NOV 22
Tom Auchterlonie

# US banks' cybersecurity reporting mandate could empower consumers and increase their digital trust

Article

**The news:** Banks in the US face new reporting requirements of major cybersecurity incidents to regulators and consumers, per a new rule adopted by three regulators.

**More on this:** The rule obligates banks to inform their primary federal regulator about significant incidents **within 36 hours of their determination** that they took place.

- Covered incidents are those that materially impact—or are likely to impact—banks' operations, the financial sector's stability, or banks' service-delivery capabilities.
- The consumer-reporting component mandates disclosure **"as soon as possible"** for any incident that materially affects consumers, or is likely to make an impact, **for at least four hours**.
- Cyber incidents that the regulators are concerned about include **using malware**, **mistakes made by banking personnel**, and **"non-malicious"** software or hardware failures.

The regulation was green-lit by the Office of the Comptroller of the Currency (OCC), the Federal Reserve, and the FDIC. **It takes effect on April 1, 2022**, and **banks must comply by May 1, 2022**.

**The rationale:** Banks and their customers are increasingly on the receiving end of cyber attacks. The rule's overview cites US Treasury Department data showing that the number of related Suspicious Activity Reports has ballooned, going from **1,221** in 2018 to **20,086** in 2020.

Regulators outlined how they want the rule to improve their responses to cyber attacks through:

- Faster awareness and better threat assessments.
- Being able to offer banks guidance sooner.
- Moving quicker to approve banks' requests for help from the Treasury Department's Office of Cybersecurity and Critical Infrastructure Protection.

**The big takeaway:** The requirements mandate transparency, which could improve consumers' trust in their banks and empower them to take steps sooner to reduce personal data risks.

The changes will also result in quicker action from officials to squelch any spread in the severity of cyber attacks.In some recent incidents, customers have been kept in the dark for for a week or more:

- **First Horizon took about two weeks** in April 2021 before it disclosed a breach involving access to accounts and the theft of customers' funds.

- **Capital One waited 10 days** in July 2019 before revealing a data breach for the personal information of credit-card applicants.
- **Flagstar Bank** learned in January 2021 that a vendor, Accellion, had a vulnerability on its platform. However, the bank **didn't notify customers until March 2021.**

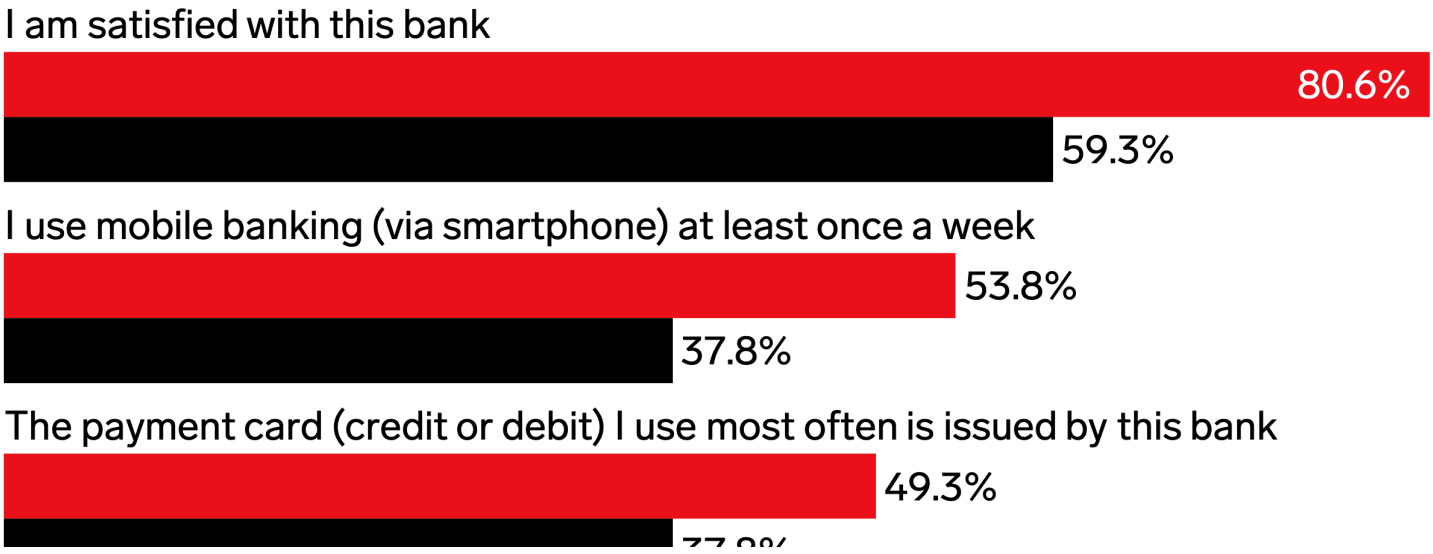
Banks with lagging cybersecurity disclosures risk undermining the trust of their customers, which is bad for business. For example, our 2021 Banking Digital Trust Report shows that security was **the highest-rated of six factors** for respondents' determinations of trust, with **78.7%** marking it as "extremely important."

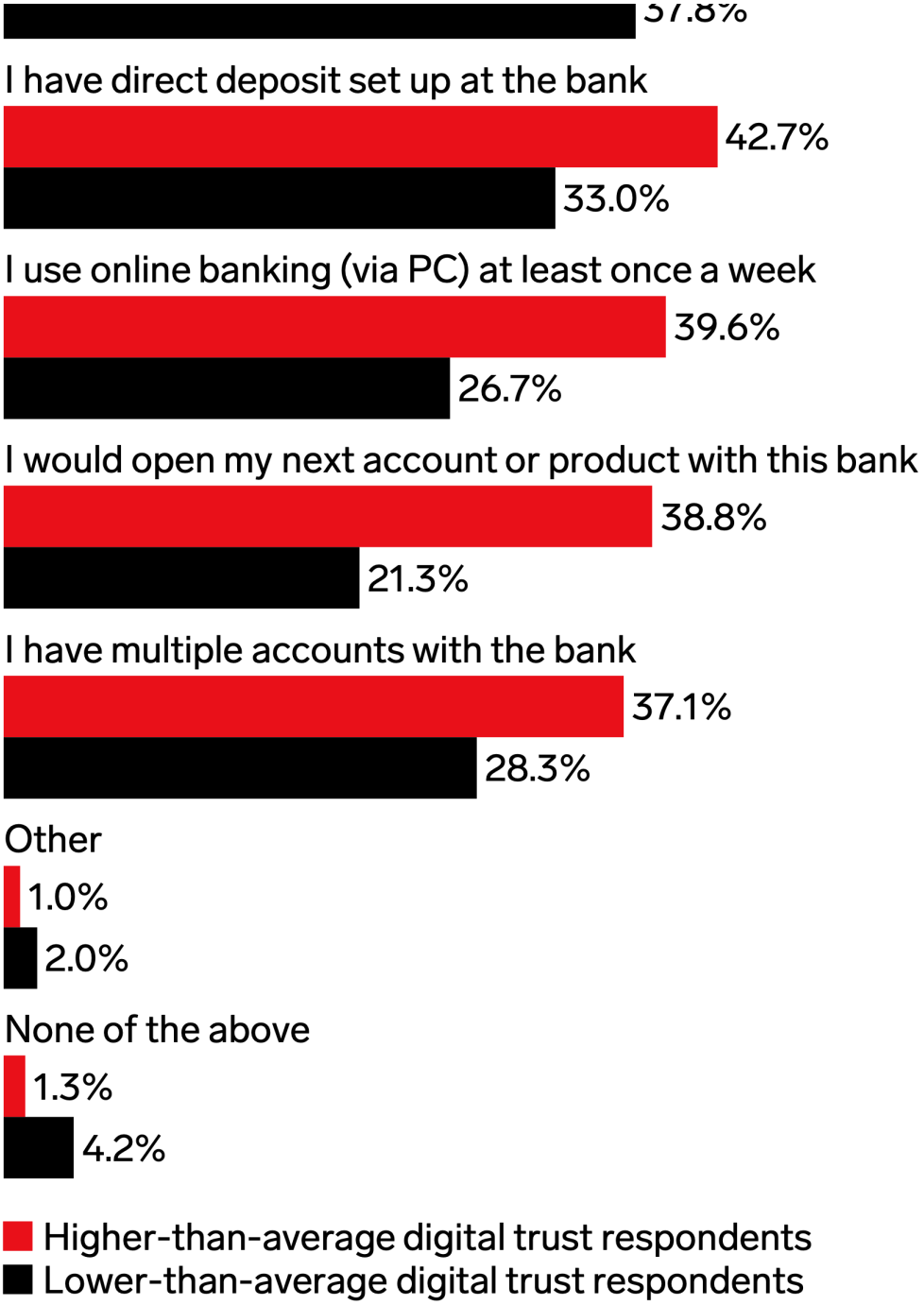
Respondents with above-average digital trust were also likelier to patronize their banks than those with below-average trust:

- They are more likely to open their next accounts or products with their current bank, with **38.8%** to just **21.3%** for the below-average group.
- Above-average trust respondents were also more likely to have multiple accounts with their bank, at **37.1%** to **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