

FOR IMMEDIATE RELEASE:

Tuesday, July 30, 2019

Michigan AG Nessel Notifies Michiganders of Another Data Breach

LANSING - Michigan Attorney General Dana Nessel today urged Michigan residents to take precautionary measures to protect their information that could have been compromised as a result of Capital One Financial Corporation's recent data breach.

According to the company, the breach impacted approximately 100 million individuals in the U.S. Exposed information included names, addresses, zip codes, phone numbers, email addresses, dates of birth, credit scores, credit limits, balances, payment history, and self-reported income. The company said no credit card account numbers or log-in credentials were compromised, however, 140,000 social security numbers and 80,000 linked bank account numbers of its customers were compromised.

Consumers and small businesses who applied for a Capital One credit card between 2005 and early 2019 are most at risk. The company has set up a consumer website about the breach at www.capitalone.com/facts2019.

The Attorney General's Office became aware of the breach through media reports late Monday. It is unclear how many Michigan residents were impacted at this time. However, Nessel's Corporate Oversight Division is seeking additional information about the breach through a letter to Capital One to determine its impact on Michigan residents.

"This data breach is yet another example of how fragile our information infrastructure is, and how vulnerable all of us are to cyber hacking," said Attorney General Dana Nessel. "And here in Michigan, we continue to rely on media reports that alert us to these terrible situations because – unlike most other states – we have no law on the books that requires that our office be notified when a breach occurs. I am determined to get information quickly and accurately to take more proactive measures to protect our residents."

"Capital One is a national bank, and is therefore regulated by the federal government under the National Bank Act and is not subject to regulation by Michigan's Department of Insurance and Financial Services (DIFS). DIFS applauds Attorney General Nessel's efforts to protect Michigan residents who are customers of these federally-regulated institutions, including through increased transparency and notification requirements in the aftermath of a data breach," added DIFS Director Anita Fox.

Since the breach occurred, the FBI has identified and arrested the person it believes is responsible. According to the criminal complaint filed by the U.S. Department of Justice, the alleged perpetrator had access to this information for about five months and attempted to sell the information online.

Nessel and Fox provided the following steps consumers can take to protect their information if they believe their information was compromised:

- Find out what information was compromised and act accordingly.
- Pull your free credit report at annualcreditreport.com or by calling 877-322-8228.
- Put a fraud alert on your credit file. The Federal Trade Commission provides a checklist for this.

- Consider a security freeze on your credit file.
- Be alert to unsolicited calls or emails appearing to be from Capital One. Hang up, do not reply, and instead call the number on your card. “Phishing” scams—calls, emails, or text messages that appear to offer protection—may actually be trying to get more data from customers.
- Take advantage of any free services being offered as a result of the breach. In this case, free credit monitoring and identity protection will be made available for everyone affected.
- Use two-factor authentication on your online accounts whenever it’s available.

For more information on what to do during a data breach, review the Michigan Attorney General’s consumer alert on data breaches.

###