Acting Comptroller of the Currency Michael J. Hsu

Remarks at the Women in Housing and Finance Public Policy Luncheon

"The Fraud Challenge"

December 11, 2024

The increasing prevalence of financial fraud presents a special challenge for us as a society. While fraud does not have the profile of Basel 3 or cyber risk, its everyday impact in people's daily lives warrants attention. Fraud not only harms consumers, but also leads to distrust in others, in institutions, and in the financial system. Effectively addressing this challenge is going to require all stakeholders—from banks to social media platforms—to each pull their weight and to act above and beyond what is currently legally required.

The situation reminds me of trash left on the street. I live in the city. Technically, litter that is not on my property is not my concern. I have no obligation to pick it up. Neither do my neighbors. And yet if no one picks up the errant bits of litter when they walk by, then more litter tends to appear. Passersby feel it is OK to drop their wrapper on the ground or leave their empty cup on the sidewalk when others have done so. Each act of littering and walking by litter is relatively small. But the cumulative effect is palpable. The neighborhood becomes less nice, less inviting, less orderly, less valued, and can even feel less safe. Over time, if left unaddressed, the situation becomes accepted as normal.

The steady rise and pervasiveness of fraud today presents each stakeholder, including regulators, with a choice. If everyone does only the minimum of what is legally required of them, consumers will continue to be harmed, people's distrust in each other and in institutions will continue to rise, and elevated levels of fraud will become normalized.

The most efficient and effective way to avoid this outcome would be for each and every stakeholder to step up and do their part to combat fraud. This would mean getting in the habit of leaning down and picking up the proverbial trash instead of just walking by it, even if doing so isn't legally required.

Fortunately, the banks I've spoken to about addressing fraud are open to this; many have already begun to act.

First, I should note the importance of complying with existing laws and regulations to promptly identify, investigate, and resolve fraud concerns, such as under the Expedited Funds Availability Act (Regulation CC), and to address potentially unfair practices prohibited under Section 5 of the Federal Trade Commission Act and Section 1031 of the Dodd–Frank Act. When consumers fall victim to fraud or scams, they should have confidence that their bank will comply with applicable laws when researching potentially fraudulent check, debit, and credit card transactions, including the provisional credit requirements of the Electronic Fund Transfer Act (Regulation E) and the billing error requirements of the Truth in Lending Act (Regulation Z).

Second, we've seen many banks increase their individual efforts to address fraud. These efforts include providing bank customers with relevant information about trending scams and how to avoid them and improving or tightening fraud detection and monitoring systems to identify potential frauds in a timely manner. I have heard countless stories of bank branch employees going the extra mile to educate customers about the risks of wiring all their funds to a suspicious account.

Third, several bank trade groups have formed fraud task forces to collaborate and share information. For example, the American Bankers Association (ABA) has created a check fraud claim directory,[1] which is intended to help banks needing to file a check warranty breach claim with another financial institution. The Independent Community Bankers of America formed a check fraud task force of banks and state bankers' associations and leads a financial sector fraud working group.[2] And Early Warning System (EWS), which operates the bank-owned Zelle network and was recently cited by the Senate Permanent Subcommittee on Investigations for various weaknesses,[3] has taken steps to further strengthen its fraud detection program.

While these and other initiatives are promising and more needs to be done, banks and industry trade groups cannot effectively address fraud all by themselves. Take, for instance, check fraud. The recent rise in check fraud can be traced in large part to bad actors intercepting checks sent through the U.S. Post Office. To combat this, the ABA and the U.S. Postal Inspection Service announced a joint effort to combat check fraud in March 2024.[4] The joint initiative focuses on educating U.S. Postal Service and bank customers, addressing money mules and collusive accountholders, collaborating with law enforcement, and training bank employees and postal workers on red flags and prevention.

---

[1] American Bankers Association, "ABA Fraud Contact Directory."

[2] Independent Community Bankers of America, "Community Banks Are Fighting Check Fraud on the Front Lines," March 20, 2024.

[3] See U.S. Senate Permanent Subcommittee on Investigations, Majority Staff Report, *A Fast and Easy Way to Lose Money: Insufficient Consumer Protection on the Zelle Network*, July 23, 2024; U.S. Senate, Committee on Homeland Security and Governmental Affairs, "An Oversight Hearing to Examine How Zelle and the Big Banks Fail to Protect Consumers From Fraud," July 23, 2024.

[4] American Bankers Association, "ABA and U.S. Postal Inspection Service Announce Partnership to Combat Check Fraud," March 19, 2024.

Similarly, a significant amount of fraud on peer-to-peer payment platforms originates from users responding to unsolicited text messages, emails, and social media posts.[5] In the United Kingdom, where liability for such fraud has been assigned to banks, several banking organizations have established a partnership with Meta, the owner of Facebook, to share information via a Fraud Intelligence Reciprocal Exchange. While relatively new, reports indicate that in an early pilot, Meta removed 20,000 scam accounts based on the collaboration.[6]

In a sign that fraud may be becoming normalized, so-called first party fraud is also on the rise. Take, for instance, the recent check-kiting social media posts regarding JPMorgan ATMs that went viral on TikTok. A temporary technical glitch let customers deposit large checks in ATMs and withdraw funds immediately before the checks could clear. Recent media reports noted that the bank is investigating thousands of possible check fraud incidents related to this ATM glitch.[7]

A laissez-faire view of this might conclude that as long as no laws or regulations are being violated, elevated levels of fraud may simply be the new normal, the cost of innovation

---

[5] Federal Trade Commission, "Who Experiences Scams? A Story for All Ages," December 8, 2022. For instance, according to data from the Federal Trade Commission, in 2021 social media was the single biggest starting point for scams against Americans ages 18–59; 31 percent of people in that age range who reported losing money to a scam said that the scheme started on social media. For those ages 18–29, nearly 40 percent of those who reported losing money to a scam said the scam originated on social media. Among adults 60 years or older, that percentage was 15 percent. See also Payment Systems Regulator Ltd., *Authorised Push Payment (APP) Scams Performance Report*, July 2024.

[6] *PYMNTS*, "Meta Teams With UK Banks to Fight Scammers," October 2, 2024.

[7] For example, *Payments Dive*, "Viral JPMorgan Chase Glitch Is 'Fraud, Plain and Simple,' Bank Says," September 4, 2024; *Reuters*, "JPMorgan Sues Customers Over Check Fraud Linked to Glitch That Went Viral," October 28, 2024.

and technological advancement. I believe this underestimates the cumulative sense of disorder and distrust that can emanate from seemingly small but repeated acts of fraud.[8]

As with many collective action problems, public-private partnerships can be effective. For instance, coordination and information-sharing efforts focused on cyber risks provide a useful model for consideration. At the OCC, we are focused on supporting and encouraging these and other collaborative fraud education and fraud prevention efforts. In addition, we are regularly engaging with our partners in interagency and international efforts to strengthen regulatory and supervisory responses to financial fraud. This includes participating in various working groups with representatives from industry, financial regulators, and law enforcement.

Banks and bank regulators can and will need to do more to address fraud. But they cannot solve the problem on their own. Social media platforms, telecommunication companies, email hosts, the U.S. Postal Service, and law enforcement need to step up and do their part as well to keep the proverbial streets clean, safe, and trusted. The OCC looks forward to continued and enhanced collaboration with all stakeholders to address this important issue.

---

[8] See *The Ezra Klein Show*, "The Hidden Politics of Disorder,", Apple Podcasts, October 18, 2024.