August 28, 2024

The Honorable Richard Blumenthal
United States Senate
Washington, D.C. 20510

The Honorable Elizabeth Warren
United States Senate
Washington, D.C. 20510

The Honorable Maxine Waters
United States House of Representatives
Washington, D.C. 20515

Re: S. 4943/H.R. 9303, the Protecting Consumers from Payment Scams Act

Dear Sen. Blumenthal, Sen. Warren, and Ranking Member Waters,

As trade associations representing the American banking industry, we write to express our opposition to S. 4943/ H.R. 9303. If enacted, this bill would not address the growing phenomenon of financial fraud—to the contrary, it would encourage and increase scams and create more victims while simultaneously harming financial inclusion by reducing consumers' access to basic deposit accounts.

The Electronic Funds Transfer Act (EFTA) and its implementing regulation, Regulation E, govern consumer electronic payments and transfers of money. While EFTA limits a consumer's liability for unauthorized transactions, it does not limit a consumer's liability for authorized transactions that the consumer voluntarily initiates, including when those transfers turn out to have been made to a criminal or bad actor.[1] S. 4943/H.R. 9303 would limit the consumer's liability in such instances and shift it to the financial institutions involved in the transaction.

This approach is only remedial and would do nothing to stop the criminals that are committing these scams. It would instead encourage them to continue and even increase the frequency of their attempts. The legislation would put many financial institutions—especially small, community financial institutions with less ability to shoulder higher fraud losses—in the untenable position of having to restrict consumers' access to deposit accounts, which would harm consumers and reduce community banks' competitiveness. To offset expensive scam losses, financial institutions may have to be more selective about who qualifies for an account and charge more for basic banking services. This could have a negative effect on financial inclusion, at a time when we have been making significant progress in reducing the number of unbanked in this country.[2]

Banks work tirelessly to identify and report suspicious activity to law enforcement, to help educate and warn their customers about common scams, to detect and prevent fraudulently induced

[1] *See* 15 U.S.C. § 1693g. Unauthorized transactions include electronic payments arising from a hacked banking portal or made using a stolen debit card. This is consistent with the general principle regarding fraud liability, as banks are best able to secure online accounts and to track and identify suspicious usage of a debit card. With scams, unlike fraud, it is the customer who makes the decision to initiate the payment or transfer the funds.
[2] FDIC, 2021 National Survey of Unbanked and Underbanked Households, https://www.fdic.gov/system/files/2024-07/2021execsum.pdf.

payments, and to root out accounts that have been used by criminals. However, the activities of these criminals touch more than just the banking industry, and the efforts to thwart scams must similarly be cross-industry and include government support. Each step in the scam ecosystem—from how a scammer identifies consumer targets, to how a scammer gains a customer's confidence, to how the money is processed—offers an opportunity to stop the flow of funds to the criminal. Banks, however, cannot win this fight on their own—it requires all players in this ecosystem to share responsibility to help protect the consumer.

The criminals committing these scams are extremely sophisticated and well-resourced with technology that allows them to impersonate legitimate entities. Banks constantly tell their customers to only send money to people they "know and trust," but by the time a customer is ready to make a payment to a scammer, they often believe they know and trust the scammer because, for example, their caller ID told them it was their bank, the social media account they follow from a famous investor said it was a can't-miss crypto opportunity, or their new romantic partner from overseas who they've talked with for months desperately needs money for a medical procedure. Every bank has a story of a teller pleading with a customer not to send funds and being ignored. In the end, it is the customer's money, and most Americans don't want their bank telling them what they can and can't do with their money.

We need a comprehensive National Scam and Fraud Prevention strategy to develop and implement a coordinated federal approach focused on stopping scams and assisting consumers affected by scams. The strategy should include developing or strengthening capabilities that reduce the ability of criminals to be "technologically authenticated" using impersonated social media accounts or spoofed/fake caller ID and text messages. Messages that impersonate a legitimate company allow criminals to show the name of a trusted company, such as a bank, and hide the fact that the consumer is talking to a criminal—not the bank that their phone display shows. These efforts need to be coordinated amongst multiple regulators and connected to law enforcement so that when these schemes are discovered, law enforcement is promptly made aware and appropriate action is taken.

Additionally, coordination among all the agencies that are fighting financial crime and gathering information is essential. Consumers are asked to report fraud to the FBI, to the FTC, to the CFPB, to their local police, etc., which can create confusion among consumers and can result in siloed data. We recommend a single streamlined and centralized government reporting process for consumers to reduce consumer confusion about where to report scams and to help law enforcement efforts by creating a comprehensive, centralized repository of information about fraud schemes and losses.

Banks cannot win this fight and protect consumers on their own. Every player in the scam ecosystem has a role to play, from the telecoms that allow spoofed caller IDs and text messages that criminals use to gain the trust of consumers, to the social media companies that host impersonated accounts for the same purpose, to the banks who provide robust security and fraud detection capabilities, to law enforcement that needs the resources and training to pursue these criminals. All sectors must see their role in protecting their critical infrastructure from being used by criminals.

Rather than further enabling these scams through legislation like S. 4943/H.R. 9303, we urge Congress to focus on stopping these scams by partnering with regulators, law enforcement, the banking industry, and other private sector stakeholders to develop a comprehensive approach to targeting these criminals. We must continue to identify ways to prevent bad actors from scamming customers out of their money, educate and empower consumers, and ensure criminals and bad actors do not profit from their harmful schemes.

Sincerely,
American Bankers Association
Bank Policy Institute
Consumer Bankers Association
Independent Community Bankers of America