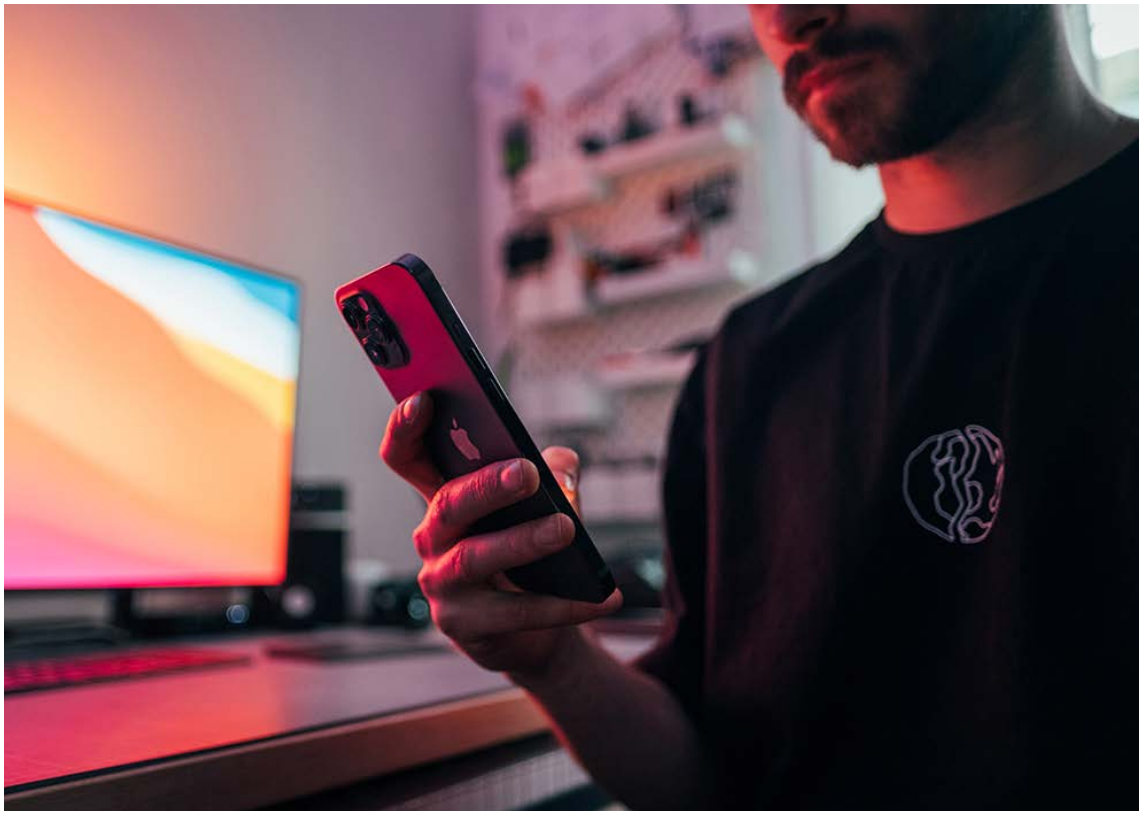
Zelle: to refund or not to refund?

Our latest free report looks at the Zelle payments scam debate: should banks be responsible for refunding victims of fraud and what are the potential implications if this is the case?

Risk Universe by RiskBusiness



WHAT IS ZELLE?

Zelle is a digital payments network owned and operated by seven US-based banks: Bank of America, Truist, Capital One, JPMorgan Chase, PNC Bank and Wells Fargo. Zelle allows consumers to transfer money from their bank into another user's bank account (in the US only) via their mobile device or the bank's website.

Zelle was first launched in 2017, but has been around since 2011 when it was known as clearXchange and was owned by Bank of America, JPMorgan Chase and Wells Fargo.

ZELLE PAYMENT SCAMS

Zelle has recently been at the centre of a widespread spoofing scam where users received spoofing emails (and text messages and phone calls) from scammers claiming they needed to transfer some money into their own bank account (a so-called "me-to-me" payment). In actual fact, the emails and phone calls were part of a sophisticated scam and the funds were immediately transferred to the scammer's account by the victims, using the Zelle platform.

WHY IS ZELLE POPULAR WITH SCAMMERS?

The speed with which Zelle transfers money from one bank account to another is what makes it so attractive to scammers. It allows funds to be instantaneously available and therefore impossible to retrieve if transferred as a result of fraud.

WHO IS RESPONSIBLE FOR REFUNDING STOLEN CASH?

Credit cards and other payment platforms such as PayPal offer the ability to recover funds lost to scammers. However, Zelle does not currently offer this protection to its users – and it has become a hot topic of debate between the large banks who own it and members of US Congress.

ELECTRONIC FUND TRANSFER ACT OF 1978: ARE BANKS WHO USE/OWN ZELLE IN BREACH OF THE RULES?

In April 2022, US Senator Elizabeth Warren launched an investigation into Zelle and the consortium of banks that owns it (known as Early Warning Services, or EWS.) According to Warren's report, the banks involved initially refused to share information on the true extent of fraud committed using their platform. At the time the report was published, JPMorgan and "several other banks" had still refused to share the full details. Only four banks shared their data (and only three provided everything that was requested), however, Warren's review identified the following key findings:

- Fraud and theft are "rampant" on the Zelle platform, and are (according to Warren's analysis) on the rise. The report says the banks who own Zelle make several claims about being "trustworthy", but the number of fraud and scam claims from their customers has increased from 8,848 in 2020, to 12,300 in 2022.
- Banks are not reimbursing most victims of fraud via Zelle. "Overall, the three banks that provided full datasets reported repaying customers in only 3,473 cases," representing 1.8% of the total 192,878 scam claims.
- Banks are potentially violating US federal law and CFPB (Consumer Financial Protection Bureau) rules. "Zelle claims to have a 'zero liability policy' for cases in which a bad actor gains access to a consumer's Zelle account and uses it to make unauthorised payments…the Electronic Fund Transfer Act (EFTA) and the CFPB's 'Regulation E' require that the banks repay customers when funds are illegally taken out of their account without authorisation." According to Warren's analysis of the data submitted for the report, less than half of this money is currently being reimbursed.

EWS claims "tens of millions of consumers use Zelle without incident, with more than 99.9% of payments completed without any report of fraud or scam. Zelle usage has grown significantly since its launch…while the proportion of fraud and scams has steadily decreased." It's important to note that as the number of users of Zelle increases, so too will the number of fraud cases reported by its users. However, according to the latest State of Fraud and Financial Crime Report by PYMNTS, 62% of financial institutions have experienced an increase in financial crime, with 51% of surveyed firms seeing an increase in fraud rates related to Zelle payments specifically.

AUTHORISED VS UNAUTHORISED PAYMENTS

EWS banks are essentially benefitting from a loophole in the current regulations, specifically in how they interpret what is meant by fraud. "The banks have made a distinction between 'fraud' and 'scam' claims on Zelle," says the Warren report. "They generally do not pay consumers back if they are fraudulently induced into making Zelle payments."

This distinction is what is currently being debated in several class-action lawsuits against EWS banks. EWS is essentially saying that clients who were victims of spoofing should have known better, and as

EWS banks are essentially benefitting from a loophole in the current regulations

An argument against tightening regulations in this area is that it impacts the customer onboarding process

they willingly transferred their money over to fraudsters (i.e. they weren't hacked), EWS should not be responsible for refunding them.

"At face value, there appears to be some merit to this argument," says class-action law firm Shamis and Gentile PA. "However, federal law does actually require banks to reverse fraudulent transactions. When they are alerted to this fact by customers, their legal representatives or consumer watchdog organisations, they quickly reverse their position and pay the requested refunds. It thus seems evident that the banks should (a) offer better protection that prevents such scams from happening in the first place, and (b) reverse the transactions and/ refund their customers when fraudulent payments do occur."

CHANGES TO US LAW THAT COULD IMPACT BANKS' OBLIGATIONS

US senators are currently working on regulatory changes designed to reduce payments fraud. A proposed update to the EFTA – which would make banks liable for refunding authorised payments as well as non-authorised – would mean banks could no longer claim zero liability for these types of scams.

REGULATION E

Extending Regulation E would address the current loophole EWS is benefitting from – i.e. that a payment authorised by the customer is not technically an unauthorised payment, even if it was the result of a scam.

From a consumer point of view, this amendment would be good news, but critics argue it won't prevent scams from happening and will cost banks money that could be spent on better fraud protection systems. Another argument against tightening regulations in this area is that it impacts the customer onboarding process, making it less streamlined and creating a deterrent for new customers.

A number of smaller banks have expressed their concerns over the proposals to amend Regulation E. Industry groups representing US community banks and credit unions, who say they would be harder hit by the requirement to reimburse all fraudulent payments, claim they may be forced to abandon their partnerships with platforms such as Zelle. "When utilising Zelle and other [peer-to-peer] applications, community banks have little room or ability to customise the applications, including fraud warnings and alerts to end users," said Rebecca Kruse, chief operating officer of Independent Community Bankers of America.

"Shifting liability for payments the customer has authorised and later claims were made to a scammer will harm consumers in the form of higher costs, fewer options, and less competition," the American Bankers Association (ABA) wrote in a letter to CFPB Director Rohit Chopra in October this year.

In the letter, the ABA claims that the share of disputed transactions made using PayPal is three times higher than Zelle and six times higher for Cash App (a similar platform). "While the banking industry has made substantial investments in fraud prevention and has had success in educating consumers, banks cannot stop all scams," it says. "Indeed, consumers are in the best position to know the reasons they are sending money, the circumstances of the payment, and who the recipient is. Banks, in contrast, typically have no knowledge about the relationship between the sender and the recipient, the reasons the consumer is sending money, or the context of the payment."

The letter goes on to discuss the potential negative implications if Regulation E amendments are implemented: "If banks must reimburse customers for P2P payments that a customer later claims were made to a scammer, banks will have to adjust their business models to reflect those risks and potential losses – over which they have little control – as well as the costs of claims investigation and compliance. While responses will vary, banks will have to consider whether: to charge for P2P transactions, which currently are usually free; to limit access to P2P services; to reduce the frequency and amounts of P2P payments; and/or to close accounts."

According to the *Wall Street Journal*, JPMorgan Chase, Bank of America and Wells Fargo are currently in discussions to create a standardised refund procedure for Zelle scam victims.

About Risk Universe

Risk Universe by RiskBusiness provides in-depth analysis, reviews and research on areas of interest within the broader governance, risk, audit and compliance landscape, designed to provide proactive, 360° intelligence for informed decision making across the enterprise.

About RiskBusiness

RiskBusiness is an international governance, risk, audit and compliance (GRAC) solution provider, delivering risk content, risk intelligence, risk tools and risk advisory services to its clients. It is an association of like-minded industry professionals, who have the aim of furthering the risk management discipline to enable better risk-reward decision making.

Risk management is an evolving discipline, which has developed in close partnership with the industry. RiskBusiness has, both as individuals and collectively, a depth of established relationships with leading players and regulators in the operational risk field. We are also active participants in industry working groups and contribute thought leadership through publications and education.

RiskBusiness was founded in 2003 and today has principal locations in Birmingham, London, Buenos Aries, Amsterdam, Hong Kong, New York, Singapore, Toronto, and Zurich. To learn more, visit **www.riskbusiness.com**

Contacts

Carrie Cook, Editor:
carrie.cook@riskbusiness.com

General enquiries:
info@riskbusiness.com

Risk Universe
by RiskBusiness

www.riskbusiness.com