White and Williams LLP

How Employers Can Respond to the Equifax Breach

By: Joshua Mooney and Linda Perkins
Cyber Law and Data Protection Alert
9.25.17

The data breach announced by Equifax in early September 2017 potentially impacted personal information of 143 million U.S. consumers – roughly half the U.S. population. According to Equifax, the breach compromised names, Social Security numbers, birth dates, addresses, and driver's license numbers. In addition, it compromised credit card numbers for approximately 209,000 people, and certain credit report dispute documents with personal information for approximately 182,000 people. In the midst of the fallout, employers are facing questions from employees and whether the employer itself could be affected.

Here are five things companies should consider when responding to questions they may receive about the Equifax breach.

1. Confirm whether the company itself is affected by the breach.

An employer should confirm whether the Equifax breach affected information provided to Equifax by the company, whether directly or indirectly. Some companies use Equifax to conduct background checks, credit checks, or other services. Other companies use third-party service providers, such as for payroll services, which use Equifax.

Importantly, if employee information was provided to Equifax by the employer or an employer's vendor, the employer should ascertain whether that information was potentially compromised. If so, the employer could face potential legal exposure and should consult a cybersecurity lawyer immediately to understand what legal obligations it may have. Employers also should review their vending contracts for risk allocation of cybersecurity events and data breaches involving information obtained by or forwarded to a third party.

2. Convey information provided by Equifax, but do not adopt it.

Equifax has released general information about the breach, including some updates on its response efforts. That information may be obtained at a dedicated website Equifax has established.

The website allows persons to inquire whether their information was compromised in the breach, and also has a section for frequently asked questions. The site also allows consumers to enroll in one year of free credit monitoring. Employers may wish to convey this information to employees, or simply notify them of Equifax's website. However, a company should not adopt or appear to endorse the veracity or precision of Equifax's statements or response efforts in its message to employees. Like many breaches, questions remain. The Equifax breach is an evolving story, and Equifax's message could change.

3. Outline proactive steps recommended by the Federal Trade Commission.

The Federal Trade Commission (FTC) provides helpful information to consumers whose information has been compromised in a data breach. An employer may pass that information along to its employees to help an employee take proactive steps. The FTC outlines steps consumers may to take to help protect themselves after a data breach, including:

- **Check your credit reports** from Equifax, Experian, and TransUnion.

- **Place a credit freeze on your files.**
- **Monitor existing credit card and bank accounts closely**.
- **Place fraud alerts** on files if a credit freeze is not instituted.
- **File taxes early**, before a scammer can.

The FTC also provides additional information an employer may pass on to its employees about identity theft.

4. Increase informational security.

Employers should instruct users and owners of computers and other digital or mobile devices that connect to the employer's data system to routinely check their operating systems for pending updates and patches. All devices, personal and business, are particularly vulnerable after issuance of software patches and updates because it is often during this time frame that hackers increase their efforts to exploit suspected vulnerabilities. Personal and other mobile devices that connect to employer systems or store employer data can be used to spread malware that can eventually compromise the employer's data system.

Also, companies and their employees should be wary of increased phishing emails, especially about the Equifax breach itself. There are those who would seek to cash in on Equifax's breach and the concern it brings consumers. Companies should warn employees about such emails, which may even appear to be official company emails sent by company officers or other leaders in the organization. These emails may request personal information not normally collected via email. Companies should consider having its information technology team set up an inbox for employees to forward suspected phishing emails to help the company identify and remove such emails from its email server, blacklist any links, and block further emails. These steps can help mitigate an employee from becoming victim to a cybersecurity event itself.

5. Review response plans, information security controls, and insurance.

The Equifax breach shows two irrefutable truths: (1) anyone can suffer a data breach, and (2) the affects on a company can be devastating. IT and in-house counsel can use notoriety of the Equifax breach as an opportunity to review information security controls and company response plans, and to obtain budget approval for an information security assessment. Risk management can assess a company's insurance coverage. Does your company have coverage for a network security event? How about loss caused by ransomware or incurred in response costs? Separate coverage may be had for computer fraud and financial loss caused by phishing scams. In addition, Human Resources can review policies and training programs to assure proper notice to employees about company policies and procedures.