BRACEWELL

INSIGHTS

DOJ Announces More Equifax Charges – Credits Chinese Hackers

February 12, 2020

On February 10, 2020, Attorney General William Barr ***announced*** the indictment of four members of the Chinese military on charges of hacking into Equifax's computer networks, maintaining unauthorized access to those networks and stealing sensitive information. The announcement highlights one of the more pronounced nation-state actor cyber threats to industry and to personal privacy. The Equifax saga also includes a since-resolved related concern—insider trading on cyber incident information. The four officers in the People's Liberation Army are accused of conspiring to hack into Equifax's computers, to maintain unauthorized access to those computers and to steal sensitive personal information of American citizens. The Department of Justice announced the indictment on nine charges the day it was unsealed. The charges include computer fraud conspiracy, computer fraud and abuse with intentional damage and unauthorized access, conspiracy to commit economic espionage, economic espionage, conspiracy to commit wire fraud and wire fraud. The four officers are currently in China, and it is unlikely that they will ever appear in U.S. court.

According to the unsealed indictment, the Equifax breach compromised the names, birth dates and Social Security numbers of nearly 145 million Americans, as well as the driver's license numbers of at least 10 million Americans and the credit card numbers and other data belonging to 200,000 American consumers. The indictment further alleges that data of more than a million Canadian and British citizens was also compromised. The U.S. Computer Emergency Readiness Team, an organization within the Department of Homeland Security, warned Equifax months before the breach that its network was vulnerable. Equifax, however, did not act quickly enough or thoroughly enough to change its practices or update vulnerabilities in its software. The indicated Chinese officers allegedly used ***encrypted communications and routed their internet traffic through 34 servers in approximately 20 countries***. Despite these tactics and efforts to erase their tracks, they were identified through review of forensic data and investigation of the malware used. After the breach, the House Oversight Committee concluded that, because Equifax was aware of the vulnerability but failed to create an adequate security program, the hack was "***entirely preventable***."

Data breaches continue to be a major concern for governments and businesses alike. While most data breaches have a pure financial or ideological motivation behind them, there is also a persistent, mixed-motive threat from nation-state actors.

When a nation-state is suspected in a cyber incident, the U.S. government's interest increases, its involvement becomes more non-negotiable, and its assistance may be required to contain the incident and evict the intruder from the target network. Unlike smaller scale, private or individualized breaches, the motivation of hackers in these nation-state breaches often spans

beyond pure financial gain or public "doxing," though economic espionage is certainly part of the equation.

This indictment and the government's account of Equifax's response efforts highlight the importance of developed cyber incident response plans that company executives, technical support staff and legal professionals are aware of and understand. Having a plan in place, on its own, is not enough. Not only should company leaders and employees know the steps to follow in the event of breach, they should have practice following the protocols closely and efficiently, to minimize the impact of the intrusion and to prepare to notify the government of the breach in concrete terms.

Avoiding the Appearance of Insider Trading

Not only does the Equifax breach raise concerns of cyber intrusions, it also highlights the potential for insider trading before cyber incidents are publicly disclosed. An Equifax executive was alleged to have ***figured out*** that there was an intruder in the company's system prior to public disclosure. On that hunch, he sold Equifax stock. He has since pled guilty to insider trading charges and was sentenced for four months in prison.

The kind of insider trading in play here, the "***mosaic theory***," is more elusive than the traditional approach to insider trading. Under the mosaic theory, the alleged insider trader is using multiple tidbits of non-public information from several sources that, taken together, provide him or her with insight to make a logical inference on what is occurring. The insider then uses that information to trade. Here, the executive had not been directly informed of the hack, rather, he used limited facts to deduce that a hack had taken place, then sold his stock.

The exact contours of "mosaic theory" are ill-defined, but the appearance of insider trading, on its own, is enough to raise concerns for companies and their officers.

When a company officer or employee has knowledge or reason to believe that there has been a data breach, the officer or employee should proceed with caution. Even if there has been no formal announcement of a breach, the executive's decision to trade on a hunch could lead the executive and the company down a path to legal trouble.

Takeaways

The announcement of the indictment of Chinese military officers in the Equifax breach is further warning to American business. Nation-state actors are hacking into sensitive data, not just for financial gain, but for national security purposes. The hackers are sophisticated: finding and ending the breach may be difficult. The best way for companies to prepare for potential intrusions is to have a cyber incident response plan in place, to be able to exercise that plan efficiently and effectively, and to ask for the assistance of legal counsel and the government. In the wake of a potential intrusion, company leadership and employees should not be acting on the non-public information they have explicitly received or discovered regarding the breach.

Bracewell lawyers can assist in developing and exercising plans, and have experience in incident response. Please contact ***Phil Bezanson*** with questions.