Massive data breach hits Capital One!

By Bill Coder, Chief Information Security Officer at Cornerstone CFCU

Did you apply for a Capital One credit card between 2005 and 2019? If so, your personal information including name, address, phone number, email address, dates of birth and self-reported income may have been compromised.

According to USA Today; Capital One announced Monday that personal information, including the Social Security and bank account numbers of more than 100 million individuals in the US, were compromised in a massive data theft that led to the arrest of a Seattle woman. In my opinion the how is not as important as to what you as a consumer needs to do next.

So what should you do now?

Start immediately by freezing your credit reports at the three major firms: Equifax, TransUnion and Experian. You will need to register on the websites and look for the "Security Freeze" link. It will request that you enter your name, address, social security number and home address.

Equifax: Equifax.com/personal/credit-report-services/
Experian: Experian.com/freeze
TransUnion: Transunion.com/credit-freeze

The benefits of a freeze is that it prevents lenders from getting access to your credit report, which is mandatory for the credit card or loan application. It protects you in that the hacker who has stolen your personal information can't open an account in your name and get access to the funds.

We also recommend:

- Stay vigilant and check your account statements regularly to find anything suspicious. Remember - You don't have to wait for the statement to arrive in the mail to check your account! Log in to OASIS and look at your Cornerstone accounts online.

  Once a year, you can request a copy of your credit report from all three bureaus at **AnnualCreditReport.com**, a federally authorized website. My recommendation is to request a report every fourth month from one of the bureaus. Here's an example: August get a report from Equifax, December get a report from Experian and in April get a report from TransUnion. This way you can keep an eye out for loans and credit cards that you didn't apply for.

- If you believe you are potentially a victim of this breach change passwords immediately. Since your personal information is at risk, all it takes is one poor password, or if you use

the same password for multiple websites hacker can use them to get into all of your accounts. Experts recommend a combination of upper and lower case letters, numbers and symbols, and that each website you visit should have a unique password. It's a good practice to change your passwords periodically anyways.

- Remember to check your store credit cards because these cards are generally supplied through credit card companies like Capital One. My coworker has a Cabela's credit card but if you look on the back it is actually provided by Capital One.

- Beware of phishing
  Now that your information is out there watch out for phishing scams. When it comes to phishing, spoofed emails are the preferred method. Beware of email messages from unknown people with calls to action, like "click here" or "act now."

  Always hover the cursor over an embedded link to see the actual URL. If in doubt, just type the business' web address directly into the browser to make sure you're accessing the real page.

  Finally, look out for misspellings within emails and web pages. Typos are a common sign of scams

- Don't fall for phone scams
  Phone scamming is as old as the telephone. This old-school scams include calls from hoaxers offering free trials or travel, pretending to be your bank, credit union or credit card company, and threatening you with lawsuits if you don't make a payment or that there is an issue with your account.

  But scammers are getting more sophisticated. New technology, like caller ID spoofing software, is helping con artists stage scams. Be hypervigilant now that your information has been compromised.

Prevention means protection when it comes to identity theft.