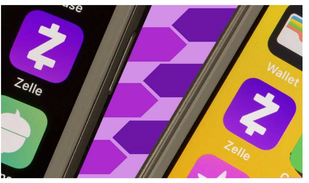
SCAMS & FRAUD

How to Avoid Scams on Zelle, Venmo and Other P2P Apps

Criminals love peer-to-peer payment methods; learn to use them safely

By Matt Alderton, AARP
Published January 19, 2024 • EN ESPAÑOL



ALAMY STOCK PHOTO

Michelle Cohen, M.D., 59, a psychologist in Delray Beach, Florida, was looking for an Italian greyhound puppy when she found a broker online who specializes in them: Amore Italian Greyhounds.

Because it looked legit, Cohen chose a puppy from nearly a dozen advertised, signed a bill of sale and sent $900 through Zelle, a peer-to-peer (P2P) money-transfer app that allows users to instantly move funds from their own bank account to someone else's. Amore Italian Greyhounds agreed to have the dog transported to Cohen's home — but the puppy never came. Instead, a company called Logistek

Transportation contacted Cohen seeking $2,300 for shipping. Something seemed fishy. When Cohen refused to send payment, all communication ceased. She realized she was the victim of a puppy scam, a disturbingly common crime.

"It was very convincing," Cohen says. "I showed the website to my whole family, and nobody questioned it until after I lost the money. That's when my niece looked it up online and found some comments about them not being real breeders." Although she contacted both the police and her bank in an effort to get her money back — the latter even opened a fraud investigation — she was told that there was no way to recover her lost funds. "The money's gone," she says.

Cohen, who reported the incident to the AARP Fraud Watch Network Helpline, isn't alone. Because they're as fast and convenient for criminals as they are for consumers, Zelle and other P2P payment apps — including PayPal, Venmo and Cash App — are favorite tools for modern-day scammers.

Why scammers like P2P apps such as Zelle

Seven of America's biggest banks established Zelle in 2017 to facilitate instant digital money transfers between individuals. Today, more than 2,000 banks and credit unions offer Zelle to their customers through mobile banking apps.

"Zelle is a powerful and very useful service," says Steve Grobman, senior vice president and chief technology officer of online security company McAfee. "Say you go out to eat with your sister and you want to split the check. If your sister slaps down a credit card and pays for it, and you want to send her $50, Zelle is great for that."

The same is true for the other cash-transfer apps.

"Consumers have decided, 'Hey, we want to be able to send money to whomever we want at the push of a button,'" explains Jason Zirkle, a certified fraud examiner (CFE) and training director at the Association of Certified Fraud Examiners (ACFE). "The other side of that is that all of those tools are also vulnerable to scammers."

P2P apps don't have the same consumer protections that credit cards have. Transferring money through them is more like paying with cash because transactions are instantaneous and usually irreversible.

Sen. Elizabeth Warren (D-Mass.) decided to investigate just how vulnerable Zelle is. Based on data furnished by four of Zelle's founding banks, she concluded that Zelle is "rampant with fraud and theft." Published in October 2022, her report found more than 190,000 cases of Zelle-related scams involving more than $213 million in 2021 and the first half of 2022.

Although it declined to provide numbers of its own, Zelle's bank-owned network operator, Early Warning Services, says it's winning the fight against scammers. "Zelle has driven down fraud and scam rates because of our prevention and mitigation efforts implemented across our network of banks and credit unions," a spokesperson for Early Warning Services told AARP. "Less than one-tenth of 1 percent of transactions are reported as a potential fraud or scam, and the percentage keeps getting smaller."

To educate consumers, Early Warning Services recently launched a series of online videos on Vox.com featuring the S.A.F.E. (Scam and Fraud Elimination) Squad, a team of investigators led by actor and producer Christina Ricci that explores and combats impostor scams. The campaign features an interactive website with facts about impostor scams and quizzes to help consumers test their knowledge.

Top Zelle and other P2P scams

- **Impersonation scams:** Criminals often persuade victims to send money by pretending to be someone they're not — for example, your grandson asking for money to pay an uninsured motorist with whom they just got into a car accident, a federal agent collecting outstanding taxes or a bank employee asking for a deposit to keep your account active. Thanks to artificial intelligence (AI) — with which scammers can clone real voices and faces — impostor scams are becoming even more common and more difficult to detect.
- **Fake seller scams:** Criminals on Facebook Marketplace or another online platform advertise a fake product or service, collect your money upfront, then disappear without delivering the goods.
- **Advance-fee scams:** Do you remember the "Nigerian prince" scams of the 1990s? Someone claiming to be royalty emails purporting to have temporarily lost access to their wealth. They're in trouble and need your help. In exchange for assistance, they promise a hefty reward once they retrieve their fortune. That's an advance-fee scam. Lottery scams — someone claims you've won the lottery and offers to send your winnings in exchange for a service fee — are another example.
- **Phishing scams:** Phishers want you to click a link that allows them to install malware on your device or otherwise record your Zelle or Venmo (or other app) credentials, which they can use to access your bank account. A common scenario, especially during the holidays, are delivery-related scams, often in the form of a "missing package" text that claims you have a lost package you can retrieve by clicking a link.

Reimbursing victims

In August, Early Warning Services announced a "new consumer reimbursement benefit for specific scam types." It didn't detail which scam types were eligible, and a spokesperson wouldn't elaborate on the statement, but Zelle suggests on its website that reimbursement is dependent on banks' policy: Unauthorized transactions (where the consumer had no involvement in the fraudulent transaction, such as when a criminal gains access to your account) can be reimbursed. But authorized transactions (where an account holder makes the transaction, even if the money ends up in the hands of a scammer) are not reimbursable. In all cases, Zelle says, you should contact your financial institution, but if you authorized the payment "you may not be able to get your money back."

Venmo also offers advice on scams on its site and says to report them to the Venmo support team. It warns that it can't reverse a payment unless the recipient gives their explicit permission. PayPal's site includes similar advice.

How to protect yourself from P2P scams

- **Only use Zelle, Venmo and other P2P apps with trusted parties:** Grobman says they are best used with people you know and trust — friends and family members, for example, or local businesses with brick-and-mortar locations and flesh-and-blood employees. If you're transacting with someone new or unseen, it's best to use a credit card. Or better yet, a virtual credit card from your card issuer, which uses a disposable number that's different from the number on your physical card. If a business accepts payments only through a P2P app, that's a red flag.
- **Be suspicious of out-of-the-blue requests:** Whether it's a knock on your door, an email, a text message or a chat request on social media, beware of unsolicited requests, says Michael Steinbach, head of financial crimes and fraud prevention at Citi, whose mantra is, "Don't take it; make it." If you get an unsolicited call from your bank, for example, don't take the call. Instead, look up the bank's phone number online and make an outbound call to ask if it was legitimate. Be especially wary of urgent messages, Zirkle says; legitimate businesses don't ask customers to send information or money "right now."
- **Treat digital payments like cash:** If you'd hesitate to mail a $100 bill to a stranger, you shouldn't send them $100 through Zelle or Venmo, either.

What to do if you're the victim of a P2P-based scam

- **Lock down your financial profile:** Take the same steps you'd take if you'd lost your credit card, suggests Steinbach. That includes setting up alerts with your bank, which can notify you every time there's a new transaction on your account; contacting your bank to change your online banking username and password; and asking the three major credit bureaus to freeze your credit.
- **File a police report:** Although law enforcement probably won't investigate, filing a police report creates a record of the event that can be helpful later in case of additional fraud or identity theft, Zirkle says.
- **Notify the feds:** The Federal Trade Commission (FTC) has a website — ReportFraud.ftc.gov — where you can report fraud.
- **Alert your bank:** If you're using Zelle or another P2P service through an online banking app, you should contact your bank or credit union at the customer support number on the back of your debit card, Early Warning Services says. If you're enrolled with your debit card through the Zelle app, contact Zelle at 844-428-8542.
- **Contact the app.** Go directly to the app's website to reach customer service. If you do a generic web search for a company's customer service department, fake sites built by crooks often will show up among the results — and you could get hit by a whole other scam, the AARP Fraud Watch Network notes.

Matt Alderton is a contributing writer who specializes in health and wellness, travel and technology. His work has also appeared in USA Today, Forbes *and* The Washington Post.