charges. This time lag may also make it harder for law enforcement to track identity thieves down.

This also assumes that the breached group is complying with any existing regulations – in the recent case of TD Bank, they were aware of a breach for six months before notifying customers.

Also realize the "notification clock" doesn't start ticking until the breach is discovered – often, data has been unknowingly exposed for months or years.

And finally, if the breach is on out-of-date or incomplete information, they may be unable to send you a notification letter. It will be up to you to keep your ear out for press coverage of breaches and investigate to see if you were involved.

2. Don't assume you are enrolled in a monitoring service

Because many breach announcements include a mention of offering monitoring services, you may be lulled into a false sense of security. Being "offered" a service and being "enrolled" in one are not the same thing. In most cases, it will be up to you to take certain steps to accept the offer and activate the monitoring, as was the case in the October 2012 breach at the University of Georgia.

Secondly, while some types of breaches (like ones involving medical records) are required to offer monitoring, not all are covered by legislation. They may simply elect to tell you to "be watchful."

3. Not all monitoring services are created equal

Most times, you will be offered credit monitoring. This is not the same – or as comprehensive – as identity monitoring. Credit monitoring only detects credit-related fraud. This type of identity theft makes up only 19% of all known types of identity theft. The other 81% involves things like medical insurance fraud, tax return theft, and even criminal identity theft, which involves using your name when arrested.

(cont. on p.2)

CORE ID SERVICES, LLC

www.coreidservices.com

ABOUT CORE ID Services

CORE ID Services, LLC provides full-service identity theft recovery and monitoring services through ARX-ID Identity Theft Protection Plans. These plans are available to individuals and as group benefits through employers and other groups. Contact us at 855-262-7610 for more information on how we provide real help for identity theft.

SPECIAL REPORT: 5 Key Truths about Data Breaches

WHAT IF YOU DON'T RECEIVE RECOVERY ASSISTANCE?

The Identity Theft Resource Center estimated that victims who contacted them for help in fixing ID theft on their own spent an average of 141 hours in the attempt.

25% of ID theft victims surveyed by the FTC were somewhat or very dissatisfied by their ability to correct their credit report. One victim said:

"It was ***easier for the thief*** to change my info on my credit report ***than it has been for me*** to change it back. Still not right after working to fix it for ***six months***."

IDTrack™ from ARX-ID monitors your full data profile -- not just your credit report -- to detect all 40 types of identity theft.

(cont. from side 1)

CORE ID Services designed their ARX-ID service to follow the recommendations made by Javelin Strategy & Research in their 2012 report on identity theft, which said:

> "The most complete identity protection services offer both personal information monitoring and credit monitoring."

4. Monitoring is not the same as recovery assistance

So you have signed up for monitoring after learning you were involved in a breach. That monitoring has detected fraudulent activity. Now what?

That depends on whether you are provided with recovery assistance as part of the breach remediation.

Recovery assistance helps a victim navigate the multi-step process of stopping and correcting identity theft. These services vary widely in how much assistance they provide. The most basic only give you a checklist to follow on your own. The most comprehensive services, such as ARX-ID, use a power of attorney to authorize a trained recovery professional to act fully on your behalf. This specialist will complete all the many necessary steps to correct identity theft, and circle back to ensure that your name was completely cleared.

5. Thieves will wait until monitoring has expired

Typically, if you are involved in a breach, you will be offered one year of credit monitoring. Not only is credit monitoring insufficient on its own, but thieves will know how long the monitoring will be in place and "sit tight" until it has lapsed. Without ongoing, life-long vigilance, your stolen data remains at risk for fraud or identity theft.

Enrolling in ARX-ID allows you to put an "IDTrack™" in place that will monitor personal data, not just credit cards, for suspicious activity. You have the choice of monthly or continuous assessments, and can log into our secure member portal anytime to view your RiskGauge™. You can also activate our RiskAlert™ service to get real-time alerts when someone attempts to use your personal data, and shut down fraud before it occurs. Unlike a credit freeze, this allows you to keep using your credit profile for your own use, but alerts you to all forms of identity theft.

Sources:

"2012 Identity Fraud Report," Javelin Strategy & Research

"Child Identity Theft," Carnegie Mellon CyLab, http://www.cylab.cmu.edu/files/pdfs/reports/2011/child-identity-theft.pdf

http://www.databreaches.net/?p=25560

http://www.scmagazine.com/university-of-georgia-latest-target-of-data-breach/article/263928/

ID Theft Data Clearinghouse, 2009, FTC, http://www.ftc.gov/bcp/edu/microsites/idtheft/downloads/CY2009/Georgia%20CY-2009.pdf

2012 Identity Fraud Report: Consumers Taking Control to Reduce Their Risk of Fraud, Javelin Strategy & Research

Aftermath 2009, Identity Theft Resource Center, http://www.idtheftcenter.org/artman2/publish/m_press/Aftermath_2009.shtml

Using FACTA Remedies: An FTC Staff Report on a Survey of Identity Theft Victims, March 2012

3rd Annual Survey on Medical Identity Theft, Ponemon Institute, June 2012