



CONSUMER ALERT

Consumer Alert: Attorney General Warns Marylanders Regarding the Capital One Data Breach

BALTIMORE, MD (July 30, 2019) – Maryland Attorney General Brian E. Frosh is warning Marylanders that their personal and credit data may have been compromised in the July 19, 2019, data breach experienced by Capital One, the national bank and credit card issuer. Earlier this week, Capital One announced that a hacker had accessed about 100 million credit card application files. The hacker, based in Seattle, has already been arrested and, according to a complaint filed by the FBI, no evidence has yet been revealed that the stolen information was sold or disseminated by the hacker to any third party.

The compromised information reportedly included consumers' Social Security numbers, the majority of which were tokenized or encrypted. About 144,000 of the compromised Social Security numbers, which were used as employer identification numbers when applying for small business credit cards, were accessed by the hackers. Other information that was reportedly compromised in the breach included applicant's names, addresses, dates of birth, and information regarding their credit history (e.g., credit scores, credit limits, balances, payment history, and contact information). Capital One has stated that no credit card numbers or log-in credentials were compromised.

Capital One is providing information regarding the breach at the following link on its website: www.capitalone.com/facts2019/. It has announced that it will be notifying affected consumers and providing them with free credit monitoring.

Consumers who believe they may have been affected by a data breach should consider taking the following steps to protect their information:

- Obtain a free credit report at www.annualcreditreport.com or by calling 877-322-8228.
- Put a fraud alert on your credit file (you only need to contact one of the three major credit reporting agencies (Equifax, Experian, or Transunion) to place a fraud alert).
- Place a security freeze on your credit file (for more information about freezes, visit <http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/freezing.aspx>).
- Take advantage of any free services being offered as a result of the breach.
- Use two-factor authentication on your online accounts whenever available.

The Office of the Attorney General has an Identity Theft Unit that offers guidance and assistance. Information about protecting yourself or your children against identity theft, and what to do if it occurs, can be found at www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx. If consumers feel they have been harmed and want to file a complaint, they may call the Attorney General's Identity Theft Unit at 410-576-6491.