Data on Reported Fraud Claims on Zelle is Misleading: Here's Why

BANK POLICY INSTITUTE

First, banks employ many safeguards to identify and prevent cases of fraud before they materialize.

- Rigorous customer onboarding consistent with relevant laws (e.g., customer due diligence and "Know Your Customer" requirements)
- Account access safeguards and cybersecurity best practices (e.g., encryption, one-time verification codes and multi-factor authentication, zero-trust architecture)
- Consumer education campaigns and helpful and timely notices to customers when authorizing Zelle transfers to be mindful of scams and tricks
- Transaction verification and monitoring
- Ongoing collaboration with law enforcement and national intelligence
- Regulatory requirements to limit customer liability for unauthorized transactions (e.g., Regulation E)

Still, not every instance of fraud reported by consumers on Zelle can be prevented. When customers report fraud, banks investigate and — as required by law — always reimburse customers for transfers confirmed to be unauthorized and fraudulent.

A fraudster hacks into a customer's online or mobile account and makes a payment with Zelle without the customer's permission, and the customer wasn't involved in any way with the transaction.

In some instances, although not required by law, banks will reimburse customers that are scammed — fraudulently induced — into authorizing a payment or transfer.

A "me-to-me" scam where a scammer pretends to be a representative of the customer's bank and induces the customer into making a transfer themselves.

Red flags that indicate possible fraud:

- Unrecognized internet service providers
- Abnormal location or device activity
- Changes to account contact information
- Unusual transaction volume and amounts
- Infrequent or abnormal activity with the transfer recipient
- Password changes
- Failed login attempts, including biometrics
- Frequent or sudden P2P token transfers

Banks don't reimburse every reported Zelle fraud claim.

Not every fraud claim is actual fraud.

- A customer may mistakenly report a forgotten purchase as a fraudulent transaction. Banks open investigations and work with the customer to provide more information when fraud claims are filed. During that process, the customer may recall that the transaction was valid. While the claim is dismissed and the customer is satisfied, the report still counts toward a bank's total reported cases of fraud.
- Another example involves transactions where a customer authorized the purchase but did not receive the product or service that they expected. A customer makes an online purchase and the product is delivered broken. A customer may file a claim with bank when the online retailer's customer service center is unresponsive or they can't come to an agreement with the merchant.
- While many fraud claims may be based on customer confusion or a mistake, there are also some who knowingly file false fraud claims to seek reimbursement for authorized purchases. These individuals try to exploit the underlying consumer protections offered by banks.

Banks are also not responsible for scams (i.e., payments authorized by the customer).

- A customer placed a down payment with a contractor for work on a home improvement project but the contractor never showed up to complete the work. The customer was clearly defrauded, but the bank is not nor should be liable.

Banks are not required by law, nor should they be, to reimburse transactions customers authorized. Expanding the current liability framework for banks would force Zelle providers to either scale back Zelle's popular instant P2P services, given the financial risk, possibly limit the instantaneous features or impose fees to recover their additional costs. Either way, consumers' access to these valued services would be limited, forcing them to meet their needs outside the well-regulated banking system.

Common signs there is no fraud (false claims):

- Service provider is consistent with login history
- No new devices added
- No contact history changes
- Past activity with Zelle recipient
- No recent password changes
- No failed attempts with facial recognition / fingerprint sign in
- No activation codes generated