Published on *The National Law Review* https://natlawreview.com

FTC and Equifax Reach Historic Settlement

Article By:

Christopher J. Buontempo

Cynthia J. Larose

The Federal Trade Commission ("FTC"), the Consumer Financial Protection Bureau, and 50 U.S. states and territories, have reached a global settlement agreement with Equifax Inc. ("Equifax"), according to which, Equifax agreed to pay at least $575 million, and potentially up to $700 million, in connection with Equifax's massive 2017 data breach that affected 147 million people.

FTC Chairman Joe Simons provided the following statement: "Companies that profit from personal information have an extra responsibility to protect and secure that data," Chairman Simons went on to say, "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."

The Complaint

According to the **FTC** complaint **against Equifax, attackers were able to steal approximately 147 million names and dates of birth, 145.5 million SSNs, 99 million physical addresses, 20.3 million telephone numbers, 17.6 million email addresses, and 209,000 payment card numbers and expiration dates**, among other things, from Equifax in the 2017 breach. According to the FTC, this resulted from a series of basic security failures that Equifax failed to address, including, Equifax's failure to properly patch a known critical vulnerability for four months after becoming aware of the vulnerability, misguided reliance on improperly configured vulnerability scanners, failure to segment database servers, failure to implement reasonable access controls, storing sensitive information in plain text, and failure to implement robust intrusion detection. The FTC also noted in its complaint that Equifax knew of its security failures since 2014, and according to Equifax's own documents, one of Equifax's systems was self-described as "archaic" and used "antiquated technology."

According to the FTC, "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 also alleged that Equifax violated the FTC's prohibition against unfair and deceptive trade practices,

as well as the Gramm-Leach-Bliley Act's Safeguards Rule.

The Settlement

The proposed settlement includes establishment of a $300 million fund, with a potential additional $125 million, to provide affected consumers with credit monitoring services, and to compensate consumers who bought credit or identity monitoring services from Equifax and paid other out-of-pocket expenses resulting from the 2017 data breach. Equifax also agreed to pay $175 million to U.S. states and territories, and pay $100 million to the Consumer Financial Protection Bureau in the form of civil penalties. In addition, Equifax will provide all affected consumers with six free credit reports each year for seven years (in addition to the one free annual credit report currently provided by Equifax and the other two national credit reporting agencies).

The proposed settlement goes beyond monetary relief. Equifax must also implement a comprehensive information security program to include the following:

- 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.

Equifax is also required to undergo third-party assessments of its information security program every two years, and provide an annual update on the status of the consumer claims process to the FTC.

FTC Commissioner Rebecca Kelly Slaughter had this to say about the settlement in a press release, "But this relief is no substitute for preventing the breach in the first place, and this breach was preventable. Equifax's alleged violations included failures to address unpatched critical and high-risk vulnerabilities across systems that persisted for months at a time. In other words, internal warnings went unheeded."

Takeaways

This historic settlement provides insight into what the FTC considers "basic" security controls to include, and serves as a stark reminder to companies to review their own information security programs. Specifically, companies should ensure that their security programs include the following "basics":

- Update and patch software;

- Do not rely on automated processes that are not updated or properly configured;
- Adequately monitor your network for intrusions;
- Segment your network; and
- Implement proper access controls.

Additionally, companies should review their privacy policies to ensure that all claims and representations about information security are accurate and up to date.

Consumers seeking to file a claim in connection with the breach may do so here: https://www.equifaxbreachsettlement.com/

National Law Review, Volumess IX, Number 211