

'Pig butchering' schemes are an emerging risk for U.S. financial institutions

By Joseph Cioffi, Esq., and Nicole Zatserkovniy, Esq., Davis+Gilbert LLP

MARCH 24, 2026

"Pig butchering" schemes, once considered a niche type of consumer fraud predominantly occurring overseas, have become a source of legal exposure for U.S. financial institutions that facilitate payments authorized by their customers but induced by a scam.

Recent lawsuits, including a high-profile case against HSBC's U.S. banking arm brought on behalf of an elderly customer, highlight the stakes for any bank that fails to identify and stop such a scheme before the consumer is harmed.

Anatomy of a pig butchering scheme

Pig butchering victims are the subject of prolonged grooming by fraudsters. The fraudsters typically initiate contact through social media, dating apps, or messaging platforms and build trust, often in a romantic context, over weeks or months. They then introduce a purported investment opportunity, often involving cryptocurrency or foreign exchange. After victims make an initial transfer, they are then shown fabricated "returns," which induce them to escalate their investments until, finally, the scammer disappears with their funds.

The Financial Crimes Enforcement Network (FinCEN) has identified this typology as a national priority risk, noting that these schemes rely on legitimate U.S. banking channels, wires, ACH transfers, and fiat-to-crypto conversions before funds are laundered offshore. Unlike account takeovers or identity theft, the transactions are typically authorized by the customer, complicating both reimbursement and enforcement.

The HSBC lawsuit as a bellwether

Filed in California federal court by conservators, the HSBC case centers on an elderly customer who allegedly lost more than \$8 million after being groomed online through two separate romance-based scams. See *Song Dow Lee v. HSBC Bank USA, Nat'l Ass'n*, No. 2:26cv01198 (C.D. Cal. Feb. 5, 2026).

According to the complaint, the victim was first contacted on social media by an individual posing as a successful investor. The investor gradually built trust with the victim before introducing a purported overseas investment opportunity. What appeared to be early returns were allegedly fabrications designed to encourage increasingly large wire transfers.

After another bank curtailed his ability to continue wiring funds, the victim allegedly opened an account with HSBC and resumed the transfers. Plaintiffs claim the bank processed high-dollar, in-person wire transfers despite escalating amounts, foreign beneficiaries, and patterns inconsistent with the customer's prior banking history.

Recent lawsuits, including a high-profile case against HSBC's U.S. banking arm brought on behalf of an elderly customer, highlight the stakes for any bank that fails to identify and stop such a scheme before the consumer is harmed.

Although HSBC reportedly imposed account restrictions, those controls were allegedly lifted, allowing additional transfers to proceed. The complaint asserts claims of negligence, breach of fiduciary duty and violations of California's elder financial abuse laws. More broadly, the case presents a developing legal theory that prolonged inaction in the face of clear indicators of social engineering fraud may support civil liability, even where the customer technically authorized the transactions.

As of the time of writing, HSBC has not yet answered the complaint as the case has been referred to mediation and the deadline to file an answer was extended to March 25, 2026.

Existing federal law: a patchwork fit for a different era

Under current federal law, consumer protection for fraudulent transfers largely depends on whether the transaction was "unauthorized." The Electronic Fund Transfer Act (EFTA) and its implementing Regulation E generally require consumers to be reimbursed for unauthorized electronic transfers. They do not address, however, transactions the customer personally

authorizes that are induced by fraud. Pig butchering schemes fall squarely into that gap.

Even so, banks are not free from federal obligations. The Bank Secrecy Act (BSA) requires financial institutions to maintain anti-money laundering (AML) programs, conduct customer due diligence and file Suspicious Activity Reports (SARs) when transactions raise red flags of fraud or money laundering. In September 2023, FinCEN issued a specific alert on pig butchering scams, identifying behavioral and transactional indicators and directing institutions to tag SARs accordingly. See FinCEN Alert, FIN-2023-Alert005, September 8, 2023 (<https://bit.ly/4rAaw0D>).

The BSA does not create a private right of action, but it can be used by plaintiffs indirectly. The theory is that failure to act on obvious red flags, particularly after FinCEN guidance, supports a finding of negligence or actual knowledge. In elderfraud cases, plaintiffs could argue that banks crossed the line from passive intermediaries to active facilitators by repeatedly processing suspicious transfers without intervention.

Potential paths for U.S. regulation

In the United States, regulatory change is more likely to be incremental than sweeping. One plausible path is the expansion of safeharbor regimes that both encourage and require intervention. Federal regulators could, for example, authorize temporary holds on suspicious wires tied to socialengineering fraud, coupled with immunity from liability when banks delay transactions in good faith.

Many states already authorize financial institutions to impose temporary holds or freezes on accounts when there is reasonable suspicion of fraud or financial exploitation. Given the proliferation of fraudulent schemes, there appears to be a growing acceptance that shortterm, preventive restrictions on account access are an appropriate consumerprotection measure. This existing patchwork of state laws may serve as a foundation for more uniform standards governing when and how such temporary freezes may be imposed.

Another pathway is clearer federal guidance tying AML obligations to consumerprotection outcomes. FinCEN's pig

butchering alert already moves in this direction by articulating specific red flags and expectations. Over time, such guidance may crystallize into examination standards, raising the stakes for noncompliance.

Looking ahead, regulators may also consider a federal regulation akin to FINRA Rule 2165, which currently permits brokerdealers to place temporary holds on disbursements or transactions for "specified adults," generally individuals aged 65 and older or vulnerable adults, when financial exploitation is reasonably suspected.

A similar federal rule applicable to banks or payment providers could formalize the authority to impose shortterm holds while investigations proceed, pairing that authority with notice, documentation, and timelimit safeguards. Such an approach would build on existing state frameworks and reflect growing regulatory acceptance of preventive intervention in cases of suspected exploitation.

Even absent statutory overhaul, courts may prove more receptive to arguments that banks cannot ignore prolonged, obvious fraud simply because the customer clicked "send."

Conclusion

Pig butchering schemes challenge longstanding distinctions between authorized and unauthorized transactions. Regulators have made clear that these scams are no longer novel or obscure, and litigation such as the HSBC case signals a growing willingness by plaintiffs to argue that repeated processing of transactions with obvious red flags can give rise to civil liability, particularly where vulnerable customers are involved.

Going forward, compliance frameworks built solely around technical authorization may be viewed as insufficient. Courts and regulators may have higher expectations for judgment and intervention when exploitation is apparent. As pig butchering schemes proliferate, bankers beware: Inaction may be actionable.

Joseph Cioffi is a regular contributing columnist on consumer and commercial financing for Reuters Legal News and Westlaw Today.

About the authors



Joseph Cioffi (L) is chief operating partner at **Davis+Gilbert LLP**, where he is also chair of the bankruptcy, creditors' rights and finance practice. He has transactional, insolvency and litigation experience in sectors marked by significant credit and legal risks, such as subprime lending and emerging industries. He can be reached at jcioffi@dglaw.com.

Nicole Zatserkovniy (R) is an associate in the bankruptcy, creditors' rights and finance group at the firm. She works with lenders, financial institutions, creditors, and businesses across a range of industries, assisting with complex bankruptcy, litigation, and transactional matters. She can be reached at nzatserkovniy@dglaw.com. The firm is located in New York.

This article was first published on Reuters Legal News and Westlaw Today on March 24, 2026.