Michelle W Bowman: A coordinated approach to consumer fraud protection

Speech by Ms Michelle W Bowman, Vice Chair for Supervision of the Board of Governors of the Federal Reserve System, at the 2026 Women in Housing and Finance Symposium, Washington DC, 5 May 2026.

* * *

Good morning. It is a pleasure to join you for the annual Women in Housing and Finance Symposium.[1] As a woman in finance, I appreciate this organization's focus on women in the industry. Thank you for the invitation to join you.

Today I would like to discuss an issue that is critical to ensuring the financial security of all Americans, but especially those who are most financially vulnerable-consumer fraud.

Obviously, this is not a new topic, in fact, it has been around as long as money itself. Since people have transacted things of value, there have been those who seek to exploit trust for profit. From ancient Greece to the Ponzi schemes of the 1920s to the telemarketing scams of the 1990s, fraud has always evolved alongside commerce.[2] But in today's environment of rapid technological advances, what we are seeing today is different in scale, sophistication, and impact.

Many of us have heard about, or even experienced, these scenarios firsthand. When you last visited your financial institution, did you see signs at the teller window prohibiting the use of a phone during a transaction? A state commissioner recently shared a common example of how customers get defrauded right in front of their bank teller. The customer stands at the bank counter, phone pressed to their ear, as a scammer on the other end walks them through each step of a fraudulent transaction at the teller window. Despite concerns the bank employee raises, the customer proceeds with the transaction, trusting the voice on the phone, and absolutely convinced they are doing the right thing.

These types of scams have become common, everyday occurrences across the financial sector. Among the most common scenarios is the impersonation of a family member over a social media platform or by phone, urgently requesting funds by a person-to-person funds transfer application. Or a social media advertising campaign convincing a consumer to share bank account credentials and other personally identifiable information that is subsequently used to steal funds. Text messages that include an active link, claiming the United States Postal Service needs an immediate response about a package delivery, which leads to a click and the target downloading malware that is used to compromise a bank account. In some cases, a fraudulent alert from an impersonated Amazon representative states that there is a problem with the customer's account, perhaps an unauthorized purchase that's caused them to freeze the account. The target is asked to "verify" login credentials or credit card details to "fix" the issue.

The consistent theme is that the messages seem authentic. The links appear legitimate and often mimic the retailer's actual website. But that personal information is later used for unauthorized purchases. These sophisticated fraud attempts are occurring at an increasing velocity on a scale that targets significant numbers of consumers.

It may not seem obvious why, as a member of the Board and as the vice chair for supervision, I am raising consumer fraud as a priority issue for the Federal Reserve. The reason is that in addition to the individual harm to consumers, ultimately fraud threatens the integrity and reliability of our financial system. One of the Federal Reserve's most important roles is to regulate banks and payments, and fraud poses a significant risk for both. At its foundation, nearly every fraud affects a bank account or is tied to a payment that involves a bank account.

Banks of all sizes are working to identify, mitigate, and address circumstances that result from or lead to fraud. In fact, fraud losses are one of the largest expenses for community banks.[3] Smaller regional banks also experience significant financial impact from fraud-one bank estimated its annual fraud costs at $40 million. The financial impact of fraud is increasing industrywide, with losses in the hundreds of millions of dollars annually for the largest institutions.

This issue extends far beyond banks. Consumer fraud and scams pose increasing risks to the financial system as noted in the Financial Stability Oversight Council (FSOC) 2025 annual report, which highlighted concerns about fraud, including cyber-enabled fraud. Fraud was also a topic discussed during the FSOC's March meeting in the context of the impact of fraud on household balance sheets.

Starting with the Data

Our own data, as shown in the 2025 Survey of Household Economics and Decision making-the SHED-indicated that one in five American adults experienced financial fraud or scams in 2024.[4] To put that into context, that's 21 percent of the adult population.

While credit card fraud was the most common type of financial fraud, the impact to the consumer is less direct as individuals are not typically required to bear these financial losses. Other types of financial products, including bank accounts, investment accounts, or other financial products were involved in fraudulent activity for 8 percent of households. With these products, in many cases there is no automatic protection and no guarantee of recovery.

The total loss from non-credit card fraud across the financial system was $84 billion in 2024. Of this amount, only $21 billion was recovered, resulting in an estimated net loss of $63 billion in losses for individual consumers.

What does this mean in practice for individual households? According to the SHED survey, on average, the median loss for victims was $500, before any recovery. Even when victims were successfully able to recover funds, about half of those victims still lost money. In the broader context of Americans' financial capacity, 13 percent of Americans cannot cover a $400 emergency expense using cash or its equivalent.

Let that sink in-thirteen percent of Americans don't have $400 in cash on hand for an emergency. The median fraud loss before recovery is $500. Therefore, it should not be surprising that 30 percent of Americans who lost money in an online scam said that it negatively impacted their financial condition.[5] For financially vulnerable households, a fraud loss can quickly escalate from an inconvenience to a crisis affecting their ability to cover essential expenses.

Given these devastating impacts on individual households, you might expect certain groups to be more vulnerable than others. But here's what the data actually shows. Adults aged 45 and older were more likely to experience fraud, largely due to higher credit card usage among these consumers. And elderly consumers are more likely to lose large amounts of money to fraud.[6] But when we examined income levels, race, ethnicity, and gender, we found that the incidence of fraud was similar across all groups.[7] This threat cuts across all demographic lines. No particular individual is insulated from these threats.

Our banking system runs on trust-the belief that accounts are secure and customers can transfer money safely and reliably. When one in five adults experiences fraud and $63 billion disappears from household accounts, that trust erodes. But here's the challenge: The payment tools banks provide that allow customers to manage their financial lives-checks, debit cards, credit cards, and electronic payments-are instrumental for criminals trying to perpetrate fraud. More than half of non-credit card fraud involved a bank account product. Bank transfers and payments were the mechanism for almost 40 percent of aggregate reported losses from fraud in 2024. Criminals are exploiting vulnerabilities in payment systems, authentication processes, and the security measures designed to protect households.

In response, banks are making unprecedented investments in security and consumer education. Yet instances of fraud continue to increase as fraudsters exploit new vulnerabilities and new technologies, while the industry works to create more effective mechanisms to identify, prevent, and remediate fraud. For example, many fraud operations are conducted in overseas scam centers beyond U.S. law enforcement reach, which complicates the ability to combat these schemes.

The Path Forward

Effectively addressing payments fraud is a complex and wide-ranging challenge that extends well beyond the Federal Reserve Board, and beyond the broader responsibilities of the Federal Reserve System. To be effective, this effort requires a comprehensive, multifaceted response and no single agency or private-sector entity can address this threat alone. Effective solutions demand coordinated action.

With that said, the Federal Reserve is committed to a comprehensive strategy that leverages our unique authorities to prevent payments fraud and protect consumers, businesses, and supervised institutions. The Board has carefully reviewed over 250 comments received in response to a Request for Information we jointly issued with the FDIC and OCC last June. These insights are now informing our approach to this issue and our work together.

In our capacity as bank supervisors, we are evaluating a range of responses, including enhanced guidance and resources for banks, as well as broader stakeholder engagement to advance innovative fraud solutions. As a payment system operator, the

Federal Reserve continues to enhance the fraud detection, prevention, and mitigation tools and services we provide to banks across our payment platforms. For example, our operations team continues engagement with the industry on fraud and scam classifier models that are integrated into our payment platforms. Right now, the same scam gets labeled differently-one may call it "online shopping fraud" another "imposter scam." A shared vocabulary around fraud types, scams, and prevention tools facilitates a better understanding of their prevalence and impact.

Promoting and standardizing a common language can also aid in better sharing of consistent data and identifying fraud schemes that are being repeated across payment methods and institutions, allowing for the development of more-informed, holistic strategies.

Success in combating payments fraud also requires strong partnerships. We are committed to working closely with state and federal partners, including law enforcement, to address this evolving threat together.

That's why Secretary Bessent, FCC Chair Brendan Carr, and I will soon build on our ongoing collaboration through a public-private roundtable. This isn't our first conversation-it is the next step in sustained engagement focused on actionable solutions. We'll be asking participants to share what they are currently doing to combat payments fraud, what informal data-sharing practices have proven effective, what prevention mechanisms they have seen that work, and what additional cross-sector or government efforts would be most helpful in this fight.

We must also strengthen bank defenses and improve victim recovery. We must examine whether our regulations address modern fraud and are positioned for the threats consumers will face in the future. And we must ensure the financial system serves everyone safely and securely. The criminals are sophisticated, organized, and relentless. Our approach must be equally robust.

I look forward to the next steps in our work-coordinating with banks, fellow regulators, law enforcement, consumer advocates, and policymakers to confront this crisis and to preserve and enhance the public's trust in the financial system.

Thank you for the invitation to join you today.

---

[1] The views expressed here are my own and are not necessarily those of my colleagues on the Federal Reserve Board or the Federal Open Market Committee.

[2] For tales of fraud in the ancient world, see https://www.trulioo.com/blog/fraud-prevention/history-fraud.

[3] See Federal Reserve Financial Services, "Key Findings From the Annual Federal Reserve Financial Services (FRFS) Financial Institution Risk Officer Survey," (PDF) Survey (Federal Reserve Financial Services, 2024).

[4] See Board of Governors of the Federal Reserve System, *Economic Well-Being of U. S. Households in 2024* (PDF).

[5] See Monica Anderson, Jeffrey Gottfried, and Eugenie Park, *Online Scams and Attacks in America Today* (PDF) (Pew Research Center, July 2025).

[6] See "Scams: Relatively Common and Anxiety-Inducing for Americans," Gallup, November 21, 2023, Scams: Relatively Common and Anxiety-Inducing for Americans, https://news.gallup.com/poll/544643/scams-relatively-common-anxiety-inducing-americans.aspx.

[7] See Board of Governors of the Federal Reserve System, *Economic Well-Being of U. S. Households.*