MEDIA FACTS

# The Facts About Zelle® and Scams

## The threat doesn't start where you think it does.

Fraud and scams are increasing in both sophistication and scale, but they don't begin on payments platforms like Zelle®. Instead, they often start with manipulative tactics from criminals, both foreign and domestic, who exploit Americans long before any money changes hands. These scams originate through phone calls, text messages, or online marketplace ads that mislead people into sending money under false pretenses.

The growing availability of generative AI is also making impersonation scams even more dangerous, enabling fraudsters to convincingly mimic the voices and identities of loved ones or trusted authorities.

## How Zelle Protects Consumers

Since the launch of Zelle, more than 99.8% of payments have been completed without a report of fraud or scam. We've continued to improve our fraud and scam defenses, and today more than 99.95% of transactions are completed without any report of scam or fraud.

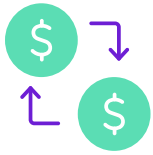
Our participating financial institutions must meet the highest standards when protecting consumers.

**Zelle requires all participating financial institutions to:**

Use authentication and enrollment controls, which may include (but are not limited to) two-factor authentication, biometric data, encrypted identity verification data, and real-time monitoring of enrollment tokens.

Send in-app alerts that help protect consumers from scams. Every year, millions of in-app alerts are sent to consumers before they send a payment.

Utilize data-driven technology for real-time identification of potential bad actors, allowing financial institutions to intercept and stop potentially high-risk transactions.



Fully reimburse customers for any instance of confirmed fraud after a reasonable investigation, surpassing the requirements of the Electronic Fund Transfer Act (EFTA) and Regulation E. Zelle also goes above and beyond what is required by law and requires reimbursement for customers for certain qualifying imposter scams where the customer authorized the transaction.

# Empowering Consumers to Stay Safe

While we continue to invest in technology and policies to protect consumers, below are a few actions everyone can take to reduce their risk of falling for a fraud or scam:

### Verify the Recipient

Only send money to someone you know, trust, and can confirm their identity. Once you approve sending the funds, the money leaves your account and is often unrecoverable.

### Don't Trust Caller ID

Scammers can spoof a legitimate phone number by altering caller ID.

### Wait and Validate

Scammers will try to rush you into acting, so you won't take time to stop, think, and verify facts.

### Stop and Get Help

If you are uncomfortable with a request received by a phone call or text that you didn't initiate, don't respond and hang up immediately. Contact the company using legitimate sources.

## Working Together To Stop Fraud and Scams at the Source

Stopping criminals from targeting individuals requires collaboration across industries, including government, social media, telecommunications, and financial services. No single sector can solve this problem alone.

To address this growing threat, we strongly support bipartisan legislation like the **Task Force for Recognizing and Averting Payment Scams (TRAPS) Act,** which would create a dedicated federal taskforce to target and disrupt criminal networks that are exploiting American consumers.

By working together across industries and with lawmakers, we can build a stronger, safer digital payments environment for everyone.

## If you believe that you've been a victim of a fraud or scam, you should:

**Contact Your Bank or Credit Union**
They are required by law to investigate reports of fraud or scam.

**Alert the Federal Trade Commission (FTC)**
Call the FTC's Fraud Victim Assistance Department at **(877) 438-4337.**
You can also submit a fraud report or identity theft report.