Federal Bill Would Broaden FTC’s Role in Cybersecurity and Data Breach Disclosures

Article By

Kristin L. Bryan
Jeffrey L. Turner

Squire Patton Boggs (US) LLP
Consumer Privacy World

Related Practices & Jurisdictions

- Communications, Media & Internet
- Antitrust & Trade Regulation
- Election Law / Legislative News
- All Federal

Tuesday, August 2, 2022

Last week, the House Energy and Commerce Committee advanced H.R. 4551, the “Reporting Attacks from Nations Selected for Oversight and Monitoring Web Attacks and Ransomware from Enemies Act” (“RANSOMWARE Act”). H.R. 4551 was introduced by Consumer Protection and Commerce Ranking Member Gus Bilirakis (R-FL).

If it becomes law, H.R. 4551 would amend Section 14 of the U.S. SAFE WEB Act of 2006 to require not later than one year after its enactment, and every two years thereafter, the Federal Trade Commission (“FTC”) to transmit to the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report (the “FTC Report”).
The FTC Report would be focused on cross-border complaints received that involve ransomware or other cyber-related attacks committed by (i) Russia, China, North Korea, or Iran; or (ii) individuals or companies that are located in or have ties (direct or indirect) to those countries (collectively, the “Specified Entities”).

Among other matters, the FTC Report would include:

- The number and details of cross-border complaints received by the FTC (including which such complaints were acted upon and which such complaints were not acted upon) that involve ransomware or other cyber-related attacks that were committed by the Specified Entities;
- A description of trends in the number of cross-border complaints received by the FTC that relate to incidents that were committed by the Specified Entities;
- Identification and details of foreign agencies, including foreign law enforcement agencies, located in Russia, China, North Korea, or Iran with which the FTC has cooperated and the results of such cooperation, including any foreign agency enforcement action or lack thereof;
- A description of FTC litigation, in relation to cross-border complaints, brought in foreign courts and the results of such litigation;
- Any recommendations for legislation that may advance the security of the United States and United States companies against ransomware and other cyber-related attacks; and
- Any recommendations for United States citizens and United States businesses to implement best practices on mitigating ransomware and other cyber-related attacks

Cybersecurity is an area of recent federal government focus, with other measures recently taken by President Biden, the Securities and Exchange Commission, the Food and Drug Administration, and other stakeholders.

Additionally, H.R. 4551 is also consistent with the FTC’s focus on data privacy and cybersecurity. The FTC has increasingly taken enforcement action against entities that failed to timely notify consumers and other relevant parties after data breaches and warned that it would continue to apply heightened scrutiny to unfair data security practices.

In May 2022, in a blog post titled “Security Beyond Prevention: The Importance of Effective Breach Disclosures,” the FTC’s Division of Privacy and Identity Protection had cautioned that “[t]he FTC has long stressed the importance of good incident response and breach disclosure as part of a reasonable information security program, and that, “[i]n some instances, the FTC Act creates a de facto breach disclosure requirement because the failure to disclose will, for example, increase the likelihood that affected parties will suffer harm.”

As readers of CPW know, state breach notification laws and sector-specific federal breach notification laws may require disclosure of some breaches. However, as of May 2022 it is now expressly the position of the FTC that “Regardless 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." This is a significant development, as notwithstanding the absence of a uniform federal data breach statute, the FTC is anticipated to continue exercise its enforcement discretion under Section 5 concerning unfair and deceptive practices in the cybersecurity context.

© Copyright 2022 Squire Patton Boggs (US) LLP

National Law Review, Volume XII, Number 214