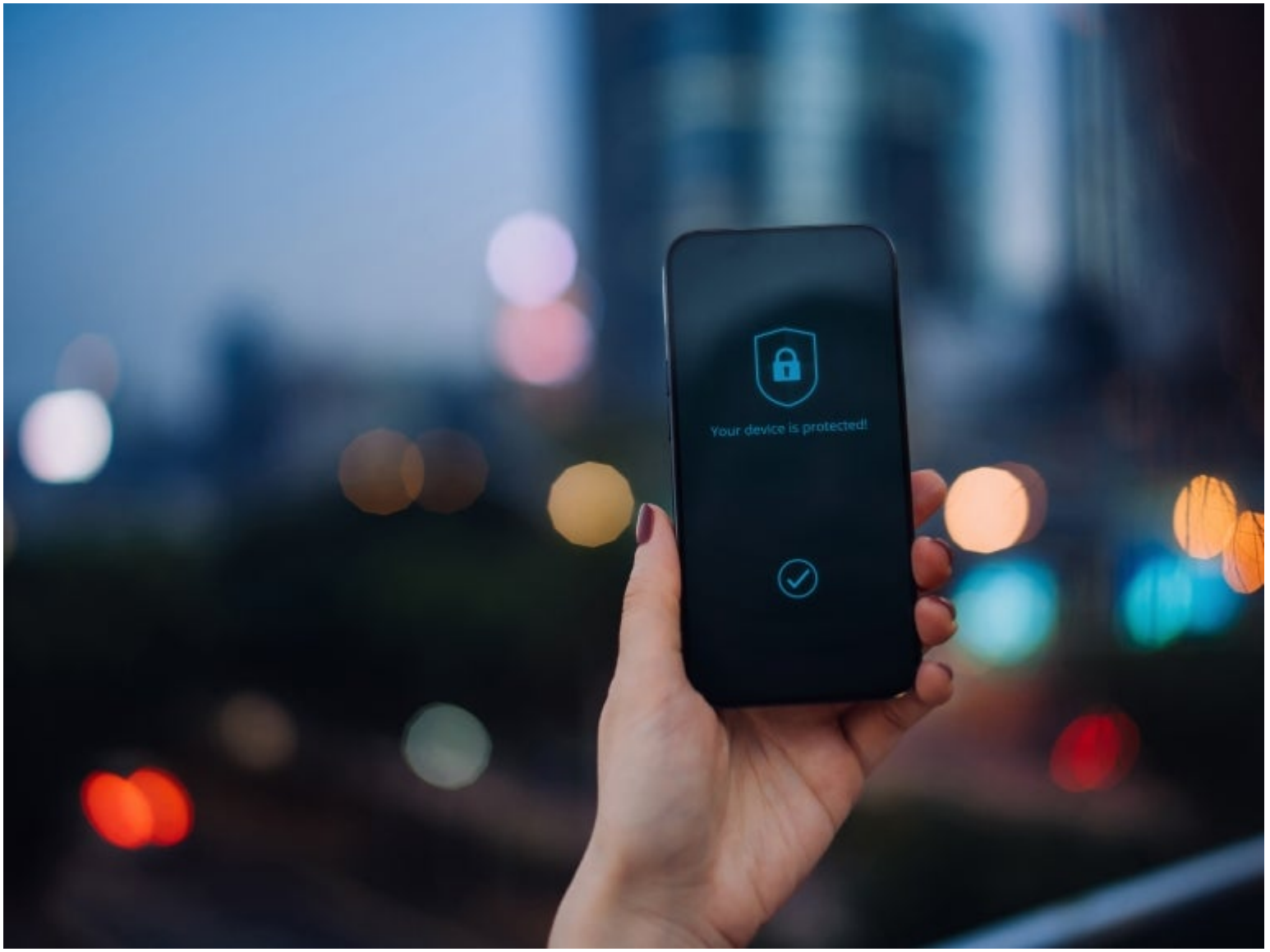

Continued cyberthreats drove expanded data security and breach notification requirements in 2024.

Although sectors deemed high-risk saw significant activity, we also saw proposed regulations that stand to have a significant impact on a wide swath of private companies in the year to come. The highlights include:

- **Enhanced sectoral regulations.** On the federal front, the Federal Trade Commission (FTC), U.S. Securities and Exchange Commission (SEC), and Federal Communications Commission (FCC) all expanded regulations that apply to companies within specialized sectors or with respect to particular types of data in their jurisdiction. The FTC's sweeping breach notification requirements applying to nonbank financial institutions went into effect in May, shortly after the FTC finalized revisions to the Health Breach Notification Rule that applies to companies working with health records that are not otherwise regulated by HIPAA. The SEC revised Regulation S-P in May to include enhanced security and notice

obligations for broker-dealers and investment advisors, and the FCC's updated and expanded breach notice obligations went into effect in March.

- **CIRCIA draft breach notification requirements.** In April, CISA released draft regulations to implement the 2022 Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). The regulations, expected to be finalized late next year, require critical infrastructure entities to report security breaches and ransomware payments. While the requirements under the rule are relatively straightforward, they require organized and rapid reporting that will need to be incorporated into incident response procedures. The proposed scope of the regulations is also intentionally broad, covering entities like retailers and software providers that may not typically consider themselves critical infrastructure.
- **California Privacy Rights Act cybersecurity audit regulations.** These rules, related to the 2020 expansion of California's omnibus privacy law, will require companies engaged in "high risk" processing to conduct an independent audit of their security controls each year. The draft regulations currently define in-scope businesses based on revenue and number of California consumers and require the audits to address a variety of specific controls, identify any gaps and vulnerabilities, and collect all breach notifications filed by the company worldwide. Comments are currently open on the draft regulations until January 14, 2025.
- **Tweaks to state notification laws**. State breach notification laws, which have been in effect in all states for almost a decade, continue to be revised and become more complex every year. This year, most notably, Pennsylvania introduced a novel requirement that companies provide free credit reports to certain individuals affected by a breach.
- **Continued focus on public messaging.** Both the FTC and the SEC brought actions this year related to companies' public statements following incidents and the alleged failure to be fully and properly transparent regarding the impact of an incident. This was also the first full year of the SEC's public company cyber disclosure requirements, and companies' perhaps over-eagerness to satisfy those requirements has caused some pushback from the SEC. Under the new administration, the FTC is expected to continue to focus on privacy and data security, but a Republican-led SEC may pull back on this type of enforcement.

For more information on recent data security law developments, please also see our prior Update regarding recent changes.

Authors

Amelia M. Gerlicher

Partner
AGerlicher@perkinscoie.com 206.359.3445

Explore more in

Privacy & Security | Data Security Counseling and Breach Response | Privacy Regulatory Investigations & Enforcement | Technology Transactions & Privacy Law

Related insights

Blog

2024 Breach Notification Law Update: Unique New State Obligations and Widespread New Federal Obligations

Blog

How the FTC’s Approach to Privacy, Security, and AI Enforcement May Change Under Trump 2.0