



9 Tips for Data Breach Victims

Follow these tips to protect your good name.

Maybe you've heard a news report about a data breach at a company where you do business. Or you've received a letter stating that your personal information may be in the wrong hands.

What does it all mean?

A data breach is the release of sensitive information into an insecure environment. Breaches can take many forms. Sometimes data is stolen or leaked. Often, though, it is inadvertently exposed when data is lost or shared.

Whether the trouble started with a pilfered laptop or an insidious cyber-attack, a breach of personal electronic data triggers mandatory notification laws in nearly all U.S. states and territories. If you haven't received such a notice already, chances are you will.

But just because your personal information—a Social Security number, birth date, or mother's maiden name, for example—was affected, it doesn't mean you'll become a victim of identity theft. It means something's happened that could put you at risk.

Follow these steps to protect your identity and credit:

1. Read the notice carefully to learn what information may have been exposed and how. (Keep the notice in case you ever need to prove that your data was compromised through no fault of your own.)
2. Review the breached account. Identify what information it contained and what was compromised. Look for unauthorized activity, such as a change in address or telephone number.
3. Know exactly what's at risk. If it's debit or credit card numbers only, there's a good chance someone will try to use them. On the upside, your exposure is limited and, if your bank thinks the risk is high, it will automatically reissue new cards (effectively shutting down the identity thief). Degree of risk gets stickier when data like Social Security numbers, birth dates and addresses are stolen. This information has a long shelf life and can be traded internationally among organized criminals. It's valuable because, unlike a single credit card number, it can spawn dozens of new accounts. While it's less likely to be used than a single stolen credit card number (which requires much less time and work), potential damage to your good name is greater.
4. If you're offered a year of free credit-monitoring, take it.
5. Pay extra attention to your account and billing statements. Check for charges that aren't yours.
6. Check your credit report and watch for other fraud. After about 30 days (long enough for fraudulent activity to show up), log on to annualcreditreport.com to get a free copy of your credit report from each of the three major credit bureaus. Look for any unusual



Michigan Millers
Mutual Insurance Company



9 Tips for Data Breach Victims

Follow these tips to protect your good name (cont.)

activity. Investigate suspicious activity and stay on top of it until the matter is resolved. Also look for signs of fraud in your medical files, on your Social Security statement, in insurance claims or in public records.

7. Change all user access credentials. If you use the same passwords for other financial institutions, change them. Watch financial statements—on paper and online—for unauthorized transactions. Be aware of potential email, phone and snail-mail scams. Enable text and email alerts when possible.
8. Notify existing creditors of the breach. Consider canceling your cards and getting new ones. Take advantage of issuers' services that alert you to unusual transactions.
9. Place a fraud alert on your credit file. An alert placed with any one of the three major credit bureaus signals to potential creditors that you could be a victim of identity theft.

©2003-2011 Identity Theft 911, LLC. All rights reserved.

Safeguarding Against and Resolving Identity Theft

As a benefit to all Homeowners policyholders, Michigan Millers provides Identity Theft Resolution Services at no additional cost. By partnering with Identity Theft 911, Homeowners policyholders receive:

- Proactive services to help protect their identity
- Resolution services to recover from identity theft and fraud
- Document replacement assistance

In addition, Michigan Millers offers Identity Fraud Expense Coverage. This is a valuable benefit for individuals and families that pays up to \$15,000 per occurrence for "expenses" incurred by an insured toward resolving identity fraud. (This coverage does not reimburse policyholders for monetary damages.)

Compensation is provided for a wide range of expenses such as costs for certified mail, loan application fees or lost income resulting from time taken off work (...up to a maximum payment of \$200 per day. Total payment for lost income is not to exceed \$5,000.)

In this age of high-tech crime and cyber-attacks, give security and peace-of-mind to your clients. Call us today at 800.888.1914 to learn more.

This article is intended to give general information only. For full coverage details, please refer to the actual coverage endorsement.



Michigan Millers
Mutual Insurance Company