Respond Quickly When Your Personal Data is Exposed

by (ARA)

It seems like thereâ€™s a new headline every day about another stolen laptop, a hacker attack or a lost data tape. And the impact of these incidents is widespread. One organization estimates that over 91 million data records of U.S. residents have been exposed due to security breaches since February 2005. You may have received a notification letter, in which an organization alerts you to the fact that your personal information has been exposed. After reading the letter, you may still have some questions about what it means for you and what steps you should take. Identity theft is the most significant risk you face following a data breach, and the severity of the risk is determined by how the data is stored and what kind of data it is. When stolen data is encrypted â€“ or stored in a scrambled fashion that requires a â€œkeyâ€• for someone to unscramble â€“ it is much more difficult for the criminal to access. Identity thieves can use your Social Security number, credit card numbers and bank account numbers to make purchases or to open new credit accounts. Your name, address and date of birth are also valuable pieces of information to criminals. The safest course of action is to take precautions if you suspect that your personal data is likely to be misused. Studies have shown that acting quickly can minimize the financial impact and time to recover from identity theft. Place a fraud alert on your credit file before the criminal has a chance to apply for credit in your name. It can save you a lot of hassle down the road. A temporary fraud alert, placed on your credit file for 90 days, lets credit grantors know that you may have been a victim of fraud and that they should take extra steps to verify your identity before extending credit in your name. To place a fraud alert on your credit file, contact one of the three national credit reporting companies: Equifax: (800) 525-6285 Experian: (888) 397-3742 TransUnion: (800) 680-7289 You will need to provide personal information for authentication purposes. The company you contact will notify the other two credit reporting companies, who will add a fraud alert to their files. Your confirmation will include instructions for requesting a copy of your credit report. Often organizations provide assistance to their customers or employees who have been impacted by a data breach. In fact, many companies have offered their customers and employees free credit monitoring, which alerts them to key changes in their credit file. For example, the addition of a new credit account or a significant increase in the balance on an existing card might signal that an identity thief has struck. The sooner you contact creditors to alert them to any fraudulent activity, the easier it is to resolve. When a company offers you free credit monitoring after a data breach, you will be given a promotional code and directions for online enrollment. You will need to provide identification information, including your Social Security number, for authentication purposes. If the free monitoring is provided through Equifax, you will not be asked to enter a credit card number to enroll for the free offer. If your data has been improperly accessed but you have not been offered free credit monitoring, consider purchasing Equifax Credit Watch Gold with 3-in-1 Monitoring to protect yourself. It provides comprehensive credit file monitoring and automated alerts of key changes to your credit files at all three national credit reporting companies.

Respond Quickly When Your Personal Data is Exposed by (ARA)