7 TAKEAWAYS FROM A RECENT FTC ENFORCEMENT ACTION IN LIGHT OF THEFT OF PRIVATE INFORMATION

Noel D. Humphreys Connell Foley LLP

The Federal Trade Commission (FTC) recently settled a matter with the owners of an online retailer related to statements and actions the company made regarding its privacy and security measures. At issue were customer-facing statements made by the company and its responses to unauthorized access to customer personal information the company was holding. The settlement orders provide a glimpse of what the FTC thinks responsible actors should be doing about protecting personal data and what the FTC may treat as "deceptive" behavior.

The settlement suggests seven takeaways.

1 Payment is just the first penalty

The immediate, out-of-pocket costs for the company's alleged deceptive practices, mostly in 2018 into 2020, were half a million dollars payable to the FTC.

2 Protect the data

If a company is going to collect and hold customers' personal information, and tell customers their information is secure, the company needs to make a genuine effort to make that a reality. The company advertised that it used "best and most accepted methods and technologies" to ensure collected personal information was "safe and secure." The FTC found that statement not to be true. At least one hacker stole personal information and sold it on the dark web. The FTC alleged the company "failed to implement readily available protections" against "reasonably foreseeable vulnerabilities." The FTC cited five different styles of often-used, unauthorized access known in the industry that the company failed to protect against. Among other issues, the company kept customer Social Security numbers in clear text, unencrypted, and never deleted customer information. The company also used an algorithm for password encryption that NIST (the National Institute of Standards and Technology) had "deprecated" years before. The FTC said the company needed to comply with its own written security procedures and to "implement reasonable procedures to prevent, detect or investigate an intrusion."

3 Don't let it happen AGAIN

After an initial breach of company servers, don't let it happen again. The company learned in 2019 that customer information was being sold on the dark web, but the company did not tell customers their information had been stolen. The company merely asked customers to change their passwords. The FTC adjudged that to be an inadequate response. The hackers had taken password reset information. Even when a customer did reset a password, the company made no effort to verify the person resetting the password was not an unauthorized intruder.

4 Do what you say you will do

A company needs to do what it tells the public it's going to do, as the FTC has long insisted. In this matter, the company billed itself as complying with the "shield" arrangement the U.S. had worked out with the European Union in conformity with European privacy law. Under that arrangement, a customer had the authority to require the company to delete the customer's information. In fact, when the company had received such a request, the FTC said, the company did not actually delete the customer information on its servers.

5 Protect the future

A company's buyer may become subject to onerous future obligations arising out of the predecessor's unlawful behavior. In this instance, the company changed hands in 2020. In the FTC settlement, the prior owner became liable for the $500,000 payment, but the new owner, like the old owner, was forced to agree to 20 years of annual reporting of responsible online digital behavior and ongoing security assessments by outside professionals.

6 It's so much more than just a penalty fee

A settlement with the FTC involves more than a $500,000 out-of-pocket settlement cost. Both the prior owner and the new owner had to undertake a "comprehensive information security program" immediately and over the next two decades regarding "collection, maintenance, use or disclosure of, or provision of access to" personal information, broadly defined. That program requires thorough internal reports annually and after a security event, as well as retention of a "qualified, objective, independent third-party professional" whose assessments are due at the FTC every 24 months.

7 You need to know what "personal information" data really means

The FTC's settlement orders view "personal information" expansively. The definition in the settlement order includes not only names, addresses and Social Security numbers but also "a persistent identifier," such as a customer number held in a "cookie," a static Internet protocol (IP) address, a mobile device identifier or processor serial number, as well as authentication credentials, such as a user ID, password and related security questions and answers.

A settlement agreement such as this one defining how to go about protecting "privacy, security, confidentiality and integrity" of "personal information" broadly defined, may set standards not only for clients but also for law firms.

For further information, as published in the Federal Register, click here.

Noel Humphreys, Of Counsel at Connell Foley in Roseland, New Jersey, focuses on business transactions, lending transactions, organizational governance and intellectual property. He advises on transactions that often involve leveraging the value of patents, trademarks, copyrights and trade secrets, and he has a particular interest in privacy issues and data protection.