June 28, 2022

FTC and Breach Notification – Time to Review Your Incident Response Plan?

On May 20, the Federal Trade Commission (FTC) published a blog post titled "Security Beyond Prevention: The Importance of Effective Breach Disclosures" in which the FTC takes the position that in some cases the Federal Trade Commission Act (FTC Act) creates a "de facto breach disclosure requirement" despite there being no explicit section of the act setting forth such a requirement. Specifically, the FTC writes that "regardless of whether a breach notification law applies," the failure to "disclose information to help parties mitigate reasonably foreseeable harm may violate Section 5 of the FTC [Federal Trade Commission] Act." Businesses should consider how this new de facto breach notification guidance from the FTC affects or should be taken into account in their data breach response plans.

The blog post begins by discussing the importance of security breach detection and response to maintaining reasonable data security. The FTC writes that effective detection and response programs can, among other things, prevent and minimize consumer harm (e.g., financial harm or the loss of personal information), provide feedback to the prevention function of a business's security team, and enable post-breach remedial measures, such as notifying customers so they may, in turn, take their own remedial actions.

The FTC then proceeds to explain that it may be a violation of the FTC Act should a business fail "to disclose information" (i.e., notify someone of a breach) to help parties mitigate harm. In support of this conclusion, the FTC cites to several recent enforcement actions in which the FTC alleged that businesses' failure to timely notify consumers or issue accurate statements to consumers resulted in unfair trade practices. Building from these enforcement actions, the FTC advises that "these cases stand for the proposition that companies have legal obligations with respect to disclosing breaches, and that these disclosures should be accurate and timely."

Noncompliance with the FTC Act may result in significant legal, financial and reputational risks. The FTC may bring administrative actions or a federal lawsuit against noncompliant companies, require companies to undertake costly remedial actions, issue injunctions bringing companies' businesses to a halt, or impose costly penalties. Penalties are routinely adjusted for inflation, and the current maximum penalty is $46,517 per violation—but in a situation involving a breach of the personal information of many individuals, when each person is counted as a violation, that could easily mean a six- or seven-figure penalty.

So what should a business do about this? We have three suggestions: (1) ensure that the business has in place an adequate incident response plan; (2) ensure that privacy and security practice representations are accurate and not misleading (think of a website or application privacy policy, for example); and (3) when faced with a data security incident, weigh whether notice should be provided even if not legally required by the applicable federal/state law, particularly in cases where there is a risk of harm to the individuals whose information was accessed/acquired. An example of the latter may be deciding to disclose a data security incident involving paper records when the applicable state data breach notification law applies to electronic information only.

Would you like to receive our *Day Pitney C.H.A.T. Newsletter?* Sign up here.

Authors



Kritika Bharadwaj
Partner

New York, NY | (212) 297-2477

kbharadwaj@daypitney.com



Heather Weine Brochin
Partner

Parsippany, NJ | (973) 966-8199

New York, NY | (212)-297-5800

hbrochin@daypitney.com



Alex P. Garens
Partner

Boston, MA | (617) 345-4872

agarens@daypitney.com



William J. Roberts
Partner

Hartford, CT | (860) 275-0184

wroberts@daypitney.com



Mindy S. Tompkins
Partner

Hartford, CT | (860) 275-0139

mtompkins@daypitney.com



Stephanie M. Gomes-Ganhão
Associate

Hartford, CT | (860) 275-0193

sgomesganhao@daypitney.com



John F. Kaschak
Associate

Parsippany, NJ | (973) 966-8034

jkaschak@daypitney.com



Phoebe A. Roth
Senior Associate

New Haven, CT | (203) 752-5045

proth@daypitney.com