Akin®

FTC on Data Breach: Complying with Breach Notification Laws Might Not Be Enough

June 1, 2022

Reading Time : **4 min**

By: Natasha G. Kohne, Joseph Hold

The Federal Trade Commission (FTC) has warned companies that compliance with data breach notification laws might not be enough: an entity that suffers a breach may violate Section 5 of the FTC Act if it fails to disclose information to help parties mitigate reasonably foreseeable harm, "[r]egardless of whether a breach notification law applies."[1].

The FTC explained in a prior blog post that Section 5's prohibition of deceptive acts and practices[2] creates a de facto breach disclosure requirement distinct from state breach disclosure requirements. The FTC is concerned that breach disclosure deficiencies may hinder the mitigation efforts of other organizations and consumers, exposing them to foreseeable harms such as "identify theft, loss of sensitive data, or financial impacts."[3] In the FTC's view:

- A failure to timely notify a party of a breach may constitute an unfair trade practice where that failure increases the likelihood that the party will suffer harm.
- Inaccurate or incomplete breach notifications may constitute a deceptive trade practice.[4]

The FTC points to four enforcement examples to illustrate this stance on breach disclosure:

- *CafePress*

The recently finalized CafePress settlement involved FTC allegations of failing to timely notify consumers and businesses after a breach. According to the FTC, CafePress notified parties five months after names, email addresses, login information, Social Security numbers and financial information were compromised in a February 2019 breach.[5] While CafePress reset passwords

after the breach, it retained an automated password reset process that used compromised security questions, resulting in accounts being compromised again. Without admitting or denying fault, Cafepress settled with the FTC for $500,000 and an agreement to implement specific cybersecurity requirements, including a new procedure for breach reporting.[6]

- *Uber*

In an October 2018 settlement, the FTC alleged that Uber's claim that it would reasonably secure consumer information was deceptive partly due to the company's year-long delay in notifying consumers after a breach occurred.[7] The FTC complaint alleges that after one data breach in November 2016, which compromised names, email addresses, phone numbers and driver's license numbers, Uber paid hackers $100,000 and did not disclose the breach to affected customers until November 2017.[8] Without admitting or denying fault, Uber agreed to a final settlement involving a slew of prescriptive requirements, including the implementation of a comprehensive privacy program.[9]

- *SpyFone*

In a September 2021 complaint, FTC alleged that SpyFone made misleading statements that it had hired a forensic firm and cooperated with law enforcement.[10]SpyFone, a maker of monitoring devices and services for parents and employers, allegedly both illegally harvested private information and exposed it to hackers. After a breach occurred in August 2018, the company promised consumers it would work with a third-party security firm and law enforcement, yet failed to follow through, according to the complaint. Without admitting or denying fault, the company was ordered to delete the surveillance data it had gathered and inform customers.

- *SkyMed*

In February 2021, the FTC alleged that travel emergency services provider SkyMed's breach notification was deceptive because it falsely claimed the company's investigation found that no consumer health information was compromised. In May 2019, SkyMed emailed notification of a breach to affected customers, claiming that SkyMed had investigated the incident and "some old data may have been exposed temporarily" but no medical information had been misused.[11]According to the FTC complaint, this was misleading because SkyMed had deleted the compromised database without verifying the types of the information stored

therein.[12]Without admitting or denying fault, SkyMed was ordered to notify affected customers and implement a comprehensive information security program.

Takeaway

Effective and thorough breach disclosure is becoming an important item in the modern company's toolbox. The recent actions and statements from the FTC, as well as actions from other agencies such as the Securities and Exchange Commission (SEC), demonstrate the pitfalls of insufficient breach disclosure. The FTC's stance on data breach disclosure demonstrates that technical compliance with state breach disclosure laws may not be sufficient: any disclosure and investigation must also be reasonable, timely, accurately describe steps that were taken and enable consumers to take actions to protect their information. To avoid running afoul of FTC enforcement, companies should ensure that their breach disclosure procedures include means of accurately and completely describing the response, as well as thorough assessments covering the risks to those affected by a breach.

Please contact a member of Akin's cybersecurity, privacy and data protection team if you have any questions about how this statement may impact your company or your company's information security program.

---

[1]Federal Trade Comm'n, *Security Beyond Prevention: The Importance of Effective Breach Disclosures*, (May 20, 2022), hereinafter "FTC blog post," available at https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2022/05/security-beyond-prevention-importance-effective-breach-disclosures.

[2]15 U.S.C. 45.

[3]*Id*.

[4] FTC blog post at 1.

[5]Press Release, *FTC Takes Action Against CafePress for Data Breach Cover Up*, Federal Trade Comm'n (March 15, 2022) available at https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-cafepress-data-breach-cover.

[6]*Id*.

[7] *Complaint*, Uber Technologies, Inc., FTC Docket No. C-4662 (October 28, 2018), available at https://www.ftc.gov/system/files/documents/cases/152_3054_c-4662_uber_technologies_revised_complaint.pdf.

[8] *Id*. at 6.

[9] *Decision and Order*, Uber Technologies, Inc., FTC Docket No. C-4662 (October 28, 2018), available at https://www.ftc.gov/system/files/documents/cases/152_3054_c-4662_uber_technologies_revised_decision_and_order.pdf.

[10] Press Release, F*TC Bans SpyFone and CEO from Surveillance Business and Orders Company to Delete All Secretly Stolen Data*, Federal Trade Comm'n (September 1, 2021), available at https://www.ftc.gov/news-events/news/press-releases/2021/09/ftc-bans-spyfone-ceo-surveillance-business-orders-company-delete-all-secretly-stolen-data.

[11] *Complaint*, SkyMed International, Inc., FTC Docket No. C-4732 (January 26, 2021), available at https://www.ftc.gov/system/files/documents/cases/c-4732_skymed_final_complaint.pdf.

[12] *Id*. at 5.

Categories

Data Breach | Cybersecurity & Information Security | Federal Privacy Policy | FTC | Privacy & Cybersecurity

York limited liability partnership authorized and regulated by the Solicitors Regulation Authority under number 267321. A list of the partners is available for inspection at Eighth Floor, Ten Bishops Square, London E1 6EG. For more information about Akin Gump LLP, Akin Gump Strauss Hauer & Feld LLP and other associated entities under which the Akin Gump network operates worldwide, please see our Legal Notices page.