NEWS BRIEF

Provided by: Conrey Insurance Brokers

Data From More Than 100 Million U.S. Capital One Customers Involved in Data Breach

Capital One announced on July 19, 2019, that the personal information of more than 100 million of its U.S. customers was compromised in one of the largest data breaches involving a bank. In an official release from the company, Capital One noted that the information exposed includes names, addresses, emails, credit scores and transaction data. In some cases, Social Security numbers and linked bank accounts of secured credit card customers were also compromised.

Capital One noted the breach occurred when a software engineer exploited a vulnerability and gained access to a company server. The company expects to lose between $100 million and $150 million from the hack, including costs related to customer notifications, credit monitoring and legal support.

This News Brief will highlight how you can find out if you were impacted by the breach and what steps you can take to further protect your data.

Was I Affected by the Breach?

Information involved in the breach reportedly came from credit card applications consumers and small businesses submitted between 2005 and 2019. Capital One has said that while the vulnerability has been addressed, they will continue to investigate the situation.

The company also said it will notify impacted individuals directly and offer free credit monitoring and identity protection.

What Else Can I Do to Protect Myself?

Outside of taking advantage of Capital One's credit monitoring and identity protection services, customers should consider doing the following to further protect their data:

1. Set up fraud alerts that notify you when someone applies for credit in your name. Equifax, Experian and TransUnion are the primary providers of this service. Placing a fraud alert does not affect your credit score.
2. Consider freezing your credit. This prevents anyone from opening credit or requesting loans and services in your name. You will need to request a freeze with each of the three credit reporting companies, which again include Equifax, Experian and TransUnion.
3. Monitor your credit reports and statements, and look for unusual or unfamiliar activity. Again, it's a good idea to take advantage of Capital One's free credit monitoring services if applicable.
4. Stay mindful of potential scams. In an FAQ hosted on its website, Capital One encouraged customers to be aware of potential phishing scams related to this breach. They stated that they do not call or email customers asking for personal information. If you suspect you have received a fraudulent email, do not reply to it or click any embedded links.

Conrey Insurance Brokers will continue to monitor this story and provide updates as needed.

Conrey INSURANCE BROKERS & RISK MANAGERS

© 2019 Zywave, Inc. All rights reserved.