Article

Equifax Data Breach: What You Should Do Now

10.04.17

The National Law Review

Equifax, one of three major U.S. credit bureaus and an aggregator of vast amounts of consumer data, announced in early September that it was the victim of a massive cyberattack and that the thieves likely accessed sensitive personal information of more than 140 million Americans. The impact and aftermath of this breach require the attention of every business that touches the web today, and individuals also should take steps to protect themselves.

WHAT IS THE SCOPE OF THE BREACH?

Equifax stores the credit histories and personal information of millions of Americans. When an unknown hacker group gained access to Equifax's enormous data trove in mid-May 2017, it made off with personally identifiable information (PII) of possibly anyone who has ever applied for credit—60 percent of the adult American population. The compromised PII includes names and associated birth dates, addresses, Social Security numbers, and driver's license numbers, as well as credit card information, credit reports, background check data, and other identity data.

In its September 7 announcement, Equifax stated that it detected the breach in late July and also confirmed that the hackers stole the credit card information of more than 200,000 people. The company has set up a website that consumers can use to determine whether their data was likely compromised and sign up for one year of free credit monitoring through another Equifax division.

WHAT SHOULD BUSINESSES DO AFTER THE EQUIFAX BREACH?

Many important lessons arise from this continually developing story. First and foremost, companies of all sizes should take cybersecurity seriously. In particular, hackers regularly target the country's nearly 30 million small and medium-sized businesses (SMBs) because they represent easier targets than large, security-conscious institutions. Indeed, half of America's SMBs have been victims of cybersecurity breaches, according to the 2017 report "State of SMB Cybersecurity in Small and Medium-Sized Businesses" from Ponemon Institute.

Approaching cybersecurity in earnest means businesses should repeatedly assess the procedures and mechanisms they have in place for protection against and detection of cyber intrusions. At a minimum, a business should invest in implementing operating system upgrades and patches as soon as software vendors release them. This mandates an emphasis on hiring skilled, well-trained information systems security personnel. Furthermore, senior managers must include in their job profile an ongoing awareness of the security measures being employed to ensure that critical systems are breach-ready, software is regularly updated, and vulnerabilities are expediently patched. Monitoring tools are also essential, even with a fully updated, fully patched system.

Focusing only on incident prevention and detection, however, simply isn't enough. Businesses should develop and institute a written plan that addresses their response to any breach. A good breach incident response plan establishes three things: a team, a process, and goals. The response team must be lean and nimble, with clearly delineated responsibilities, and each member must be engaged in testing the process with multiple exercises to ensure that the plan can be executed without hesitation when a breach occurs. The plan must also lay out attainable goals that incorporate both industry best practices and breach incident disclosure requirements for all states and territories in which the company conducts business.

A critical element of an incident response plan is the time the company takes to notify stakeholders—likely the highest priority after shutting down a breach. The reasonableness of this interval will impact the business's exposure to regulatory scrutiny and penalties as well as to lawsuits. As a best practice, a company's response plan should include a reasonable and realistic notification goal, dependent on factors laid out in the plan, such as whether law enforcement becomes involved.

Breach notification is governed by state law, and the law of each state the business touches must be consulted to determine whether its notification procedure is adequate. In most states, a "data collector" that suffers a loss of state residents' PII must notify both that state's attorney general and its affected residents "in the most expedient time possible and without unreasonable delay." La. Rev. Stat. § 51:3074. Several states impose a maximum notification delay period, which varies from 15 days (California) to 30 days (Florida) to 90 days (Connecticut). Thus, the residences of the individuals whose PII a business holds must be carefully considered in its breach incident response plan.

If your business evaluates consumer credit and relies on the credit report data maintained by any of the three major U.S. credit reporting agencies, be aware that evaluating the reported data should now include verifying the data's validity. This may slow credit origination activity, but it is a necessary side effect of this breach.

If your business deals directly with individuals, be aware that the traditional markers of identity confirmation (e.g., Social Security numbers, dates of birth) may already be in the hands of third parties with nefarious purposes. Indeed, reports confirm that this type of information is being bought and sold on the "Darknet" (the alternative information superhighway used for illegal peer-to-peer file sharing). You should investigate and consider using more stringent identity authentication prior to permitting a user to access PII or material containing PII.

WHAT SHOULD INDIVIDUALS DO TO PROTECT THEMSELVES?

Because every American has potentially been affected by the Equifax breach, the Federal Trade Commission has recommended that individuals find out whether their information was exposed, by clicking on the Equifax website at www.equifaxsecurity2017.com and following the "Potential Impact" prompt. If your data has been compromised, it may be in the hands of thieves involved in lucrative scams to, for example, commit credit card fraud or apply for multiple disability payments.

Whether or not your information has been affected, you should consider enrolling in Equifax's credit monitoring service, which will send you alerts of any suspicious activity. Equifax also recently announced that in January 2018 it will debut a "credit lock" tool, so consumers can lock and unlock access to their credit data as needed.

At a minimum, individuals should check their credit report (for free, at http://www.annualcreditreport.com) and immediately contest any activity that they did not initiate.

All three credit reporting agencies (Equifax, Experian, and Transunion) offer a "credit freeze" feature, which can be accessed online, to thwart any unauthorized credit applications using your identity. These agencies typically charge a $10 fee (unless your state restricts this fee). Lifting the freeze in order to seek credit may incur an additional $10 fee—a frustrating but inexpensive insurance that reduces the likelihood of a fraudster taking out credit in your name. Again, Equifax is offering monitoring and freeze/unfreeze services at no cost for a limited time.

Other measures every individual should consider taking against identity theft and fraud include:

- Monitor your credit card and bank accounts for invalid charges.

- If you opt against a credit freeze, place a fraud alert on your files to notify creditors that they should verify the identity of anyone seeking credit in your name.
- File your taxes as early as possible to thwart tax identity theft.

While he certainly did not have cybersecurity in mind, Benjamin Franklin's advice is apt: "An ounce of prevention is worth a pound of cure." The impact of the 2017 Equifax data breach will be felt for years to come and requires that businesses and individuals take action now. Your Social Security number, like a fingerprint (or, arguably, a mobile phone number), stays with you forever, and this vital identifier may be in the hands of crime syndicates engaged in widespread identity theft. Businesses should also be vigilant and proactive in the ongoing war against hackers, by giving highest priority to updating their digital environments and by planning and preparing for breach incidents and their aftermath.

To read more, click here.

Primary Contacts

David Roth
Houston
713.222.4045
droth@munsch.com