Roman Kepczyk • Oct. 01, 2008

From the Oct. 2008 Issue

Over ten million Americans have been a victim of identity theft according to the TrustedID.com website. Virtually every week, there is another newspaper story about hackers breaking into systems and capturing personal information that could be utilized by criminals to steal the identities of your personnel, members of their families, and your clients. And those are just the breaches that are discovered and reported to the media! With the increased utilization of digital personal records, digital payments and online banking systems, the opportunity for hackers to get access to large volumes of information will only increase the risk of identity theft. Surveys indicate that the average victim of identity theft will spend $8,000 resolving the issue and will take an estimated 600 hours of personal time to do so. If one of your personnel or a member of their family becomes a victim of identity theft, imagine the impact on their productivity and the corresponding impact on the firm during that time. For this reason, we feel it is imperative that firms take a proactive approach to managing the risk of identity theft, which can be done with education of personnel, providing resources to deter and respond to identity fraud, and having a prepared response in the event that one of your associates becomes a victim, to minimize the impact.

Education

The first step in managing identity theft is educating your personnel on how it occurs and what they can do to minimize the risk. In addition to online breaches, identity thieves steal purses and wallets, "skim" credit cards when you pay for services, and sift through garbage to find un-shredded credit card statements or other financial records that they can use to open other accounts

or change the address so they can bypass delivery of statements. They also use

salary amounts are correct and that no one else is using your SSN for payroll.

Identity Theft Resources

The Federal Trade Commission (FTC) is the watchdog for consumers in the United States, and they have developed resources specifically to assist identity theft victims at www.ftc.gov/idtheft. They have also set up a telephone hotline where they can be contacted directly: 877-IDTHEFT. The FTC created a document entitled, "Take Charge: Fighting Back Against Identity Theft," which can be downloaded from their website and stored on the firm's network for easy access or forwarding. The Federal Deposit Insurance Corporation (FDIC) has also developed materials for dealing with stolen wallets (Your Wallet: A Losers Manual) or abuse of checking accounts (A Crook Has Drained Your Account. Who Pays?) at www.FDIC.gov and through their hotline at 800-934-3342. Reviewing these documents can assist the firm in creating educational materials, as well as planning a response.

Third-party services can help with the prevention, detection and remediation of identity theft, and firms should consider providing some of these as an employee benefit. Services range from $5 to $20 per user per month, and some have plans that include every member of the family for less than $200 per year. A list of providers can be found at NextAdvisor.com, comparing services such as LifeLock, TrustedID, IdentityTruth, IdentityGuard, IDWatchdog, FamilySecure, LoudSiren and Equifax. This is not intended to be a comprehensive listing of all resources and is provided for illustrative purposes. Some of these services will place a fraud alert on your account for you every 90 days, provide you with regular access to your credit report, and manage the removal of your name from pre-approved credit listings.

While all three of these services can be done by individuals for free, some

even suspecting they are a victim, they should have a package prepared for the person to respond as quickly and aggressively as possible to minimize loss. This document should list the action steps beginning with the phone numbers for the fraud departments of the three major credit bureaus (Experian, TransUnion and Equifax) to place a "fraud alert" on the user's record and to post a "victim's statement" requesting that you be contacted prior to opening any new or making changes to any existing accounts. The employee should ask for a free copy of their credit report to verify all the accounts that are open and to review the section on inquiries for new accounts. This fraud alert will usually be in place for 90 days and can be renewed. In the event of a proven loss where the victim has filed an Identity Theft Report with the Police, the victim can ask for an extended fraud alert, which will be in place for seven years and will require potential creditors to contact the victim directly before extending any credit.

The victim should then contact each creditor including banks, utilities and the phone company and ask to talk to the fraud department, which should be followed up in writing. All accounts that have any appearance of being tampered with should be immediately closed. The victim should also make a concerted effort to file a police report with the local department where the theft took place as well as contacting the Federal Trade Commission, which has many available resources to assist victims. If the victim's driver's license was stolen, the victim should contact the licensing department and notify them of the theft and get a new license issued.

Identity Theft can happen to anyone, leading to extensive lost time and possible financial ruin. For this reason, firms need to take a proactive approach to

minimize the impact on the firm and to develop the resources to protect their

NextAdvisor.com —
list of third-party service providers that can help with prevention, detection
and remediation of identity theft

Technology