Protecting Your Assets

Lost Data? Create An Emergency Response Plan

by Denise Richardson

(NAPSA)—Chances are this may have happened to you: A letter or e-mail arrives from a company with which you do business, informing you that their customer data files were "accessed by a third party."

These messages generally include reassuring statements that they take your privacy very seriously, that steps have been taken to improve data security and you have no need to worry. Sometimes, they even apologize for the inconvenience.

What should you do next? Here are a few suggestions:

Richardson

•**Be Cautious:** The company that lost your personally identifiable information may tell you they believe your important information is secure because it was encrypted, kept on a different server or not saved after your last transaction. This may be accurate but you should take necessary precautions.

•**Change Your Password:** Start with the online site that was compromised. If you use the same username and/or password to access other sites, change those passwords too.

•**Use Strong Passwords/ Passphrases:** Your phone number or pet's name is too easy to guess. Skilled hackers can break most passwords in a matter of seconds. Use a random password generator, which lets you choose password length, case sensitivity and whether to use special characters. Then store them with a password manager or in a secure place of your own. Consider using a pass "phrase" instead of a password.

Skilled hackers can break most passwords in a matter of seconds. You may want to use a random password generator.

•**Check Your Statements:** Data thieves move fast, so make a point of checking your credit card or bank statements often. Even small transactions that you don't recognize can be a sign that thieves are checking for valid card numbers before they make big purchases. Report any transaction you don't recognize.

•**Check Your Credit Report:** Request credit reports from the three major agencies every year, for free, by visiting AnnualCreditReport.com or call the toll free automated line at (877) 322-8228.

•**Guard Against Phishing:** If you get an unsolicited e-mail claiming to be from the business where the breach occurred, it very well could be a "phishing" e-mail from the data thief, trying to collect even more personal info. Don't click on a link in the e-mail or call the phone numbers provided. Go to the business' home page or call them directly at a number you trust.

•**Sign up for Identity Protection and Restoration:** Companies such as LifeLock can help protect you against more than just credit fraud, they can alert you whenever your personal information is used to apply for wireless services, retail credit, utilities and mortgage loans. If you become a victim of identity theft while you are a member because of some failure or defect in the service, they will spend up to $1 million to hire experts, lawyers, investigators, consultants and whoever else it takes to help your recovery. For more information, visit www.lifelock.com.

•**Don't Equate a Data Theft with a Mere Credit risk:** Today's identity thieves are savvy and have found new methods to access your data and even more methods to use it.

•**Report All Fraud:** Keep in mind, the bad guys who stole from you today will steal from somebody else tomorrow. Report fraud to your local police and file an identity theft report with the Federal Trade Commission.

Denise Richardson is a consumer advocate and author of "Give Me Back My Credit!" A victim of identity theft, she became a certified identity theft risk management specialist, trained by The Institute of Fraud Risk Management and is a member of the National Association of Consumer Advocates.