May 11, 2017

What to do When Fraud Occurs

AUDIT, BUSINESS ADVISORS, RISK ADVISORY/INTERNAL AUDIT
BY BERNIE RAFFERTY

The letter arrived in the mail two days after I saw the story on the news; my credit card had been used at a hotel that was hacked last fall. On a work trip, I stayed at a reputable hotel and provided my credit card for incidental expenses, as the clerk requested at check-in. I have read articles and heard suggestions regarding how to prevent becoming the victim of credit card theft or other forms of fraud, but in this case there was nothing that I could have done differently to prevent my credit card information from being stolen.

Large-scale incidents of credit card theft have received considerable media attention over the last few years; when combined with ransomware attacks, phishing schemes, theft of Personally Identifiable Information (PII), and other forms of fraud, the threats seem endless.

This article is meant to act as a "What to do" resource in the event that you, a friend, family member, or a client becomes the victim of fraud. The specific circumstances surrounding the fraud will influence the steps that should be taken to respond to the fraud. In my situation, the company had already identified the breach and taken measures to respond to it, but the steps below provide a starting point to respond to the incident and recover from the fraud.

The first thing victims should do is notify their primary financial institution that the incident has occurred. Care should be taken to make sure to call the correct customer service number that is found on the statement or the back of the credit card. Scammers may try to fool their victims by giving them the wrong contact information, which will only make the situation worse by extracting more sensitive information from them. The financial institution should place a fraud alert or another notation on the victim's accounts, which may prevent illicit activity from occurring within those accounts.

Once the primary financial institution has been notified, victims should consider any other financial institution that they do business with that may be compromised. In my example, my credit card information was the only data stolen, but if the theft had been the result of an attack on my online banking account, where I have links to multiple financial accounts, I would have to notify all of the possible institutions of the breach.

One way to mitigate some of the risk of having credit card information stolen is to have a dedicated credit card, either a different brand or one that is unlinked from the primary card, that is only used online or for over-the-phone purchases. By limiting the exposure of the card, if the online card becomes compromised, or vice-versa, the other card can still be used to make purchases.

Victims should notify police or other authorities about the fraud. If the fraud was perpetrated online, the Federal Bureau of Investigation (FBI) is the agency charged with investigating those crimes. The FBI's Internet Crime Complaint Center (IC3) provides a link to report the crime online at www.ic3.gov. Ransomware, credit card fraud, email account attacks, and phishing/spoofing are some of the crimes that can be reported online. In addition, if online account information has been compromised, it is important to change the passwords to any account where the victim used the same password.

If the fraud was committed in person or locally, victims should inform their local police department. The victim may be the latest in a string of crimes that the department is investigating, or it may alert the department to an issue and prevent additional victims. Local scammers could be part of a larger network that is perpetrating crimes in locations around the country.

The next thing a victim of fraud should do is to request a free credit report to determine if any other accounts have been opened or if there appears to be any unusual activity. The only resource to receive a completely free credit report is www.annualcreditreport.com. Other sites may have annual fees or other terms and conditions, but by using annualcreditreport.com, everyone is entitled to a credit report each year from each of the three credit reporting agencies (Equifax, TransUnion, and Experian). The agencies have slightly different information, so it may be wise to request reports from more than one of the agencies. The information needed to verify the report request ranges from previous addresses, to monthly car payment amount, to the payoff date of a department store credit card, so it is important to have access to that kind of financial information when requesting the report.

As victims attempt to recover from an incident, they may receive more detailed instructions from their financial institutions or the authorities. The process of recovering from the fraud will take time and effort on the part of the victim, but hopefully this article provides a plan to begin the recovery process.

Please contact us if you have questions regarding what to do if you, or someone you know becomes a victim of fraud and visit the Our Thoughts On... blog for more articles.

You've heard our thoughts... We'd like to hear yours

The Schneider Downs Our Thoughts On blog exists to create a dialogue on issues that are important to organizations and individuals. While we enjoy sharing our ideas and insights, we're especially interested in what you may have to say. If you have a question or a comment about this article – or any article from the Our Thoughts On blog – we hope you'll share it with us. After all, a dialogue is an exchange of ideas, and we'd like to hear from you. Email us at contactSD@schneiderdowns.com.