Armstrong Teasdale

November 29, 2021 • Advisory • www.atllp.com

FTC EXPANDS THE SAFEGUARDS RULE, ANTICIPATES 'TECHNOLOGICAL SHIFTS'

Since 2010, the United States Federal Trade Commission (FTC) has resolved more than 50 cases involving alleged cybersecurity incidents and data privacy violations. In 12 of these cases, the FTC targeted directors and officers, in addition to their organizations. In short, the FTC has been an active enforcer of consumer rights per Section 5 of the FTC Act, which prohibits unfair and deceptive practices.

But 2019 was a year like no other for the FTC. In the span of two days, July 22 through 24, the FTC announced a $700 million settlement with Equifax for a data breach and a $5 billion civil penalty against Facebook for violating consumers' privacy. In comparison, the subsequent two years were relatively quiet, other than a settlement with an analytics company for failing to ensure one of its vendors was adequately securing personal information.

Now, within the last two months, the FTC has again reaffirmed its status as a key cybersecurity enforcer.

THE 'UPDATE' ERA BEGINS

On Oct. 1, 2021, the FTC's new Chair Lina Khan declared: "Policing data privacy and security is now a mainstay of the FTC's work" and "we must update our approach to keep pace with new learning and technological shifts."

On Oct. 27, 2021, the FTC updated the Safeguards Rule, something it hadn't done since 2002. The Rule requires financial institutions to implement measures that keep customer information secure. In addition to developing their own safeguards, companies covered by the Rule are responsible for taking steps to ensure that their affiliates and service providers also safeguard customer information in their care.

Notably, the definition of "financial institution" includes many businesses that may not normally describe themselves that way. In fact, the Rule applies to all businesses, regardless of size, that are "significantly engaged" in providing financial products or services. This includes, for example, check-cashing businesses, payday lenders, mortgage brokers, nonbank lenders, personal property or real estate appraisers, professional tax preparers, courier services

PEOPLE

Jeffrey Schultz, CIPP/US

Casey E. Waughn, CIPP/US

SERVICES AND INDUSTRIES

Data Innovation, Security and Privacy

Financial Services and Banking

and even ATM providers who receive customer information.

WHAT THE RULE MODIFIES

Generally speaking, the Rule contains the following five modifications to the previous Safeguards Rule:

1. More detailed guidance on how to develop and implement Written Information Security Programs (WISPs).
2. Added provisions designed to improve the accountability of WISPs.
3. Exemption of some financial institutions that collect less customer information.
4. Expansion of the definition of financial institutions to include "finders" – companies that bring together buyers and sellers of a product or service covered by the Rule.
5. Provision of defined terms and related examples.

KEY TAKEAWAYS FOR 'FINANCIAL INSTITUTIONS'

The Rule further supports the common threads that have emerged from the patchwork of legal, regulatory and industry standards, namely WISPs, risk assessments (RAs) and incident response plans (IRPs).

Have a WISP

The Rule requires implementation of a WISP, just as the FTC required of Equifax in 2019, but this time the Rule refers to the implementation of certain technical requirements as well, including:

1. encryption to protect customer information in transit and at rest;
2. continuous monitoring or periodic penetration testing and vulnerability assessments;
3. multi-factor authentication for anyone accessing an information system; and
4. retention of service providers that are capable of maintaining appropriate safeguards for customer information.

Perform an RA

The Rule requires that WISPs be based on RAs and sets forth three general areas that the RA must address:

1. criteria for evaluating risks faced by the financial institution;
2. criteria for assessing the security of its information systems; and
3. how the identified risks will be addressed.

Other than these requirements, financial institutions are free to perform their

RAs in whatever way they choose, as long as the method identifies reasonably foreseeable risks. Importantly, the Rule does not contemplate financial institutions scrapping their WISPs and starting over via a new RA, but rather, comparing their existing WISPs and addressing any gaps.

Update the IRP

The Rule requires that IRPs be thorough. Specifically, they must be designed to promptly respond to and recover from any security event materially affecting the confidentiality, integrity or availability of customer information in their control.

The Rule also requires IRPs to address:

1. the goals of the IRP;
2. the internal processes for responding to a security event;
3. the definition of clear roles, responsibilities and levels of decision-making authority;
4. external and internal communications and information sharing;
5. identification of requirements for the remediation of any identified weaknesses in information systems and associate controls;
6. documentation and reporting regarding security events and related incident response activities; and
7. the evaluation and revision as necessary of the IRP following a security incident.

Employee Training and Reporting to Boards

The Rule also expands on two other fundamental aspects of a WISP, employee training and reporting to boards.

The Rule requires financial institutions to provide their personnel with "security awareness training that is updated to reflect the risks identified by the risk assessment."

The Rule requires that financial institutions have a qualified person report in writing, regularly and at least annually, to a board of directors or governing body about a WISP. Specifically, the report shall include the following:

1. the overall status of the WISP and compliance with the Rule; and
2. material matters related to the WISP, such as RAs, risk management and controls decisions, and recommendations for changes in the WISP.

Importantly, the Rule exempts small businesses – those that collect information on fewer than 5,000 consumers – from the above requirements. Nevertheless, the Rule will require numerous financial institutions to assess their WISPs, RAs and IRPs to ensure they comply.

As the FTC examines how to update its approach “to tackle the slew of data privacy and security challenges we presently face,” financial institutions should assess their cybersecurity posture in light of the Rule. For most of the discussed requirements, financial institutions will have one year to develop and implement practices, policies and procedures that comply with the new Rule.