CAPITAL ONE DATA BREACH & EQUIFAX SETTLEMENT:
WHAT YOU NEED TO KNOW

July 2019

Nicholas Breit, CFA, CFP®
Senior Consultant & Financial Planning Practice Leader

On July 29, Capital One, the nation's third largest credit card issuer, announced that a hacker gained access to a server, revealing information of more than 100 million customers. The Capital One breach is far from an isolated event, as it represents the latest in a long list of large-scale data breaches in recent years that impacted companies such as Equifax, Yahoo, Marriott, Target, Home Depot and many others.

The Capital One news follows less than a week after Equifax announced a settlement covering more than 140 million customers affected by a 2017 data breach. The article that follows highlights key aspects of the recent Capital One data breach, details of the proposed Equifax settlement and practical considerations for consumers.

Capital One Data Breach
The recent Capital One theft is unique from other recent breaches in that it was reportedly carried out by a single hacker rather than by a group of criminals with a potential nation-state connection. In this case, a software engineer was able to exploit a misconfigured application firewall, allowing for the theft of more than 100 million customer records, 140,000 Social Security numbers, one million Canadian social insurance numbers and 80,000 linked bank details of Capital One customers. The breach is believed to have occurred between March and July of this year.

In a statement, Capital One noted, "Based on our analysis to date, we believe it is unlikely that the information was used for fraud or disseminated by this individual." The company also added, "No credit card account numbers or log-in credentials were compromised and over 99 percent of Social Security numbers were not compromised." Capital One estimates that the breach will cost up to $150 million, including the cost of credit monitoring for affected individuals.

While more details are likely to follow in the weeks ahead, customers who fear their data may have been compromised can find out more on Capital One's website, https://www.capitalone.com/facts2019/2/. Capital One advised customers that the company is *not* calling customers to ask for credit card, account information or Social Security numbers over the phone or via email. Therefore, any attempt to obtain such information should be considered suspicious.

Proposed Equifax Settlement over 2017 Data Breach
On July 22, Equifax announced a proposed settlement for which it would pay at least $575 million, and potentially as much as $700 million, as restitution for the 2017 data breach that exposed the data of more than 147 million Americans. The settlement would set aside a $300 million fund for affected individuals (potentially expanding to $425 million), $175 million to 48 states, the District of Columbia and Puerto Rico and $100 million for civil penalties to the Consumer Financial Protection Bureau (CFPB). Individuals impacted by the data breach should take the following steps:

Step #1 – Beware
The Federal Trade Commission (FTC) has warned that scammers created fake websites in an effort to access consumers' personal information. Individuals should take additional precautions to access only legitimate websites.

Step #2 – Check Your Eligibility
To determine if you were affected by the data breach, check the official settlement website. Only those impacted by the data breach will be eligible for compensation.

- https://eligibility.equifaxbreachsettlement.com/en/eligibility

Step #3 – Choose Among the Compensation Options

- "Alternative Reimbursement Compensation" – file a claim for free credit monitoring or $125
  - Free Credit Monitoring - at least four years of three-bureau credit monitoring, offered through Experian. Consumers can also get up to six more years of free one-bureau credit monitoring through Equifax.
  - Consumers may instead select a $125 reimbursement, though Equifax will only make such payments until requests total $31 million after which payouts will be lowered and distributed on a proportional basis.
  - Consumers selecting either of the above options will waive their right to pursue future legal action against Equifax.
  - Deadline is January 22, 2020.
  - https://www.equifaxbreachsettlement.com/file-a-claim

- File for a larger reimbursement
  - Consumers who lost money as a result of the data breach can file a claim for up to $20,000, after including proof of time and money spent.
  - Consumers may simply file for time spent, at $25 per hour for up to 20 hours. If a claim is submitted for more than 10 hours, the FTC notes that the individual must document the actions taken and provide substantiation of the identity theft or fraud.
  - Consumers selecting this option will waive their right to pursue future legal action against Equifax.
  - Deadline is January 22, 2020.

- Pursue separate legal action
  - Consumers affected by the data breach are *automatically included* in the settlement. Consumers wishing to seek greater compensation by way of legal action must opt out ("request for exclusion") by November 19, 2019.

Play Good Defense – Safeguard Data and Monitor Credit Reports
The frequency with which broad data breaches (such as Capital One and Equifax) have occurred in recent years, combined with fraudsters' increasingly sophisticated schemes, underscores the importance of taking extra precautions to safeguard and monitor sensitive information. In light of such prevalent security threats, individuals are strongly encouraged to keep the following "best practices" in mind:

1. Review Your Credit Report Annually. By law, individuals can obtain a free credit report every 12 months from www.annualcreditreport.com. According to the Federal Trade Commission, this is the only authorized source for the free annual credit report. The credit report should be reviewed for any discrepancies such as unauthorized accounts. Additionally, individuals can pay for a three-in-one credit report detailing the credit report from each company (Equifax, Experian and TransUnion) and may also include a FICO score.

2. Use Strong Passwords: Use a combination of numbers, symbols and letters to form a long, complex password. Use unique passwords for each online login and regularly change all passwords.

3. Use Multi-Factor Authentication: If available, enable two-factor authentication for email, social media, financial accounts, etc. This functionality sends a one-time code to a mobile device to verify access, thus preventing unauthorized parties from accessing your account without the code.

4. Keep Software Updated: To limit computer/device vulnerabilities, be sure to promptly update any security software, operating system or other software releases.

5. Only Use Secure Wi-Fi Networks: To deter cybercriminals from accessing devices through a home's wireless router, change the Wi-Fi network's factory-set default username and password. Avoid unsecure access to public Wi-Fi networks, such as in coffee shops, airports, hotels, etc.

6. Use Caution over the Phone: Avoid divulging any banking or personal information to a caller over the phone and do not give in to pressure to take immediate action. The IRS, the Social Security Administration and law enforcement agencies will not call with requests for information.

Additional Resources:

- Equifax Settlement Website – https://www.equifaxbreachsettlement.com/
- Federal Trade Commission (FTC) - Equifax Data Breach Settlement https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement
- Equifax Announces Details about the Proposed Settlement for Consumers https://investor.equifax.com/news-and-events/news/2019/07-26-2019-180040460
- An Equifax hack settlement promises a $125 payout. The truth is more complicated. https://www.washingtonpost.com/business/2019/07/27/equifax-settlement-guide-how-get-money-what-you-need-know/
- Equifax settlement owes you $125 but the free credit monitoring might be the better offer https://www.cnet.com/how-to/equifax-settlement-owes-you-125-but-the-free-credit-monitoring-might-be-the-better-offer/
- Capital One FAQ – https://www.capitalone.com/facts2019/2/
- Here's What You Need to Know About the Capital One Breach https://www.nytimes.com/2019/07/30/business/capital-one-breach.html

About the Author:

Nicholas Breit, CFA, CFP®
Financial Planning Practice Leader, Senior Consultant, The Wealth Office™

Nick provides investment consulting services to nonprofit organizations, corporate executives, family trusts and other high net worth investors. He services clients by providing advice and expertise on asset allocation, portfolio design, investment policy statements, manager search process and overall investment management. Nick is also a member of the firm's Core Investment Strategy Group. Prior to joining the firm in 2007, Nick was a Senior Financial Planner with The Ayco Company where he provided comprehensive advice to affluent clientele. Nick earned a BA in Finance and Economics from the University of Illinois at Urbana-Champaign. He obtained the designation of Certified Financial Planner (CFP®) from the College of Financial Planning and is a CFA® charterholder and member of the CFA Society of Chicago. Nick enjoys long distance running (having completed three marathons and multiple half-marathons) and spending time with his family.