The FTC Commeth – Deadline Fast Approaching for its Updated Safeguards Rule

If variety is the spice of life, then we're all in luck as there always seems to be a new set of cyber rules on the horizon. June 9th marks the revised deadline for implementing of the Federal Trade Commission's (FTC's) "new" Standards for Safeguarding Customer Information (the Safeguards Rule or the Rule), that was published in December 2021.

As is often the case with new cybersecurity rules, this one contains the familiar, but also comes with a number of very specific prescriptions that need to be addressed by regulated organizations – some of which were newly swept under the FTC's watchful eye.

What Was That Rule Again?

The FTC issued updates to its Safeguards Rule, found at 16 C.F.R Part 314 in December 2021. The effective date of the Rule was January 10, 2022, but the bulk of its new provisions were deferred to December 9, 2022. In consideration of the impacts of COVID, implementation was further delayed until June 9, 2023.

The FTC's authority finds its provenance in the Gramm-Leach-Bliley Act of 1999 (GLB). GLB's focus is on the privacy and security regulation of financial institutions. As such, GLB is the source of statutory authority for regulation over banking institutions by a patchwork of federal agencies, depending on the size of the financial institution. These regulators aligned their implementation standards through an interagency group known as the Federal Financial Institutions Examination Council (FFIEC), but the FTC has gone it alone in its regulation of a bevy of non-banking organizations that are on the margin of what one might expect to be considered "financial institutions."

What's New?

The Safeguards Rule establishes some very specific requirements. Key items include:

- A comprehensive written information security program (WISP), managed by a "qualified" individual.
- Written risk assessments that meet specific requirements and include mitigation or risk acceptance processes.
- Designation of a "qualified" individual to oversee the organization's program.
- Either (1) an annual penetration test with semi-annual vulnerability assessments or (2) implementation of "continuous monitoring" of the in-scope environment.
- Encryption of customer information in transit over external systems and at rest.

- Use of a vendor management program to oversee service providers with access to regulated information.
- Use of multifactor authentication.
- Reports to governing bodies, like boards of directors.
- Processes for logging/disposing of customer information.
- Controls to detect unauthorized access to, use of, or tampering with regulated information.

Who is Covered?

The applicability of the FTC's Safeguard Rule has had an interesting run over the years. At one point, the FTC attempted to sweep in supermarkets as financial institutions, because cashing a check or getting cash back at checkout, it analogized, was like a service at a bank. Until the new Rule, the battle lines had largely settled around an eclectic group of organizations, including mortgage brokers, motor vehicle dealers, collection agencies, tax preparation firms, payday lenders and check-cashing businesses that operate outside the GLB-driven regulation of what one might think of as a financial institution, like banks examined under the FFIEC standards. Interestingly, most colleges are subject to the Rule, because of their processing of student loans despite the ostensible reach of other cyber rules.

Under its new Rule, the FTC gave itself the authority to expand its reach to "finders," i.e., those that bring together sellers and buyers of a product or service. The full scope of that reach is ostensibly limited to those that handle regulated information and the FTC kindly enumerates 13 old types of business that are subject to the new rule (though providing little help with "finders") and 4 types that aren't subject to the Rule. As an act of regulatory mercy, those presumably small businesses that maintain regulated information for fewer than 5,000 individuals are exempt.

Compliance Strategies

As we have reviewed the new Rule with clients, there are a couple of opportunities to meet the Rule's objectives, which should be considered:

- Fractional Security Officer. Outsourcing the "responsible" individual to a security firm provides an answer to the requisite skills intended by the rule, without needing to hire those skills full-time. Fractional or "VCISO" engagements can be adapted to the needs

and budgets of organizations. Such an individual can craft and perform the requisite elements, including risk assessment, vendor management, WISP management, reporting, etc. While some of that work can be supported by traditional audit firms, they tend not to provide the hands-on components needed by the rule. In addition, this individual should be separated from managed service providers who otherwise perform core operational IT services to maintain a separation of duties.

- Penetration testing and vulnerability scanning are probably preferrable to "continuous monitoring." The former are discrete and well understood use of security tools and processes. The latter is ill-defined in the rule, especially as to the scope and type of monitoring that would be considered sufficient. It's reasonable to assume, based on FTC enforcement practices, that such sufficiency will be defined ad hoc through findings of inadequacy following a breach or cyber incident. Also, organizations should be judicious in their selection of penetration testing services, as many cheaper, commodity "pentests" are largely indistinguishable from vulnerability scans.

There is still time for organizations to rally to the new FTC requirements, though the window is closing! With an activist bent in the current FTC leadership, staying ahead of these new Rules is important for all regulated organizations – new and old.

About Ande Smith

A member of the New Hampshire and Maine bars, Ande Smith is President and founder of Deer Brook, an IT and cybersecurity consultancy. Deer Brook provides a range of cybersecurity services, including penetration testing and security program management, to many sectors of the SMB market. It can be found at www.deer-brook.com and Ande can be reached at asmith@deer-brook.com.

deer-brook.com

DEER BROOK

CYBER | TECHNOLOGY | SOLUTIONS