The Equifax Breach

Lockton Provides Guidance to Consumers and Businesses

September 2017 • Lockton Companies

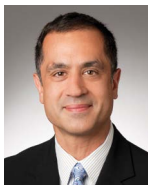
What Happened

On September 7, 2017, Equifax Inc. (NYSE: EFX) announced a cybersecurity incident potentially impacting approximately 143 million US consumers and an unspecified number of UK and Canadian citizens. Criminals exploited a US website application vulnerability to gain access to certain files between mid-May and July 2017. The information accessed included some or all of the following:

- Names
- Social Security numbers
- Birth dates, addresses
- Driver's license numbers
- Credit card information
- Credit dispute documents with personal identifying information

Equifax has found no evidence of unauthorized activity on Equifax's core consumer or commercial credit reporting databases.

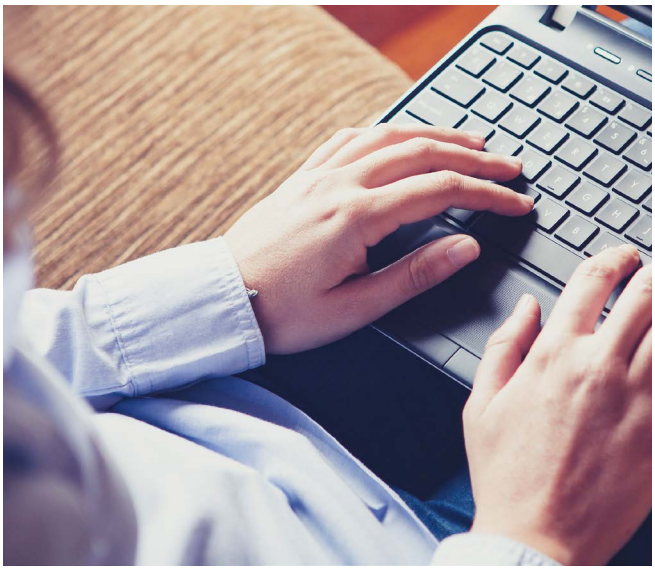
MICHAEL BORN, JD, CIPP/US
Vice President
Account Executive
816.960.9975
mborn@lockton.com



ADDITIONAL INFORMATION

Equifax is making information about the breach available at www.equifaxsecurity2017.com.

LOCKTON®



Next Steps

Individual Consumers

Equifax encourages consumers to review its dedicated website, www.equifaxsecurity2017.com, to determine if their information has been potentially impacted. The site also offers US consumers the opportunity to sign up for credit file monitoring and identity theft protection. The offering, called TrustedID Premier, includes three-bureau credit monitoring of Equifax, Experian, and TransUnion credit reports; copies of Equifax credit reports; the ability to lock and unlock Equifax credit reports; identity theft insurance; and Internet scanning for Social Security numbers. The TrustedID Premier service is provided free of charge for one year to all US consumers regardless of whether their information was compromised in the breach. The website also provides additional information on steps consumers can take to protect their personal information.

Equifax recommends that consumers with additional questions visit www.equifaxsecurity2017.com or contact a dedicated call center at 866-447-7559, which the company set up to assist consumers. The call center is open every day (including weekends) from 7:00 a.m.–1:00 a.m. Eastern time.

It has been reported that the terms of use for the credit monitoring and identity theft protection services offered by Equifax includes a release of the individuals' rights to participate in a class action lawsuit and requires them to arbitrate any dispute relating to the breach. Equifax has since clarified that the arbitration clause and class action waiver in the terms of use apply only to the services provided, and that they do not limit rights consumers may have as a result of the data breach.

In addition to the website, Equifax will send direct mail notices to consumers whose credit card numbers or dispute documents with personal identifying information were impacted.

Companies Using Equifax Services

Equifax offers many services to businesses including Affordable Care Act management, paperless payment solutions and customer account analysis. If your business uses any Equifax services, you may have provided confidential, personal information on employees or customers to Equifax and it is unclear whether or not this information was affected by the breach.

The strategy for your response, if any, should be coordinated between your internal and external legal resources.

FAQs Related to Equifax's Data Breach

If a business uses Equifax services, does the business have an obligation to notify individuals about the breach?

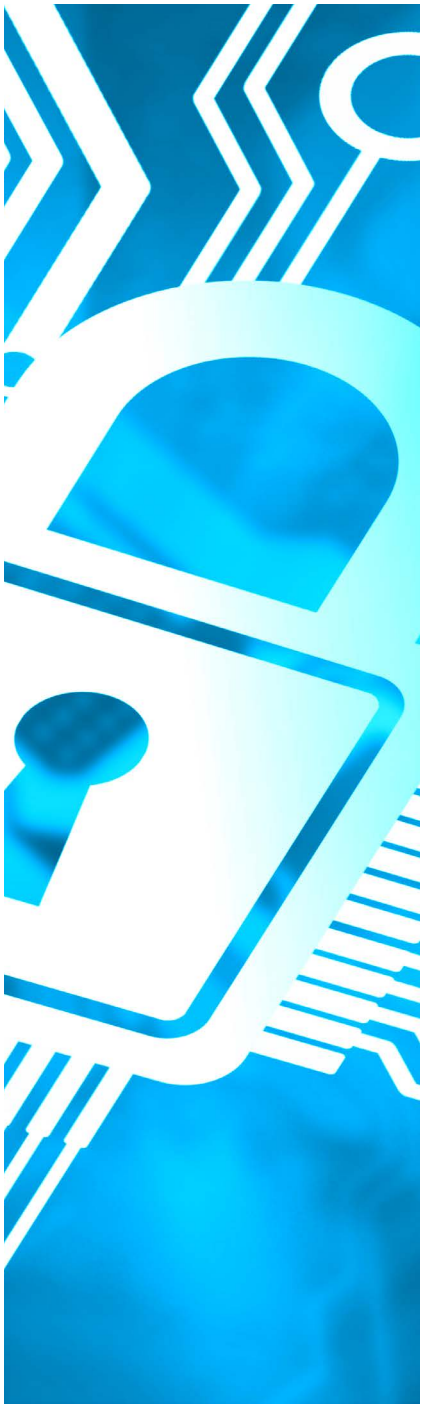
The obligation to provide notice of a breach of "personally identifiable information" (PII), such as names, Social Security numbers, or addresses is generally governed by state law, though if the data contains protected health information, federal law may also be implicated.

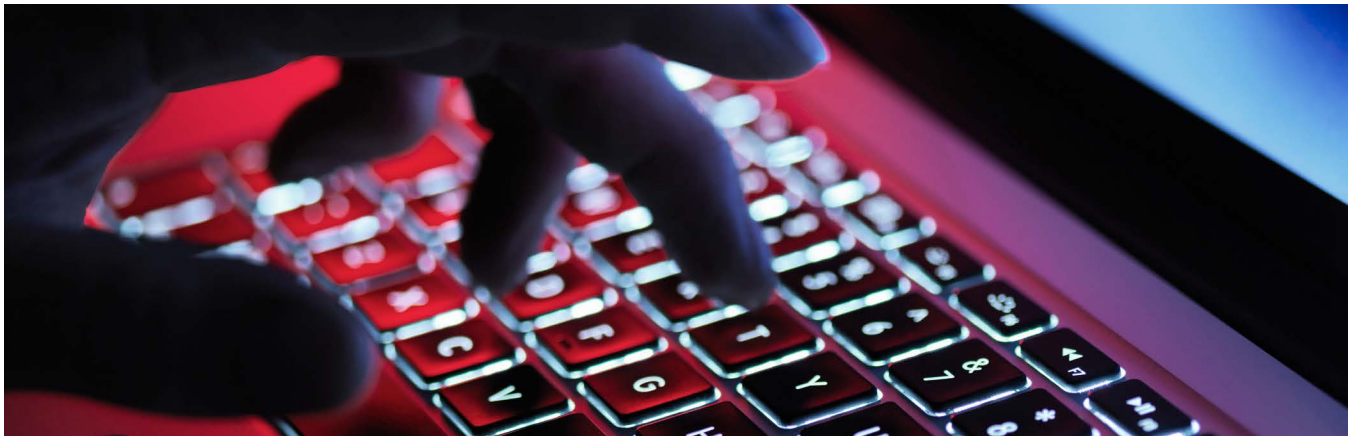
Equifax has specific notice obligations and has publicly stated it intends to notify, by direct mail, consumers whose credit card numbers or dispute documents with personal identifying information were impacted. Whether a business using Equifax as a service provider has a notice obligation to its affected employees or customers depends on a variety of factors.

Generally, it is the data owners' responsibility to supply notice to affected individuals, and in some cases, federal authorities and media outlets. However, a business and its service provider may be able to agree upon who will actually supply the notice. *In this case, it is worth noting that Equifax has indicated that it will provide direct mail notices to only a small fraction of all affected individuals.*

Is a business using Equifax as a service provider responsible for any financial consequences of the Equifax breach?

The loss resulting from the Equifax breach could be enormous. Estimates of the cost of a breach like this run from $100 to $230 per individual affected. Based on Equifax's public statements, costs to notify affected individuals and provide identity theft protection and other services should be borne, initially or ultimately, by Equifax.





If a business using Equifax services incurs costs as a result of the breach affecting their employees or customers, will the business's insurance policies pay them?

Whether any losses incurred will be covered by insurance depends on the nature of the loss and the terms of the relevant insurance policies.

If a business incurs any direct costs related to the breach, such as notification, legal, public relations, call center, or credit/identity monitoring costs, its data security and privacy liability (cyber) insurance policy may cover those expenses, especially if it is determined that the business is legally obligated to respond to the breach.

If a lawsuit or other claim is filed against the business for damages related to the Equifax breach, the privacy liability insuring agreement in the business's cyber policy may provide coverage for defense costs and damages associated with the claim.

Does a business affected by this need to provide notice to its cyber liability insurers now?

The Equifax breach may include data for which your company has an obligation to notify affected individuals. Some states require notice to be given quickly. Cyber policies are intended to cover the cost of legal advice needed to determine the existence and extent of any notice obligation as well as other expenses incurred as a result of a breach. Such policies are triggered by timely notice given to the insurer. Lockton recommends that companies give formal notice of the breach to their cyber insurers now.

Are there resources available to me to help me determine how I should respond?

Your insurance broker, in conjunction with experienced privacy counsel, can help determine the appropriate response to this breach and advise you on any insurance coverage that might be available. They can, in turn, direct you to any other resources you may need, such as public relations and communication teams, to assist in the strategy for the overall response.