Equifax settlement provides insight into regulators' thinking

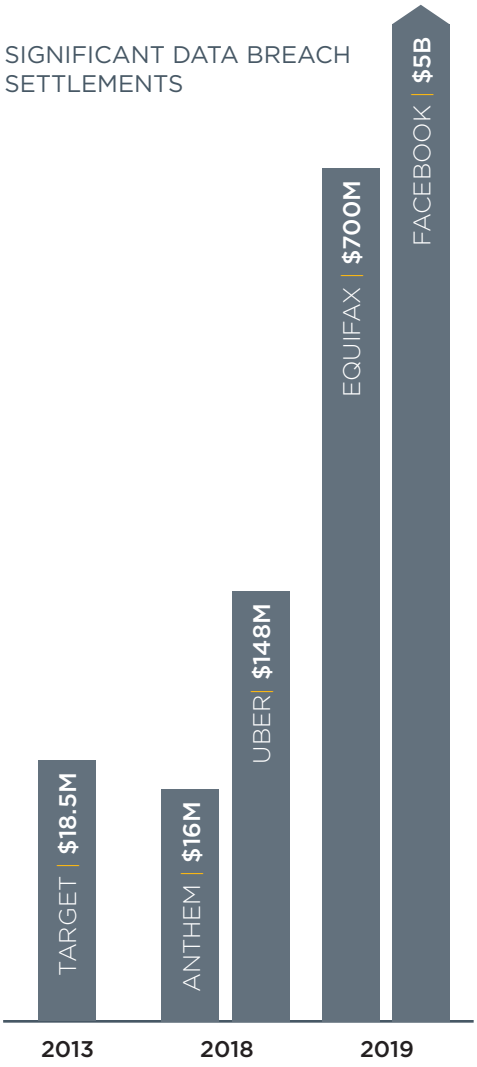
August 2019

LOCKTON®

Author

Tim Monahan
Senior Vice President
Insurance & Claims Counsel
Washington, DC

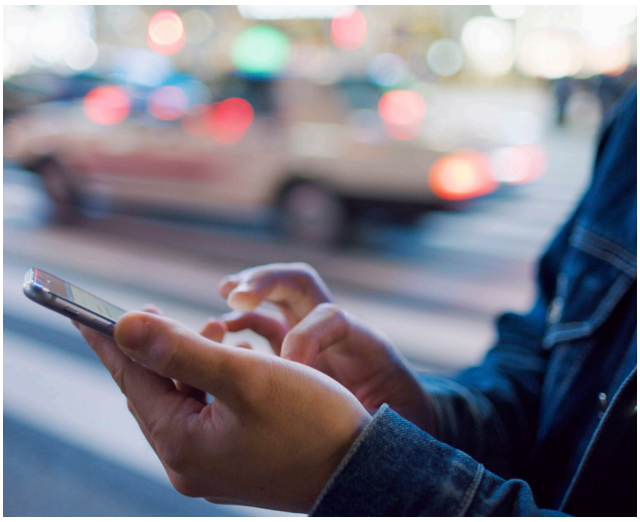
SIGNIFICANT DATA BREACH SETTLEMENTS



On July 22, 2019, the Federal Trade Commission (FTC), the Consumer Financial Protection Bureau (CFPB), 48 states and the District of Columbia and Puerto Rico announced a global settlement with Equifax arising from the company's 2017 data breach. The settlement will be effectuated through (at least) three court orders:

- A final judgment and consent decree entered in the attorney general proceeding brought in Maryland state court.
- A stipulated order for permanent injunction and monetary judgment with the Federal Trade Commission entered in the US District Court for the Northern District of Georgia.
- A stipulated order for permanent injunction and monetary judgment with the Consumer Financial Protection Bureau, also entered in the US District Court for the Northern District of Georgia.

Equifax has agreed to pay up to $700 million; $425 million of which will be paid to a consumer redress fund and $175 million will "be divided among the Attorneys General." Additional civil money penalties will be paid to the FTC and CFPB. While the Equifax settlement is dwarfed by the FTC's recent $5 billion settlement with Facebook, the settlement is much larger than others stemming from significant data breaches. For example, in 2018 Uber reached a $148 million settlement with all US states for a breach affecting 57 million accounts. Also in 2018, Anthem paid $16 million to the US Department of Health and Human Services and the Office for Civil Rights in connection with the breach of the protected health information of 79 million people. As a result of its 2013 breach of payment card information of 40 million shoppers, Target paid an $18.5 million settlement to 47 US states.



While the size of the Equifax settlement is noteworthy by itself, the information security requirements imposed on Equifax by the regulators are also informative. The three separate court orders were clearly negotiated in concert and include similar provisions. There are numerous, detailed information security requirements that Equifax must follow, which provides insight into the standards of conduct that regulators expect from corporations in possession of consumer personal information.

The information security requirements include three categories: "information security program," "personal information safeguards and controls," and "specific technical safeguards and controls." Companies with complex information security environments and who are in possession of a substantial number of consumer records should read the orders closely. Many of the safeguards and controls imposed on Equifax are likely already implemented by many companies. However, the imposition of these requirements by regulators reflects their current view of what security measures are important, which is enlightening standing alone. Some of the highlights of the requirements imposed include:

Information security program

- "Equifax shall implement, maintain, regularly review and revise, and comply with a comprehensive information security program."
- Equifax is required to employ a Chief Information Security Officer (CISO) who is required to report to the Board of Directors.
- The CISO must report any network security breach to the CEO and to the Board within 48 hours of discovery.
- Must employ a Business Information Security Officer in each business unit of the company "responsible for implementing, maintaining and monitoring the Information Security Program for that business unit."
- Maintain a written incident response plan that addresses eight separate areas and conduct "at a minimum" biannual table-top exercises "to test and assess its preparedness to respond to a security event."

Personal information safeguards and controls

- Equifax must encrypt personal information or implement equivalent controls to protect personal information.
- Equifax "shall make reasonable efforts to reduce its use and storage of consumer Social Security numbers," and conduct an internal study that must be provided to the California attorney general's office.
- Social Security numbers must be encrypted during storage and transmission.

Specific technical safeguards and controls

- Segmentation of networks required.
- Ongoing penetration testing and risk assessment required, including "at least once weekly vulnerability scan of all systems" with reports available to a third-party assessor.
- "Administrative level passwords shall be encrypted."
- CISO must be notified of any security event within eight hours.
- Conduct asset inventories and identify each security update and patch applied to assets.

Can insurance cover any of these costs?

Cyber insurance can cover many of the costs that Equifax has incurred in this process. A good cyber insurance program can cover most, and potentially all, of the types of costs Equifax incurred in this settlement. Companies should make sure their policies expressly cover any amounts deposited into a consumer redress fund. The policies should also cover civil fines and penalties imposed by a government entity through a regulatory action where insurable by law. These coverages are available in the cyber insurance marketplace and should be a key consideration when evaluating policy forms.

A strong cyber policy should also respond to the forensic and legal fees incurred to respond to the breach and to defense costs for civil litigation arising from a data breach, including claims brought by federal and state (and international) regulators.

It is important to realize that the costs Equifax will incur in responding to the non-monetary provisions of the settlement will probably not be covered by a cyber policy. Policies are typically written to exclude such costs.

The staggering amount of costs Equifax faces from the settlement alone reflects the importance of purchasing appropriate cyber insurance limits. Companies should continually evaluate how they would respond to a significant cyber event and what role insurance would play. While the Equifax figures are high, the current political environment suggests that politicians and regulators intend to continue to seek even greater financial consequences for similar events.[1]

[1] Sen. Mark Warner, D-Va., issued a statement that if a bill he has sponsored titled "The Data Breach Prevention and Compensation Act" had been in effect at the time of this event, Equifax "would have had to pay at least $1.5 billion for their failure to protect Americans' personal information."

- RISK MANAGEMENT
- EMPLOYEE BENEFITS
- RETIREMENT SERVICES

LOCKTON.COM