

# Equifax to Pay \$575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach

[FTC ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related](https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related)

July 19,  
2019




**NOTE:** The FTC hosted an *IN-PERSON* press conference at FTC Headquarters, 600 Pennsylvania Ave, NW, Washington D.C., on July 22, 2019. [Watch archival video of the press conference.](#)

Participants included: FTC Chairman Joe Simons, CFPB Director Kathy Kraninger, and Maryland Attorney General Brian Frosh.

Equifax Inc. has agreed to pay at least \$575 million, and potentially up to \$700 million, as part of a global settlement with the Federal Trade Commission, the Consumer Financial Protection Bureau (CFPB), and 50 U.S. states and territories, which alleged that the credit reporting company's failure to take reasonable steps to secure its network led to a data breach in 2017 that affected approximately 147 million people.

In its [complaint](#), the FTC alleges that Equifax failed to secure the massive amount of personal information stored on its network, leading to a breach that exposed millions of names and dates of birth, Social Security numbers, physical addresses, and other personal information that could lead to identity theft and fraud.

**The Equifax Breach – A Global Settlement**

-  \$575,000,000+ settlement
-  **Free** credit monitoring and identity theft services
-  Strong **data security** requirements

→ **Learn more: [ftc.gov/Equifax](https://www.ftc.gov/Equifax)**

Source: Federal Trade Commission | FTC.gov

As part of the [proposed settlement](#), Equifax will pay **\$300 million** to a fund that will provide affected consumers with credit monitoring services. The fund will also compensate consumers who bought credit or identity monitoring services from Equifax and paid other out-of-pocket expenses as a result of the 2017 data breach. Equifax will add up to \$125 million to the fund if the initial payment is not enough to compensate consumers for their losses. In addition, beginning in January 2020, Equifax will provide all U.S. consumers with six free credit reports each year for seven years—in addition to the one free annual credit report that Equifax and the two other nationwide credit reporting agencies currently provide.

The company also has agreed to pay \$175 million to 48 states, the District of Columbia and Puerto Rico, as well as \$100 million to the CFPB in civil penalties.

“Companies that profit from personal information have an extra responsibility to protect and secure that data,” said FTC Chairman Joe Simons. “Equifax failed to take basic steps that may have prevented the breach that affected approximately 147 million consumers. This settlement requires that the company take steps to improve its data security going forward, and will ensure that consumers harmed by this breach can receive help protecting themselves from identity theft and fraud.”

“Today’s announcement is not the end of our efforts to make sure consumers’ sensitive personal information is safe and secure. The incident at Equifax underscores the evolving cyber security threats confronting both private and government computer systems and actions they must take to shield the personal information of consumers. Too much is at stake for the financial security of the American people to make these protections anything less than a top priority. For consumers impacted by the Equifax breach, today’s settlement will make available up to \$425 million for time and money they spent to protect themselves from potential threats of identity theft or addressing incidents of identity theft as a result of the breach. We encourage consumers impacted by the breach to submit their claims in order to receive free credit monitoring or cash reimbursements,” said Consumer Financial Protection Bureau Director Kathleen L. Kraninger.

### **Company’s Security Failures**

The FTC alleges that Equifax failed to patch its network after being alerted in March 2017 to a critical security vulnerability affecting its ACIS database, which handles inquiries from consumers about their personal credit data. Even though Equifax’s security team ordered that each of the company’s vulnerable systems be patched within 48 hours after receiving the alert, Equifax did not follow up to ensure the order was carried out by the responsible employees.

In fact, Equifax did not discover that its ACIS database was unpatched until July 2017, when its security team detected suspicious traffic on its network. A company investigation revealed that multiple hackers were able to exploit the ACIS vulnerability to gain entry to Equifax’s network, where they accessed an unsecured file that included administrative credentials stored in plain text. These credentials allowed the hackers to gain access to vast amounts of consumers’ personally identifiable information and to operate undetected on Equifax’s network for months.

The hackers targeted Social Security numbers, dates of birth, and other sensitive information, mostly from consumers who had purchased products from Equifax such as credit scores, credit monitoring, or identity theft prevention services. For example, hackers stole at least 147 million names and dates of birth, 145.5 million Social Security numbers, and 209,000 payment card numbers and expiration dates.

Hackers were able to access a staggering amount of data because Equifax failed to implement basic security measures, according to the complaint. This includes failing to implement a policy to ensure that security vulnerabilities were patched; failing to segment its database servers to block access to other parts of the network once one database was breached; and failing to install robust intrusion detection protections for its legacy databases. In addition, the FTC also alleges that Equifax stored network credentials and passwords, as well as Social Security numbers and other sensitive consumer information, in plain text.

Despite its failure to implement basic security measures, Equifax’s privacy policy at the time stated that it limited access to consumers’ personal information and implemented “reasonable physical, technical and procedural safeguards” to protect consumer data.

The FTC alleges that Equifax violated the FTC Act’s prohibition against unfair and deceptive practices and the Gramm-Leach-Bliley Act’s Safeguards Rule, which requires financial institutions to develop, implement, and maintain a comprehensive information security program to protect the security, confidentiality, and integrity of customer information.

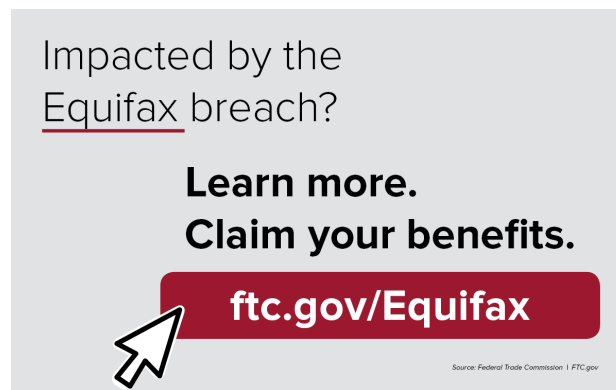
### **Settlement Requirements**

In addition to the monetary relief to consumers, Equifax is also required to implement a comprehensive information security program requiring the company to take several measures including:

- Designating an employee to oversee the information security program;

- Conducting annual assessments of internal and external security risks and implementing safeguards to address potential risks, such as patch management and security remediation policies, network intrusion mechanisms, and other protections;
- Obtaining annual certifications from the Equifax board of directors or relevant subcommittee attesting that the company has complied with the order, including its information security requirements;
- Testing and monitoring the effectiveness of the security safeguards; and
- Ensuring service providers that access personal information stored by Equifax also implement adequate safeguards to protect such data.

The proposed settlement also requires the company to obtain third-party assessments of its information security program every two years. Under the order, the assessor must specify the evidence that supports its conclusions and conduct independent sampling, employee interviews, and document reviews. The order grants the Commission the authority to approve the assessor for each two-year assessment period. The order also requires Equifax to provide an annual update to the FTC about the status of the consumer claims process.



Finally, the FTC encourages Equifax employees who believe the company is failing to adhere to its data security promises to email the FTC at [equifax@ftc.gov](mailto:equifax@ftc.gov). Consumers can find out more about the settlement at [ftc.gov/Equifax](https://ftc.gov/Equifax).

The Commission vote authorizing the staff to file the complaint and proposed stipulated final order was 5-0. The FTC expects to file the complaint and proposed order today in the U.S. District Court for the Northern District of Georgia.

**NOTE:** The Commission files a complaint when it has “reason to believe” that the named defendants are violating or are about to violate the law and it appears to the Commission that a proceeding is in the public interest. Stipulated final orders have the force of law when approved and signed by the District Court judge.

The Federal Trade Commission works to promote competition, and protect and educate consumers. You can learn more about consumer topics and file a consumer complaint online or by calling 1-877-FTC-HELP (382-4357). Like the FTC on , follow us on , read our blogs, and subscribe to press releases for the latest FTC news and resources.