



FRAUD SPOTLIGHT

Banks pay the price when they miss the signs of fraud

BY CATHERINE MUSTICO, CFE, MARY SCOTT

SHARE: SAVE:



WRITTEN BY:
[Catherine Mustico, CFE](#)
[Mary Scott](#)

DATE: MARCH 2, 2026
READ TIME: 8 MINS

Anti-Fraud Laws Regulations and Compliance

Consumer Fraud and Scams

Investigation

Banking and Financial Services

As fraud schemes grow more sophisticated, banks are increasingly facing scrutiny for denying customer reimbursement claims in the presence of clear red flags. Fraud examiners can lead the shift toward evidence-driven reviews, stronger controls and more accountable institutional responses.

“Bill” (a pseudonym) received a call from someone posing as his financial institution’s fraud department warning that his account had been hacked and directing him to a link to secure it. He clicked on the link and signed in with his credentials, unknowingly handing over access to his account. A fraudster impersonating a bank employee liquidated his mutual fund holdings within hours. By the next day, a series of wire transfers for \$99,900 to accounts in Hong Kong had drained his life savings.

Nothing about these transactions resembled his usual activity. He’d never wired funds or liquidated investments in this way, yet the transactions went through. When the institution learned of the loss, its response was blunt: Nothing could be done. Bill had used his credentials and verified the activity. He then received a denial letter for his reimbursement request.

Ad

Rather than accepting the bank's decision, Bill hired an attorney who retained me (Catherine Mustico, CFE) through my firm, Fundamental Compliance Consulting, LLC, to reconstruct the events that led to Bill's loss. What our review revealed wasn't just troubling but illustrative of a larger, recurring issue affecting financial institutions and their customers.

As I reviewed the documents, including the recorded calls, what happened became clear. Bill misunderstood later conversations with his financial institution about "fraud on the account," believing he was helping resolve a problem the scammer had fabricated. The recordings made this disconnect unmistakable.

After receiving confirmation emails about the liquidations, Bill contacted his institution. The sales had occurred, but the proceeds hadn't yet moved out of his account. Still convinced the initial impersonation call was legitimate, he told representatives that the "fraud department" had instructed him not to log in for two days. During that window of time, the institution still had the ability to stop the loss.

Internally, representatives recognized that no legitimate fraud team would tell customers to avoid accessing their accounts. That recognition, however, was never clearly communicated to Bill. Bank representatives also didn't inform him that his account had been secure before the impersonation, no fraud had been detected, and the threat arose solely from the access the scammer had obtained.

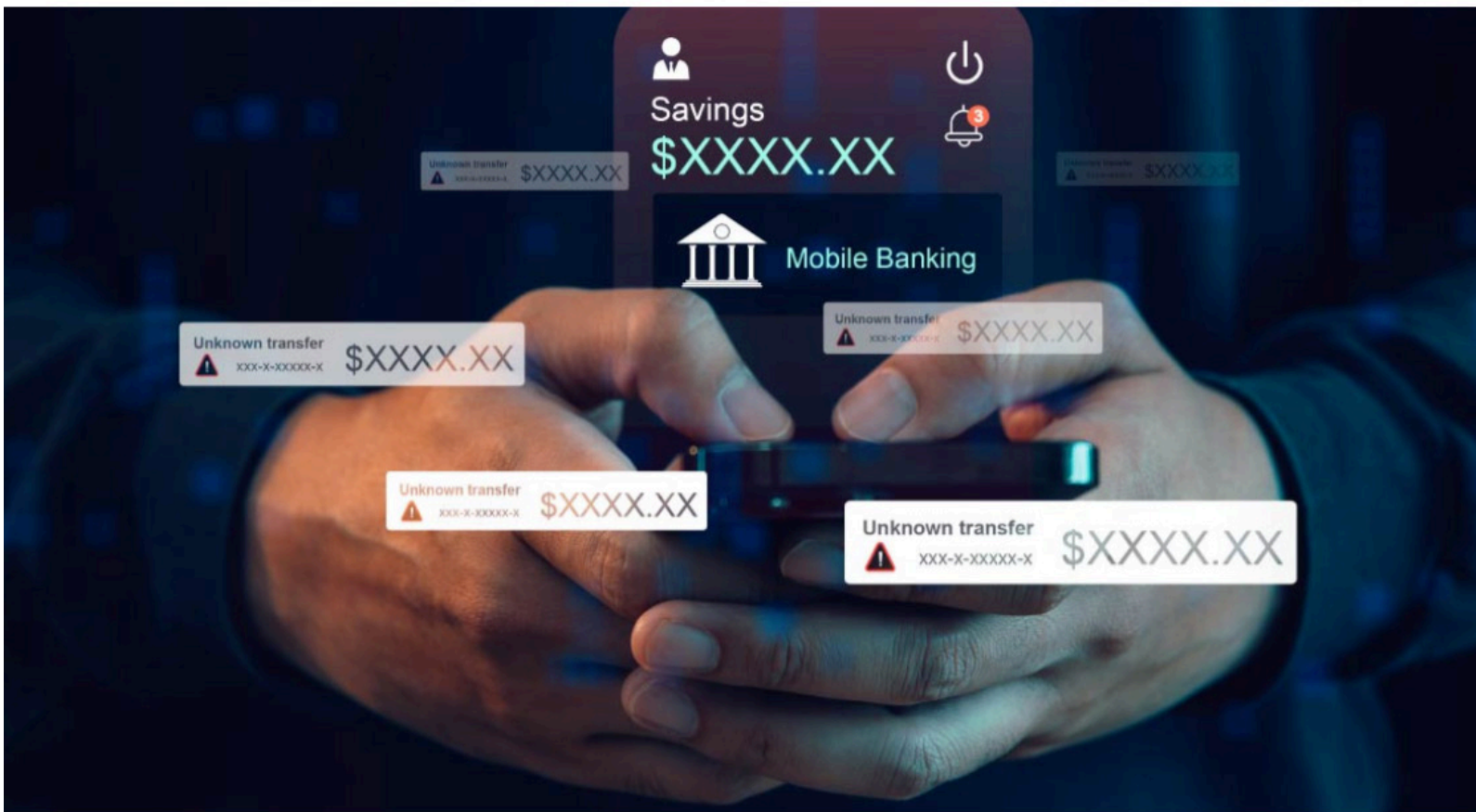
Compounding the confusion, the institution told Bill to expect a follow-up call from the fraud department, priming him to accept later contact from the impersonator. Still believing he was following legitimate instructions, Bill later called to restore his online access. A representative unlocked the account without questioning the request, and fraud department notes visible to the representative further reinforced the false narrative instead of prompting intervention.

With access restored, the impersonator wired Bill's money without his knowledge. His cooperation wasn't careless; it was shaped by his interactions with the institution, which never corrected the misinformation.

These findings were central to my expert opinion. The bank's controls failed. Bill didn't. If employees with system access and training couldn't distinguish fact from fiction in real time, a customer with no internal insight certainly couldn't. Ultimately, Bill reached a settlement in which the bank absorbed the loss and litigation costs.

Bill's case isn't rare; it's representative. Not every loss is reimbursable, and banks aren't liable for every fraud case, as each case turns on the unique facts and circumstances. But when impersonation crosses into account takeover, institutions have independent obligations to detect red flags and intervene. That's the point where denials based on "customer authorization" collide with internal data that says otherwise.

In this column, we encourage fraud examiners to ground investigations in data and enforce procedural rigor to push for better controls and more responsible responses from financial institutions. Case studies of banks that denied customer reimbursement claims and didn't follow procedures serve as examples of banks' duties to monitor accounts, detect red flags, address suspicious activity, and in some circumstances, prevent or mitigate identity theft.



WHEN IMPERSONATION CROSSES INTO ACCOUNT TAKEOVER, INSTITUTIONS HAVE INDEPENDENT OBLIGATIONS TO DETECT RED FLAGS AND INTERVENE.

What fraud victims don't know

While Bill's story had a happy ending, many victims of financial fraud aren't as lucky. As fraud examiners, we've all seen it play out: A consumer responds to a text that mirrors a legitimate bank alert or a phone call featuring a voice that sounds authoritative and informed. And before they realize what's happened, their funds have vanished.

Fraud awareness campaigns are clear: Don't click the link, don't respond to the text, and don't answer the call. That advice is sound, but consumers can't be the primary line of defense. Institutions have roles to play, as well. Financial fraud events often involve sophisticated social engineering, credential theft or system-level deception that far exceeds an individual's ability to detect or prevent them.

What fraud victims often don't know, and what fraud examiners must remember, is that independent regulatory obligations overlap in ways institutions can't avoid. The specific frameworks may differ depending on whether the institution is a bank, broker-dealer or another intermediary. But the through line remains the same: Institutions are expected to maintain systems reasonably designed to monitor activity, detect red flags, respond to suspicious circumstances and, in certain contexts, mitigate harm.

Suspicious activity monitoring frameworks require institutions to identify and respond to red flags of potential money laundering, including red flags of predicate crimes that generate illicit proceeds. Theft, fraud, forgery and identity theft aren't merely customer problems. They're underlying crimes that produce illicit funds moving through the financial system.

The U.S. Bank Secrecy Act (BSA) of 1970 requires financial institutions to help the government fight money laundering, tax evasion and terrorism financing by keeping records and reporting suspicious activities and large cash transactions (over \$10,000) to the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN). The regulations require financial institutions to adopt monitoring systems reasonably designed to identify suspicious activity, investigate it and respond.

Identity theft regulations such as the Red Flags Rule apply to banks' responsibilities to their customers. The rule, part of the Fair Credit Reporting Act, requires financial institutions and creditors to implement identity theft prevention programs to detect, prevent and mitigate identity theft in covered accounts, such as credit cards, mortgages and auto loans. These programs identify "red flags" (unusual account activity or fraud alerts), establish appropriate responses (denying access or delaying any changes until heightened verification), and require staff training and oversight.

Financial institutions are part of the defense system against fraud because they're required to be. Telling people not to click a link or answer a call is only half the message. The other half should be focused on financial institutions as part of the defense system.



Customers take banks to court

Fraud victims are suing their financial institutions over the troubling pattern in banks' responses to unauthorized transfer claims. Recent cases show that when consumers report clear signs of impersonation fraud or account compromise, institutions sometimes deny reimbursement by treating coached customer actions as authorization rather than a crime. The lawsuits and regulatory scrutiny that follow highlight the widening gap between consumer vulnerability and institutional responsibility.

In 2024, two Pennsylvania consumers filed a class-action lawsuit against Wells Fargo, alleging the bank unlawfully refused to reimburse them after a fraudster made a large unauthorized wire transfer from their account. The plaintiffs immediately reported the fraud to Wells Fargo, which initially acknowledged the dispute. However, days later the bank declined reimbursement, stating the transaction was considered “authorized” because the customer had provided a verification code. Wells Fargo repeatedly refused to return the funds and ultimately closed the case in 2024.

The lawsuit argues that Wells Fargo’s actions violate the Electronic Fund Transfer Act (EFTA), which limits consumer liability for unauthorized electronic transfers when theft is reported within the proper timeframe. Plaintiffs claim they followed all required steps but were still held responsible for losses caused by impersonation fraud. The case is ongoing.

In 2024, New York Attorney General Letitia James filed a lawsuit against Citibank, accusing the bank of failing to protect customers from fraud and unlawfully refusing to reimburse victims whose accounts were drained by criminals. According to the complaint, Citibank allegedly maintains weak data security and anti-breach controls, allowing criminals to gain access to customer accounts and steal millions. James argues that Citibank not only failed to detect or respond to red flags, such as suspicious login attempts and unauthorized wire transfers, but also misled consumers about their rights under the EFTA and improperly denied reimbursement claims.

Two Citibank customers reported substantial losses from scams, but both say the bank refused to reimburse them. In the first case, a woman received a fraudulent text message that ultimately allowed a scammer to reset her banking password and move \$40,000 out of her retirement account. In the second, a scammer used deceptive tactics to move funds between a customer’s accounts and initiate a wire transfer. Citibank reportedly approved these unusual transactions without contacting her, resulting in a loss of \$35,000. The bank allegedly refused to reimburse both customers.

A federal judge ruled in January 2025 that the case could move forward, rejecting Citibank’s attempt to dismiss the lawsuit. The court found that the EFTA does apply to certain unauthorized wire transfers, contradicting Citi’s argument that such transfers are exempt.

In addition to consumers taking legal action against banks, regulators are stepping in when financial institutions don’t follow procedures and ignore red flags. They may face massive fines, consent orders, admissions of unsafe practices, operating restrictions, executive bans and ongoing regulatory supervision.

In 2024, the U.S. Securities and Exchange Commission (SEC) imposed a \$15 million penalty on Morgan Stanley after finding that the firm had failed to maintain adequate cybersecurity measures, leading to the exposure of sensitive client information and enabling unauthorized transactions. According to the SEC, four financial advisers, later barred from the industry, had executed hundreds of unauthorized transactions, stealing millions of dollars from clients’ accounts. The SEC concluded that the firm failed to adopt “policies and procedures reasonably designed to prevent and detect such theft.”

Morgan Stanley agreed to settle without admitting to or denying the allegations and stated that it had strengthened its data security systems, including improving encryption and access controls. The SEC's enforcement action demonstrates regulators' increasing emphasis on cybersecurity, fraud prevention, and the duty of financial institutions to proactively protect customer accounts from compromise and exploitation.



IN ADDITION TO CONSUMERS TAKING LEGAL ACTION AGAINST BANKS, REGULATORS ARE STEPPING IN WHEN FINANCIAL INSTITUTIONS DON'T FOLLOW PROCEDURES AND IGNORE RED FLAGS.

An opportunity for fraud examiners

Institutions see what customers can't. They have access to authentication logs, device indicators, behavioral baselines, internal notes, alert histories and claims data. Customers don't. Financial institutions can't reasonably outsource primary fraud defense to consumers, and banks' post-loss determinations can't rest solely on customer explanations offered under stress and shaped by coaching. Fraudsters use well-tested techniques to gain access to accounts, including scripts that instruct victims on what to say, how to express urgency and how to deflect skepticism.

For this reason, fraud examiners can't accept customer narratives as conclusions. They're starting points. Fraud examiners' roles are to test them against the data customers can't see. Claims data should be analyzed not only for recovery outcomes, but for patterns revealing where controls require recalibration. Repeated denials aren't merely outcomes; they're data points.

Bill's loss and recovery relied on evidence, not a narrative. The controls failed; the customer didn't. Fraud examiners are uniquely positioned to lead this shift toward evidence-driven reviews, stronger controls and more accountable institutional responses. By insisting on evidence, resisting oversimplified narratives and ensuring that adopted processes are followed we can do better. For fraud examiners, this isn't just a cautionary tale; it's an opportunity to lead.

Catherine Mustico, CFE, is managing director of Fundamental Compliance Consulting, LLC. Contact her at Catherine.Mustico@fundamentalcc.com.

Mary Scott is the director of operations at Fundamental Compliance Consulting, LLC. Contact her at Mary.Scott@fundamentalcc.com.