

US cybersecurity and ransomware reporting mandates will benefit banks

Article

The news: The US House of Representatives is [considering](#) legislation to [force banks](#) and other companies handling critical infrastructure to report cybersecurity incidents and

ransomware payments. The US Senate passed the bipartisan measure last week.

What will banks need to do? If passed, the legislation would require banks to report:

- **Certain cybersecurity incidents** to the Cybersecurity and Infrastructure Security Agency (CISA) **within 72 hours** after the bank discovers them.
- **Ransomware payments within 24 hours** after they are paid.

The bill calls for a rulemaking process to determine which companies must comply and which types of cybersecurity incidents would be covered.

CISA's director would be allowed to issue subpoenas to compel non-compliant companies to cooperate. The director could get the US attorney general involved for civil action if banks failed to comply with the subpoenas.

How we got here: The mandates are part of the Strengthening American Cybersecurity Act, spearheaded in the Senate by Sens. Gary Peters (D-Michigan) and Rob Portman (R-Ohio), the chairman and ranking member of the body's Homeland Security and Governmental Affairs Committee, respectively.

The legislation was introduced last month amid concerns that the Russian government could conduct cyberattacks retaliating for the US supporting Ukraine.

The bigger picture: The measure follows a rule that three banking regulators adopted in November 2021, which forces banks to **report significant cybersecurity incidents to their primary regulator within 36 hours** after determining that they happened.

- The rule takes effect on April 1, 2022, but banks must comply with it by May 1, 2022.

While the two requirements appear to overlap, **they serve different purposes**, the Bank Policy Institute's Heather Hogsett told American Banker.

- The 36-hour mandate, Hogsett said, is designed to "allow bank regulators to keep a pulse on **what is happening in the country's financial services industry.**"
- The proposed bill, Hogsett added, is meant to help CISA "**produce reports about threat actors and provide early warning of potential attack vectors.**"

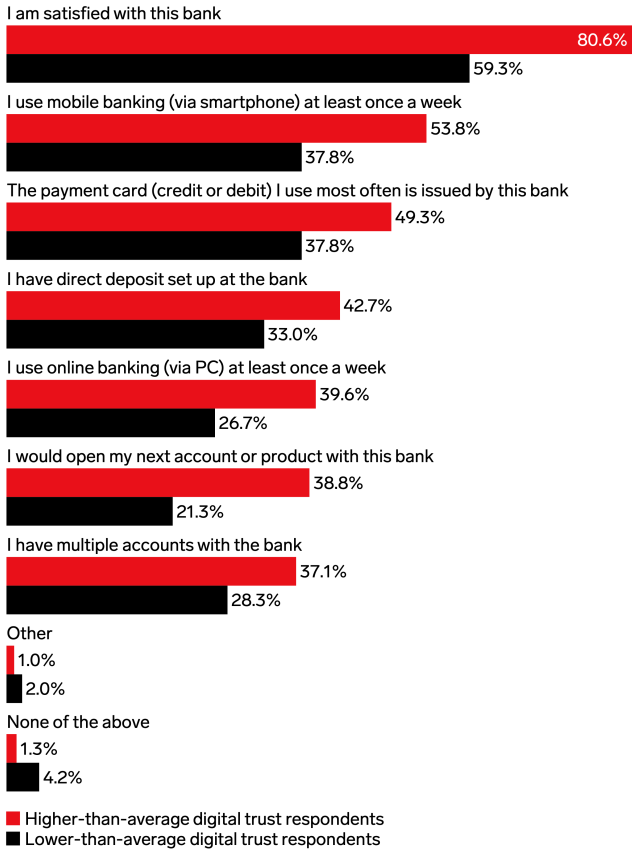
The big takeaway: The pending legislation will help combat rising cybersecurity incidents against banks, which is critical to maintaining digital trust with consumers—a key competitive

advantage in which banks have an edge over nonbanks.

- US Treasury Department data [shows](#) that related Suspicious Activity Reports skyrocketed in recent years, from **1,221** in 2018 to **20,086** in 2020.
- In some recent incidents, banks [took a while](#) to disclose their breaches to customers: **First Horizon** took about two weeks in April 2021 and **Capital One** took 10 days in July 2019.
- Banks that don't readily report cybersecurity incidents risk undermining consumers' trust, per our 2021 [Banking Digital Trust Report](#). It shows that **cybersecurity was the highest-ranked out of six factors surveyed**, and 78.7% of respondents deemed it "extremely important."
- Respondents with above-average digital trust were more likely to open another account or product with their bank (38.8%) than those with below-average trust (21.3%). The above-average cohort was also more likely to maintain multiple accounts with their bank (37.1%) compared to the below-average group (28.3%).

How High-Trust and Low-Trust US Digital Banking Users Perceive and Interact with Their Bank

Q: Which of the following statements apply to you when it comes to your bank? Select all that apply.



Source: Insider Intelligence Banking Digital Trust Survey, Q1 2021
 Methodology: Respondents to the online survey (n=2,412) are digital banking users at the top 10 US banks. Respondents were sourced from a third-party sample provider to resemble US demographics on the criteria of gender, age, and income.

1039342462281

PRIMARY RESEARCH FROM
INSIDER
 INTELLIGENCE