Credit Monitoring: How to Check Your Credit Report for Fraud

Posted on May 31, 2016 by David Rabinovitz in Credit Fraud & Monitoring, Personal

As a security best practice, we often advise people to check their credit reports to protect themselves from identity theft. This type of credit monitoring is helpful for spotting potentially fraudulent activity, but it's not always a straightforward process.

How can you look at that list of numbers and creditor names and know what's what?

Credit reports may have different formats from one another, because each credit reporting agency uses its own template. However, they all contain the same basic information. Make the most of your credit monitoring efforts by looking closely for these red flags:

- **Incorrect old addresses:** Even if your current address is correct, be sure to pay close attention to previous addresses. Identity thieves may have committed mail fraud by using your name and another address in order to sign up for credit cards or open accounts.
- **Court decisions you didn't know about:** Part of your report will include a section usually called "adverse accounts," which collects the negative items pulled from public records. These include court judgments, bankruptcy decisions and tax liens. This may be where you find out your identity was used in a courtroom without your knowledge. For example, a criminal may have claimed to be you during an arrest. Even if the claim amount is minor, it's worth getting this fraud removed from your record, since it can count against your credit reputation.
- **Collections for bills you paid or never had:** Often, debts that are significantly overdue are sold to debt collection agencies. Mistakes can occur during this process, however. For instance, if the company selling to a collection agency has inefficient bookkeeping practices or poor data management, paid debts may get bundled together with other records. In some cases, an identity thief may have been the one racking up the debt, and you may not find out until it appears as collection activity on your report.
- **Credit accounts you don't recognize:** Look carefully at all the data provided for your credit accounts, which can sometimes reflect over a decade's worth of accounts you've opened and closed. This is one of the easiest ways to spot fraud during credit monitoring.
- **Inquiries that seem suspicious:** Most companies that can claim a legitimate purpose — like offering you a credit account or signing you up for insurance — don't have to get your permission to view your credit report. But others, including employers, need permission. Look closely at which companies and individuals have requested your report recently to make sure you're not being targeted for fraud.

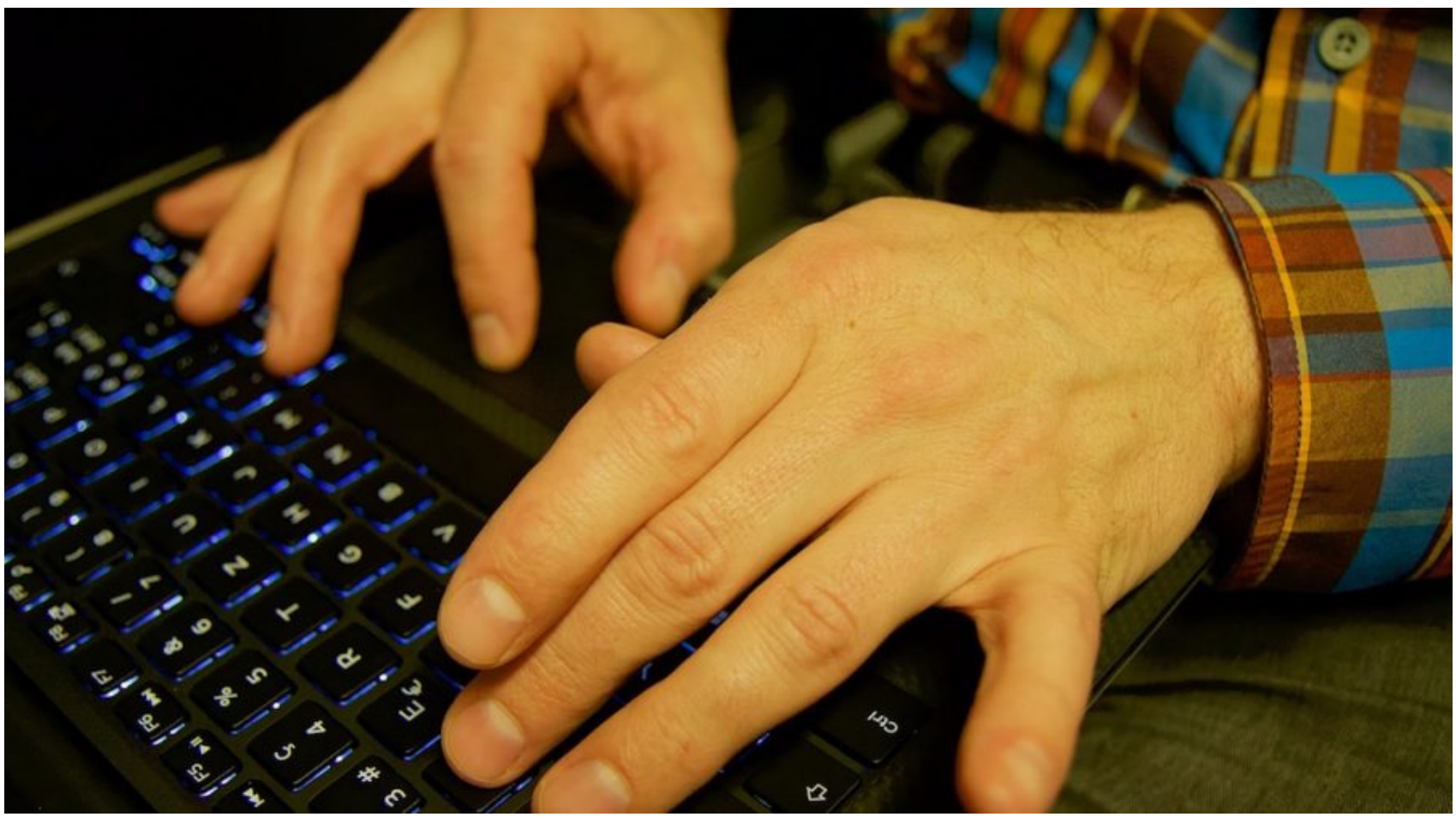
If you spot something that doesn't look right, don't hesitate to report the error right away. The sooner you can start an investigation, the less damage control you'll have to do. You may also consider a credit freeze as the situation is getting sorted out.

By getting a better handle on the details of your credit report, it's likelier your credit monitoring efforts will be more effective and you'll maintain a fraud-free record.

Image courtesy of LendingMemo.com.

IdentityForce.
A Sontiq™ Brand

Scam Alert: Online Petition Scams & Other Threats



Posted on July 22, 2016 by Heidi Daitch in Personal, Scam Alerts

When debate gets especially heated, as it is right now about many hot-button issues, people can be passionate about their opinions. And that's fine — as long as voicing them doesn't lead to security risks.

Identity thieves and other criminals are particularly drawn to newsy topics like tragedies, because pleas often go out for donations along with names and addresses on online petitions. While many of these efforts are legitimate, some might be a decoy for financial theft and data gathering.

Here are some common ploys to keep in mind as you're debating and donating, with tips on staying safe.

- **Online petition scams:** Thanks to the Internet, anyone can start an online petition about any issue. Unfortunately, criminals like identity thieves can set up fraudulent sites to harvest email addresses and other information. Your details might be used directly for identity theft or sold to other scammers. Even in-person petitions have been linked to petition scam attempts. *Tip:* As with charities and emails, check out the source and be wary about giving away too many personal details. Adding your name to a legitimate petition is fine, but there's no reason you should have to give your address, date of birth or other details.
- **Charity scams:** Just hours after the tragic Orlando shootings, the Better Business Bureau reported that questionable solicitations and click-bait schemes had started, with many more expected. Charity scams are always popular among thieves, especially during the holiday season, and tying them to a newsworthy event or contentious issue preys on emotion. *Tip:* Check out sites like Give.org and Charity Navigator to find legitimate charities, and think twice if you're contacted directly by phone or email.
- **Phishing:** Email newsletters and donation appeals tend to be frequent during an election year. With higher email volume comes a higher chance of phishing scams — or the newest threat, "shmishing," which is sending scams via text message. *Tip:* Only open emails from senders you recognize, and even then, avoid opening any attachments or clicking on links. Go directly to an organization's or news source's website rather than navigating there through a link in an email or text.
- **Personal fundraising appeals:** There are thousands of personal appeals online for funds to help those who are going through tough times or need support of some kind. The largest charitable crowdfunding website, GoFundMe.com, reportedly raises nearly $2 million every day. But scammers can take advantage of the fact that these fundraising vehicles are easy to set up. *Tip:* When directing your funds, do some research on the individuals or situations in question.

Political season or not, it's always smart to stay aware of potential scams. When giving your opinion or your charitable donations, do some double-checking first to make sure you're protected.

Watch Out for Credit Card Skimmers This Summer

Posted on June 16, 2016 by Jennifer Bellemare in Credit Fraud & Monitoring, Personal

School's out, vacation time is confirmed and your trip is booked. Unfortunately, fraudsters and identity thieves share your excitement. Summer tends to be a busy time for these criminals, who gear up for lost debit cards, more credit card charges and sporadic reviews of recent transactions by consumers.

One of the fastest-growing scams to hit vacationers are credit card skimmers. What is a skimmer? It's a device that is hooked up to ATMs and gas pumps, and made to look like legitimate equipment. Once installed, credit card skimmers record credit and debit card numbers as well as PINs. The thieves then either gather the information remotely or come back to collect the devices with all the numbers stored on them.

Either way, the transactions still go through normally. So you can still get cash or check your balance at an ATM or fill up at a gas pump without realizing that the credit card skimmer is stealing your information.

Growing Threat

The risk of skimming is increasing, according to security experts. Even one person skilled in skimming can cause significant damage. For example, *The San Diego Union-Tribune* recently noted that a skimming suspect placed devices throughout a countywide area and managed to loot nearly a half-million dollars from bank accounts before getting caught.

Global security expert Brian Krebs wrote that skimming attacks have increased at an alarming rate in the past year, in both the United States and Europe. From 2014 to 2015, **ATM skimming alone rose by 546 percent**. Furthermore, the Vice President of Fraud Solutions at FICO pointed out in a report that criminals are moving faster and making it harder for banks to shut down the compromised machines.

Stopping the Credit Card Skimmers

Unfortunately, the clunky skimmers that were once in place — sporting mismatched buttons, seams of dried glue and off-kilter swipe strips — have been replaced by devices that **look remarkably like the real thing**. Even worse, they're cheap and plentiful. One news report noted that fraudsters can buy credit card skimmers on eBay for less than $100.

While it can be challenging to spot a skimmer today, there are a few protective steps you can take:

- **Use an ATM inside a bank if possible.** Outdoor ATMs are more susceptible to skimming, since criminals have better access and can install skimmers more surreptitiously.
- **Safeguard your PIN.** Some credit card skimmers use cameras pointed toward the keypad. Covering your hand as you punch your code can help shut down some skimming.
- **Check your gut.** If something doesn't feel right about a device, don't use it.
- Whenever possible, **use cash instead of a card**, so that you have fewer credit or debit transactions. (If you are victimized, this also makes it easier to determine where a skimming incident may have occurred.)

One of the top ways to thwart fraud and subsequent identity theft is through credit and bank monitoring, especially with a service like IdentityForce that issues alerts if any suspicious activity occurs. With threats like credit card skimming becoming more difficult to detect, it's more important than ever to step up protection with 24/7 vigilance.