July 31, 2019

NEW YORK STATE OF OPPORTUNITY. Department of State

Consumers Urged to Safeguard Personal Information in Wake of Capital One Data Breach

In light of reports that more than 100 million Capital One customers' applications for accounts and credit cards were illegally accessed by a hacker earlier this year, the New York State Division of Consumer Protection is advising New Yorkers about steps to protect their identities and credit.

According to Capital One, an individual accessed an untold number of individuals' names, addresses, credit information, balances and more, plus 140,000 Social Security numbers and 80,000 bank account numbers. While the bank states that no credit card account numbers or log-in credentials were compromised, New York State urges all consumers to ensure their information is secure.

"We too often hear of major institutions suffering data breaches that impact millions of Americans," said New York Secretary of State Rossana Rosado, who oversees the Division of Consumer Protection. "However, there are steps individuals can take to reduce the chance of identity theft. An educated consumer is the best weapon against identity theft."

As required by New York State law, Capital One informed the Division of Consumer Protection of the number of New York residents impacted by this breach. The impacted individuals will be contacted by the company.

The Division of Consumer Protection urges consumers to follow these tips if they are subject to this or any other data breach:

- Get the facts before doing anything. The notification from the breached entity will inform the consumer as to what data was compromised and when the breach occurred. The notification should also provide contact information for the breached entity so the consumer can investigate further.

- Inquire as to what the breached entity will do to reduce the risk of identity theft (e.g. offer credit monitoring services at no cost for a specific period of time).

- Ask whether the breached entity will notify the three major credit reporting agencies (TransUnion, Equifax and Experian).

- Watch for signs of fraud. Not every security breach ends in theft or fraud. Check credit card billing statements for fraudulent charges and monitor bank and other financial statements. If a consumer spots something suspicious or unusual, they should report it to their credit card or financial company immediately.

- Check credit reports. Under the law, consumers are entitled to one free credit report per year from each of the three major credit reporting agencies. Consumers should review the report carefully and follow-up to dispute or correct any errors or fraudulent entries.

- Close accounts. Depending upon the nature of a data security breach, a consumer may need to close certain accounts and open new ones with different passwords.

- Learn more about personal information protections. Consumers may want to consider contacting a credit reporting agency and placing a Fraud Alert or Security Freeze on their credit file (see below).

- Retain paperwork. Consumers should keep all records about the data security breach and retain notes of any follow-up conversations for future reference.

Consumers may place a one-year fraud alert and security freeze on their credit reports with all three reporting credit bureaus free of charge. To place a fraud alert, consumers need only contact one of the three credit bureaus, which will notify the other two bureaus.

Free credit freezes: A credit freeze will restrict access to a consumer's credit file, making it harder for identity thieves to open new accounts in a consumer's name. The consumer is issued a unique PIN to use each time they wish to freeze and unfreeze their account to apply for new credit. Whether consumers ask for a freeze online or by phone, the credit bureau must put the freeze in place within one business day. When consumers request to lift the freeze by phone or online, the credit bureaus must take that action within one hour. If consumers make these requests by mail, the agency must place or lift the freeze within three business days.

Free child credit freezes: Consumers may also freeze children's (under 16 years-of-age) credit files free of charge until they are old enough to use credit.

Year-long fraud alerts: A fraud alert notifies businesses that run consumer credit reports that they should check with the consumer before opening a new account.

The fraud alerts and security freezes are free and identity theft victims are entitled to an extended fraud alert for seven years.

For more information, consumers may call the Division of Consumer Protection's Consumer Assistance Hotline at (518) 474-8583 or (800) 697-1220.