ALSTON & BIRD

WWW.ALSTON.COM

Consumer Protection/FTC ADVISORY ■

MAY 25, 2022

FTC Guidance Creates New Breach Notification Obligations

By **Alex Brown**, **Kathleen Benway**, *and* **Dan Felz**

On May 20, 2022, the Federal Trade Commission (FTC) issued guidance that uses Section 5 of the FTC Act to create new breach notification obligations. These obligations appear to go beyond existing U.S. and EU laws and potentially require companies to report breaches that existing statutes do not require to be reported. If enforced, the FTC's guidance could represent a significant update to the U.S. law on breach reporting, potentially more closely aligning the U.S. with EU standards.

The FTC followed up recent enforcement activity in the data breach space by issuing guidance to any company facing a security incident: strong security and breach detection are not enough – timely, accurate, and actionable security disclosures are also necessary to avoid potential liability under Section 5 of the FTC Act. The FTC's "Team CTO" and the Division of Privacy and Identity Theft Protection published guidance on May 20, 2022 in the Tech@FTC Blog advising that the FTC Act creates what it calls "a de facto breach disclosure requirement" because the failure to disclose will, for example, increase the likelihood that affected parties will suffer harm and may constitute an unfair practice under Section 5. As a reminder, an act or practice is unfair if it causes or is likely to cause substantial consumer injury that consumers cannot reasonably avoid and for which there are no countervailing benefits to consumers or competition.

In the blog post, the FTC acknowledged the importance of effective detection and response programs, which enable companies to (1) take remedial actions "to counter, prevent, or mitigate an attack before its worse potential consequences are realized"; (2) "prevent and minimize consumer harm from breaches by protecting consumers against cyberattacks"; (3) "provide valuable information to the prevention function of a security team, including information on what types of attack surfaces attackers are targeting, so security leaders can determine what investments in information technology are most impactful for security"; and (4) remove an "attacker and allow for post-breach remedial measures."

The FTC's guidance focuses on the fourth prong – the potential for Section 5 liability arising out of those post-breach remedial measures – namely, the breached company's disclosure obligations. According to

This advisory is published by Alston & Bird LLP to provide a summary of significant developments to our clients and friends. It is intended to be informational and does not constitute legal advice regarding any specific situation. This material may also be considered attorney advertising under court rules of certain jurisdictions.

the FTC, the legal analysis under the state- and sector-specific federal data breach notification laws is only the beginning of that analysis. The FTC contends that "[r]egardless of whether a breach notification law applies, a breached entity that fails to disclose information to help parties mitigate reasonably foreseeable harm may violate Section 5 of the FTC Act." The staff points to the FTC's recent enforcement actions against CafePress, Uber, SpyFone, and SkyMed as examples of when a company's post-breach behavior ran afoul of Section 5. The FTC alleges that CafePress failed "to timely notify consumers and other relevant parties after data breaches, thereby preventing parties from taking measures to mitigate harm." Similar allegations followed Uber's failure to disclose a breach for over a year. Complaints against SpyFone and SkyMed included allegations of public misstatements following a breach.

The FTC appears poised to closely scrutinize companies that fail to timely and accurately disclose security incidents when those failures could hinder consumers from taking critical actions to mitigate foreseeable harms like identity theft, loss of sensitive data, or financial impacts. In doing so, the FTC appears to move closer to the standard codified in Article 34 of the General Data Protection Regulation (GDPR), which requires companies to notify data subjects whenever incidents affecting personal data create a "high risk" to their rights and freedoms. However, the FTC's standard could potentially be broader than the GDPR, since the FTC states notice is required not just to consumers but also to "other relevant parties," suggesting the FTC guidance could require notification in the business-to-business context as well. To avoid potential FTC liability, companies will need to engage in this analysis in addition to the approach more focused on personally identifiable information outlined in the state- and sector-specific federal notification statutes.

You can subscribe to future *Consumer Protection/FTC* advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or any of the following:

Kathleen Benway
202.239.3034
kathleen.benway@alston.com

Kelly Connolly Barnaby
202.239.3687
kelly.barnaby@alston.com

Alexander G. Brown
404.881.7943
alex.brown@alston.com

Kristine McAlister Brown
404.881.7584
kristy.brown@alston.com

Patrick Eagan-Van Meter
704.444.1447
patrick.eagan-vanmeter@alston.com

Joseph H. Hunt
202.239.3278
404.881.7811
jody.hunt@alston.com

Robert H. Poole II
404.881.4547
robert.poole@alston.com

T.C. Spencer Pryor
404.881.7978
spence.pryor@alston.com

John C. Redding
704.444.1070
john.redding@alston.com

ALSTON & BIRD

WWW.ALSTON.COM

© ALSTON & BIRD LLP 2022

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86.10.85927500
BRUSSELS: Rue Guimard 9 et Rue du Commerce 87 ■ 3rd Floor ■ 1000 Brussels ■ Brussels, 1000, BE ■ +32.2.550.3700 ■ Fax: +32.2.550.3719
CHARLOTTE: One South at The Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
FORT WORTH: Bank of America Tower ■ 301 Commerce ■ Suite 3635 ■ Fort Worth, Texas, USA, 76102 ■ 214.922.3400 ■ Fax: 214.922.3899
LONDON: 4th Floor ■ Octagon Point, St. Paul's ■ 5 Cheapside ■ London, EC2V 6AA, UK ■ +44.0.20.3823.2225
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 1950 University Avenue ■ Suite 430 ■ East Palo Alto, California, USA 94303 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333