Bond

INFORMATION MEMO
CYBERSECURITY AND DATA PRIVACY

AUGUST 18, 2020

Fallout from Capital One Breach Continues as Company is Ordered to Pay $80 Million Fine

Just over a year ago, on July 19, 2019, one of the largest confirmed data breaches in history was identified. The Capital One data hack exposed the personal information of more than 100 million customers and credit applicants in the United States and Canada. The exposed data included names, addresses, phone numbers, self-reported income, credit scores and payment history, as well as the Social Security numbers of more than 100,000 Americans and the Social Insurance numbers of more than one million Canadians.

The breach was allegedly accomplished by a single hacker: a former Amazon Web Services employee named Paige Thompson. Amazon Web Services hosts the database that was breached. According to Capital One, during the transition to cloud-based servers, a "specific configuration vulnerability" occurred. Thompson was then able to take advantage of a misconfigured firewall to access and steal the information of millions of users. The breach was only discovered after a fellow hacker reported Thompson, who had been bragging about the breach in online forums. Thompson was soon thereafter arrested and told authorities that she did not sell or share the data. Thompson is currently in federal custody, awaiting trial on charges of computer fraud and abuse, charges that could see her facing up to five years in prison and a $250,000 fine.

Lawsuits by customers whose data was compromised against Capital One soon followed. A separate lawsuit was also filed against Amazon, alleging that the company "did nothing to fix" the known issue with their cloud-based service that allowed the hacker to gain access to the database. A discovery decision from one of the Capital One lawsuits could have far reaching consequences in the cybersecurity world. A magistrate judge ruled that Capital One must provide the plaintiffs' attorneys with a third-party response report detailing the circumstances surrounding the breach. In other words, Capital One was ordered to provide all of the forensic details uncovered that showcase the technical as well as the procedural failures that allowed the breach to occur. Information such as this had previously been shielded from disclosure by claims of attorney-client privilege. Should this decision be embraced by other courts, experts predict that it could have a chilling effect on companies utilizing outside vendors to improve the security of their cyber positions. In this case, the judge cited to Capital One's sharing of the report with multiple regulators and its auditor, Ernst & Young, in his finding that the privilege argument was "unpersuasive."

The fallout from the Capital One breach continues as the company was recently ordered to pay an $80 million fine. This fine will be paid to the U.S. Treasury. In a consent order filed August 6, the Office of the Comptroller of the Currency (the OCC) cited Capital One's "failure to establish effective risk assessment processes prior to migrating significant information technology operations to the public cloud environment and the bank's failure to correct the deficiencies in a timely manner." In the order, the OCC provided a scathing indictment of the company's history of lax security, discussing an incident where the company was made aware, through internal audit, that its cybersecurity was woefully inadequate, yet the company's board of directors "failed to take effective actions to hold management accountable." Under the order, the company must establish a compliance committee by the end of August, which will meet quarterly beginning in October and provide regular updates. This committee will assess if the company has any continuing cybersecurity issues and

report with fixes within 60 days. The company is also required to create an action plan to detail how it is improving security. The Federal Reserve also issued a cease and desist order in accordance with the data breach requiring the company to comply with the OCC order and to submit a series of plans within 90 days that outline how the company plans to strengthen its risk management, internal controls, and governance, among other things.

If you have any questions regarding this memo, or any other related matter, please contact Kristin Warner, or any of the attorneys in the Cybersecurity and Data Privacy practice.