DATASHEET

Radar® Privacy

The FTC Safeguards Rule in Radar® Privacy

Streamlined FTC compliance for non-banking financial institutions

The FTC's Safeguards Rule requires non-banking financial institutions, such as mortgage brokers, motor vehicle dealers, and finance companies, to develop, implement, and maintain a comprehensive security program to keep customers' information safe.

A new data breach disclosure requirement went into effect on May 13, 2024, requiring covered entities to notify the FTC within 30 days of discovery when it involves the personally identifiable information of 500 or more individuals. When notification requirements aren't met, fines and penalties can be extensive—and result in an erosion in trust from consumers and regulators alike.

Speed and Process are Key

Effective May 13, 2024, **a critical update to the FTC's Safeguards Rule includes a new data breach disclosure requirement**. This update poses unique challenges to covered entities as the definition of personally identifiable information is incredibly broad.

Unlike typical state breach notification laws, the FTC Safeguards rule does not clearly delineate specific data elements that qualify as personally identifiable information. Rather, under the Safeguards Rule, **if information can be used to identify an individual, is not public, and impacts 500 or more individuals, notification to the FTC is required, regardless of the risk of harm**.

The FTC's atypical definition of personally identifiable information (PII) makes it particularly critical to have a defined process in place—well before you need to rely on it to assess an event.

Organizations must have a process in place that is easier to do than not do, from decision-making to documentation, as well as notification and post-event debrief and analysis. People will follow a well-defined process, as long as it is intuitive, easy, and well understood.

To ensure you have the right process in place, supported by the right technologies, processes should be practiced before an event occurs.

You do not want your team to be running a process or protocol for the first time while in crisis mode. **A privacy team's worst enemies are pressure and time**. Alleviate both via tried and tested, technology-supported processes.

Entities Covered Under the Safeguards Rule

The FTC's Safeguards Rule covers non-banking financial institutions, including but not limited to the following:

- **Mortgage lenders and brokers**
- **Account servicers**
- **Finance companies**
- **Check cashers**
- **Collection agencies**
- **Credit counselors and financial advisors**

GLBA vs. the Safeguard Rule

Is it possible for a single organization to be subject to both the GLBA and the FTC's Safeguard Rule? **Yes**, although it depends on how the company is structured.

If an organization has multiple lines of business, each may be subject to different regulations, including the Safeguard Rule and the GLBA, as well as any applicable state or global laws and regulations.

The FTC Safeguards Rule:

- Covers non-banking financial institutions
- Requires notification to the FTC for events involving the PII of 500 or more individuals
- Defines PII broadly
- Provides 30 days to notify the FTC
- Does not require individuals be notified
- Does not provide for a harm test as a condition of notification

FTC Notification Obligation Intelligence with Radar® Privacy

We live and work in a dynamic regulatory environment. Despite the ever-evolving legal landscape, there is little room for error—unless you have a defined process in place for identifying, documenting, and notifying regulators of data breaches.

The FTC understands that breaches are often a when—not if—event. **Their expectation is that your organization is deeply prepared with consistent processes for documenting, assessing, and notifying when an event occurs**. The first time you trial a playbook should never be in the midst of a live remediation effort.

Put your processes—and technologies—through their paces before you need them, and you will be well on your way to quelling any potential fines and penalties from the FTC in the event of a data breach.

Automation to Simplify FTC Compliance

Radar® Privacy operationalizes and simplifies compliance with the FTC's Safeguards Rule by applying assessment automation and intelligent notification guidance to eliminate the subjectivity and inconsistency inherent in deciding whether privacy incidents and breaches are reportable under the FTC's Safeguards Rule.

The FTC's Safeguards Rule is unique in that it offers a very broad definition of personally identifiable information, while not explicitly delineating the data elements considered personal information. In addition, the rule does not include a harm standard as a trigger for notification.

The FTC module in Radar® Privacy is uniquely configured to address these specific assessment needs. The intelligent decision automation provided by the module ensures consistent and timely incident assessments to decrease time to resolution and ensure your organization can meet even the strictest FTC notification timelines.

Avoid costly penalties and fines—and an erosion of trust—with the FTC module in Radar® Privacy.

Ready to learn more?
Schedule a demo of Radar® Privacy.

INFO@RADARFIRST.COM | 1.844.737.3778

Schedule a Demo >

RadarFirst

Learn more at radarfirst.com

RadarFirst supports governance, risk, and compliance (GRC) with incident management solutions that automate intelligent decisions and streamline compliance with cybersecurity, privacy, and compliance laws. Our patented assessment technology enables organizations to act quickly to comply with evolving obligation requirements and notification deadlines. Build trust and reduce enterprise risk with RadarFirst.