INSIDE CYBERSECURITY
News. Analysis. Community.

DAILY NEWS

Data privacy group EPIC offers support for FTC incident reporting rule, amid industry concerns

By **Charlie Mitchell** / February 9, 2022

Tweet LinkedIn

The Electronic Privacy Information Center, an advocate for consumer privacy and digital rights, is praising the Federal Trade Commission's proposed cyber incident reporting requirement for financial entities and said it will incentivize better security practices and promote transparency around "security events."

Among a handful of proposed changes, EPIC called for adding a consumer notification requirement to the rule.

A **comment period closed** Monday on an FTC proposal to amend the Safeguards Rule by requiring financial entities subject to the Gramm-Leach-Bliley Act to report "security events" affecting 1,000 or more customers. The proposal was **issued in December 2021**.

About a dozen trade associations filed **comments** with several saying the requirements were duplicative and unnecessary.

But the public interest group EPIC offered strong support with several recommended tweaks that it said would strengthen the proposal.

"EPIC urges the Commission to adopt the [proposal] requiring security event reporting to the Commission. This safeguard will further incentivize the use of strong data security measures by financial institutions, bring additional accountability and transparency to the handling of security events, and enhance the data security and privacy of all consumers," according to the **EPIC filing**.

The group said, "In response to the questions posed by the Commission in its supplemental notice of proposed rulemaking, EPIC offers the following additional recommendations:"

1. *the Commission should require that the four proposed elements be included in all security event notices but should also demand a more comprehensive account of the security event;*
2. *the Commission should require notification for any security event implicating the personal information of 1,000 or more customers and should not provide a carve out for encrypted data;*
3. *the Commission should look to state notification deadlines to inform the timing of security event reports;*

4. *the Commission should not allow an institution to withhold notice of a security event from the Commission but could delay public dissemination of that notice where there is a compelling law enforcement basis to do so;*
5. *the Commission should publish notification information by default, only delaying publication where there is a compelling law enforcement basis to do so or where the vulnerability causing the incident remains exploitable;*
6. *a stand-alone reporting requirement is appropriate because it will pose only a de minimis burden on most covered institutions;*
7. *the Commission should impose a requirement on covered entities to notify the Commission of security events; and*
8. *the Commission should impose a requirement on covered entities to notify affected consumers of security events implicating their personal information.*

Major industry groups expressed support for the goals of the FTC proposal coupled with varying degrees of concern over imposing new regulatory burdens and duplicating existing requirements.

CTIA-The Wireless Association said, "While the wireless sector agrees safeguarding customer information is critical, the current proposal in the Supplemental NPRM will not further that goal, and it will only add unnecessary cost and complexity to an already fragmented reporting and notification landscape. Accordingly, CTIA respectfully requests that the FTC not establish a reporting requirement or standard for financial institutions under the Safeguards Rule."

The Clearing House Association, which addresses payments issues, "commended the FTC for its work improving and strengthening the Safeguards Rule, and for proposing to provide data security event reporting requirements for FTC-regulated institutions. These institutions, including many financial technology companies, often engage in activities that are similar to the activities undertaken by banks subject to oversight by the federal prudential regulators."

But the group noted, "The Clearing House remains concerned about differences that exist between the standards to which traditional financial institutions regulated by the prudential regulators are subject and those that the FTC has proposed in the supplemental notice of proposed rulemaking."

The Consumer Data Industry Association, representing Equifax and other consumer credit rating agencies, said the proposal is unnecessary given state breach notification requirements. Equifax was the target of a major hack in 2017 and faced extensive criticism for the slow pace of its efforts to notify authorities and consumers of the data breach.

Former FTC Chairman Joseph Simons, a Republican, in 2019 **said the Equifax case** underscored the need for new civil-fines authority at the commission, among other powers.

The U.S. Chamber of Commerce **in its comments** said, "The FTC should forgo moving forward on the security event rulemaking unless it can articulate a reasonable plan to harmonize the myriad regulations that affect industry at the state, federal, and international levels vis-à-vis the Safeguards Rule, among many other requirements."

The Bank Policy Institute and Securities Industry and Financial Markets Association in **joint comments filed to the FTC**. said the proposal should make clear that new "reporting obligations should apply only to situations where such notice is not redundant to existing notification requirements and only to those institutions for which the [FTC] is the principal financial regulator."

BPI and SIFMA said, "Adding the [FTC] to the long list of regulators already receiving notice of security incidents from Financially Regulated Institutions would not create any supplemental benefits for the consumer or entities that are already prudentially regulated. More significantly, adding the Commission could unnecessarily interfere with the discretion of the primary federal regulator and result in consumer confusion." -- *Charlie Mitchell (cmitchell@iwpnews.com)*

13181

RELATED NEWS

- **U.S. Chamber urges FTC to hold off on incident reporting rule; financial groups say avoid duplication**

© 2022. Inside Washington Publishers