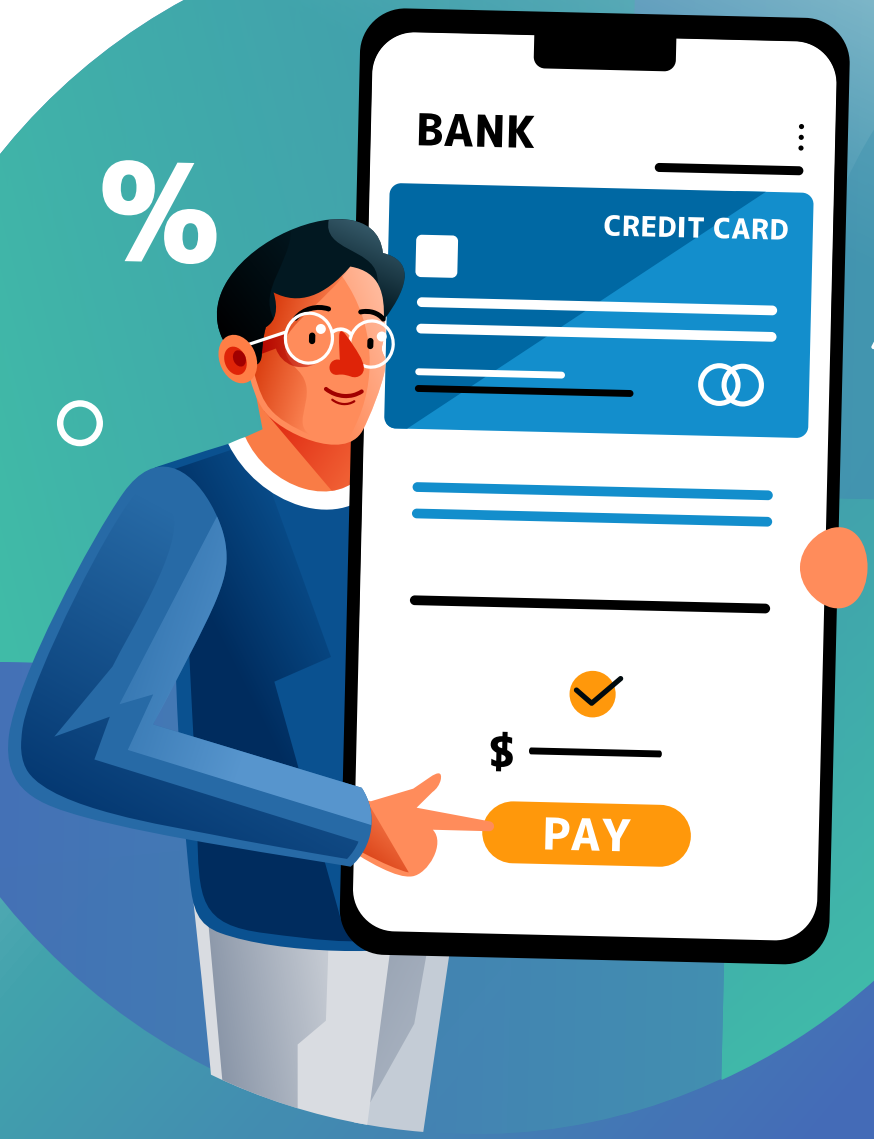
TOOLCASE



Zelle and P2P Fraud

And Its Effects on Financial Institutions

by TOOL**CASE**

Table of Contents

Zelle and P2P Fraud and Its Effects on Financial Institutions 1

Introduction 1

Zelle and P2P Fraud 2

Zelle and P2P Fraud Is Escalating Out of Control 3

Zelle Fraud and Scam Claims 4

Zelle and P2P Fraud: How They Work 5

The Initiation of Zelle Scams 5

The Process of Zelle Scam 5

Zelle Scammers and Fraudsters 6

Effects of Zelle and P2P Fraud on Financial Institutions 7

Implications for Bank-Customer Relationships 7

The Greatest Downside of Zelle and P2P Frauds 8

Zelle and P2P Fraud Solution 9

AI-based Anti-fraud Detection 10

Real-time Fraud Detection 12

ToolCASE: Provider of a Comprehensive Suite of AI-Based Solutions and Services 12

RembrandtAi Fraud Detection 13

Adaptive to Change 13

Request a Demo 15

INTRODUCTION

In today's modern world, where technology is swiftly improving to help people's lives to be better and more comfortable, credit cards and digital payment apps offer particular advantages over cash; they can connect businesses with banks, employees, suppliers, and new industries for their products and services simply and cost-effectively. Digital payments can boost an entrepreneur's profits by making financial transactions with consumers, suppliers, and the government easier, safer, and less expensive.

More importantly, credit cards and digital payment apps provide transparency and security by improving traceability and accountability, which reduces corruption, theft, and scams. However, while technology advances to help prevent digital fraud, scammers and fraudsters get more creative and improve their strategies; often faster than the fraud technology that's designed to catch them. Recently, we have seen a rise in Zelle and peer-to-peer (P2P) fraud.

ZELLE AND P2P FRAUD is a rising threat in today's digital world. Zelle is a huge payment platform that has millions of users. However, Zelle, a peer-to-peer digital payment network owned by seven major banks, seems less concerned about its users' safety and security than other payment platforms, making it a primary target for digital and P2P fraud.

Evermore common, a fraudster pretends to be from your bank or credit union and will try to persuade you to send money via Zelle, seizing your Zelle account or having money transferred to theirs. Unfortunately, according to the Los Angeles Times, if you use Zelle to pay someone who turns out to be a fraudster, your chances of retrieving the money from your bank are almost zero. The same is true if you transfer money to an incorrect recipient. Once you click "Send", the money is gone. Some critics believe Zelle and its banking partners are misinterpreting the Electronic Fund Transfer Act of 1978 and its implemented regulations, which protect consumers from much of the risk of "unauthorized" transactions. An unlawful transfer typically occurs when someone else initiates a transfer from your account without your permission.

ZELLE AND P2P FRAUD IS ESCALATING OUT OF CONTROL

A recent official report from Senator Elizabeth Warren's office has highlighted what many in the banking industry are already struggling with: Zelle fraud is increasing at an alarming rate, and unless proactive, cost-effective measures are implemented soon, it may become out of control. Senator Warren launched an investigation in April 2022 to determine the extent of fraudulent activity on Zelle, as well as to understand if and how Zelle, and the banks that own and operate it, makes consumers whole when they are defrauded on the platform.

Senators Warren, Menendez, and Reed wrote to Early Warning Services (EWS), seeking data on the number of scams and fraud, as well as the service's policies for redressing consumers who have been defrauded.

Warren's report says,

"The information provided by EWS revealed that an estimated $440 million was lost by Zelle users through frauds and scams in 2021..."

but that the banks that participate in the network appear not to have provided sufficient recourse to their customers. In particular, EWS's response indicated that Zelle facilitates fraudulent activity of many kinds. This includes activity in which a user's account is accessed by a bad actor and used to transfer a payment, an "unauthorized" transfer; as well as "authorized transactions," where users were duped by a scam, although they technically authorized payment.

SCAM AND FRAUD CLAIMS FROM ZELLE USERS ARE EXPECTED TO RISE 183% at banks examined by Senator Warren's office, from more than $90 million in 2020 to more than $255 million in 2022. Keep in mind, this growth in fraud is only reported at a very small number of institutions and is not an industrywide total. According to statistics provided to the Senate by only three institutions that fully participated,

- **PNC Bank had 8,848 occurrences of Zelle fraud in 2020 but is likely to have over 12,300 cases this year, marking a 39% rise over the two years.**
- **In 2020, US Bank had 14,886 cases, compared to 27,702 cases the previous year, representing an 86% rise. In addition,**
- **Truist Financial reported 9,455 Zelle fraud instances in 2020 and 22,045 in 2021.**

Another four banks also took part and gave Senator Warren pertinent data, indicating that the value of scam and fraud claims received in 2020 was more than $90 million, which increased by more than 250% to over $236 million in 2021 and is on track to exceed $255 million in 2022. In other words, the trend shows a phenomenal 133% growth in fraud cases a year.

ZELLE AND P2P FRAUD: HOW THEY WORK

Scams are growing increasingly common as digital payment systems become more accessible, fast, and convenient to send money. Fraudsters' scam tactics are growing more sophisticated to dupe victims into handing over their money, especially since P2P transactions are immediate and often difficult to reverse. Here is how the latest Zelle and P2P fraud works.

ⓘ THE INITIATION OF A ZELLE SCAM

Scammers and fraudsters have ways of getting a consumer's phone number; often from stolen PII found on the dark web. Once obtained, fraudsters will then act as a member of a credit union or a bank institution and send a message to the consumer asking if they had attempted to transfer a large amount of money through Zelle. The text message requires consumers to answer "Yes" or "No." If the consumer replies "No," the fraudster will call the consumer using a spoofed phone number (identical to the institution) claiming to be a representative of the fraud department to help them retrieve the stolen money.

ⓘ THE PROCESS OF A ZELLE SCAM

When a consumer answers the call, the fraudster has the opportunity to scam them. In the call, the fraudster will tell the consumer that there is a Zelle transfer transaction under their account, but since they said they did not attempt the Zelle transfer, the fraudster will assure the consumer that the stolen money is recoverable. The fraudster instructs the consumer that to recover the so-called transferred money, the consumer must use Zelle to send the money back to themselves using their phone number — claiming it is a standard process in retrieving the stolen money.

Then, the fraudster will link the consumer's mobile phone number to the fraudster's Zelle account. During the linking of the phone number, Zelle will send a two-factor authentication passcode to confirm the mobile phone number. The passcode is sent to the consumer's mobile phone. However, the fraudster tricks the victim into providing the passcode over the phone, again claiming it to be the standard process. When the fraudster obtains the passcode, they enter the passcode to activate the mobile number on their Zelle account, and the Zelle transfer goes to the fraudster's account.

ZELLE SCAMMERS AND FRAUDSTERS

Scammers and fraudsters approach their victims in numerous ways. Credit unions and banking institutions stated that fraudsters successfully acted as call center representatives and changed cell phone numbers on consumers' accounts, allowing the fraudsters to obtain the passcodes. In certain circumstances, fraudsters compromised consumers' email accounts to intercept passcodes supplied via email.

It may be difficult for some people to think that the whole process is a scam because fraudsters are also effective at acting as reliable and helpful representatives from a credit union or a bank institution.

When the customer realizes it was a scam, it's too late. At this point they won't hear anything from the so-called credit union representative, and when they check their bank account, the exact amount of money that they tried to send (recover) to themselves is gone.

EFFECTS OF ZELLE AND P2P FRAUD ON FINANCIAL INSTITUTIONS

The Zelle and P2P problem is escalating. However, it is not just these huge financial institutions that took part in Senator Warren's investigation and their clients that have fallen victim to Zelle fraud. Every institution, regardless of size, has experienced an upsurge in P2P fraud reports. Zelle is currently available at over 1,700 banks and credit unions of all sizes. Meaning every one of them, their customers, and members, are susceptible.

However, as the service grows in popularity among consumers, even more financial institutions are likely to adopt the technology, which has also grown in popularity among scammers, fraudsters, and criminals, making the potential for financial losses massive.

IMPLICATIONS FOR RELATIONSHIPS BETWEEN INSTITUTIONS AND THEIR CLIENTS/MEMBERS

With millions of users on Zelle, the possibility of fraud is increasing. Not only do Zelle and P2P frauds harm consumers, but they also harm banks and financial institutions; both monetarily from confirmed “unauthorized” fraud reimbursements, and reputation. Being a victim of fraud affects customer/member perceptions of feeling secure and protected at their institutions.

Fraud may harm the bank-customer relationship by destroying trust and confidence, as well as increasing discontent due to a perceived service failure or lack of care. As a result, client loyalty may suffer, and shifting behavior may increase, harming the banks' image and reputation, and restricting the acquisition and retention of new customers or members.

THE GREATEST DOWNSIDE OF ZELLE AND P2P FRAUDS

According to Senator Warren's report, numerous banks are refusing to reimburse consumers who dispute "authorized" Zelle payments. Banks refund only 10% of Zelle and P2P scam claims, mostly the ones they can confirm as “unauthorized.” With Zelle, banks have taken a stance on fraud and scam claims. They normally do not reimburse consumers who are duped into making Zelle payments, but they do claim to reimburse consumers who incur unlawful, non-authorized transfers on Zelle.

According to JPMorgan Chase, "we reimburse customers for unauthorized transactions reported in a timely manner." Similarly, Wells Fargo stated, "We organize our customer fraud processes in compliance with Regulation E, which provides consumer liability protections and error resolution requirements for electronic fund transfers... In addition to the protections provided by Regulation E, Zelle customers are not liable for any portion of an unauthorized transaction reported in a timely manner."

However, those banks that do not refund “authorized” Zelle scam payments may be in violation of federal law and CFPB rules, according to Senator Warren. As a result, Zelle fraud costs and reimbursements may have a growing and significant impact on every institution participating in the network, regardless of size. This may be especially true if new laws are enacted to protect consumers against “authorized” P2P frauds.

Right now, all financial institutions must cooperate in Zelle fraud claims and reimburse if the fraud is proven. Financial institutions incur significant operational costs when they reimburse consumers' monetary losses. Should they be responsible for “authorized” payments fraud, these costs could skyrocket.

ZELLE AND P2P FRAUD SOLUTION

Seeing as scammers and fraudsters have excellent methods of scamming people using digital payments like Zelle, the ultimate solution is to have advanced fraud security — an AI-based anti-fraud detection and prevention solution that operates in real-time, as Zelle does.

As an institution, you should not rely on digital payment platforms themselves to improve their security and safety features to prevent fraud and scams. Although it is their responsibility to keep their users safe from scams and fraud, it is best to take the initiative because being a victim of fraud and scams will have a significant impact on your business and the relationships with your customers or members.

AI-BASED ANTI-FRAUD DETECTION

Every financial institution has at least the minimum required fraud detection practices in place, which refers to the process of identifying fraudulent actions and scams. Most fraud detection methods utilize specialized fraud and risk teams to manually identify possible fraudulent activities from their customers and users via the analysis of Core banking data and batch data. However, the technology and creativity of scammers is evolving, making traditional fraud detection methods and systems particularly useless. Fortunately, as technology progresses, it also now provides financial institutions with a solution to boost fraud detection. Real-time, AI-powered tools are now an important part of fraud detection and prevention procedures, supplementing or in some cases, even replacing manual detection. The complexity and sophistication of fraud schemes are increasing, but the development of machine learning and Ai techniques goes hand in hand, providing institutions and their members with the ability to prevent fraud and defend themselves from scams, in real time, while staying ahead of fraud trends and tech.

A real-time, AI-based anti-fraud detection and prevention system can automate the process while providing accuracy and consistency. Manually detecting fraudulent activity is extremely difficult, regardless of how well-trained and hardworking fraud teams are. Further, since many risk and fraud teams analyze for fraud in batch data, frauds that have been found have already occurred, and the money already gone.

Real-time operating and reporting fraud detection and prevention systems, powered by artificial intelligence is changing this, and have become fraud teams' strongest weapon yet in the fight against fraud.

Even for real-time Zelle and other P2P frauds.

HOW DOES AI-BASED ANTI-FRAUD DETECTION AND PREVENTION WORK?

AI-based anti-fraud detection solutions are a system that a financial institution's fraud and risk teams use to detect fraud automatically, in real-time streaming data. The AI technology of the system combines supervised learning algorithms with unsupervised learning to provide faster evaluation of transactions for possible fraud. With the help of AI technology, financial institutions can better identify and prevent unauthorized activity.

DETECTING ZELLE FRAUD:

There are two main Zelle fraud types that can be identified by real-time AI, before the Zelle is originated.

The first fraud type is when a Zelle payment is sent out after a check has been deposited. These are often RDC checks and may include a scam check. By monitoring these deposits, funds can be held before a Zelle request can be completed.

The second is an account takeover that leads to a Zelle payment. By monitoring non-financial activity such as OLB password changes, address, and email changes the takeover can be identified before a Zelle is requested.

Lastly, Zelle transactions can be monitored for early detection of any other suspicious transactions.

REAL-TIME FRAUD DETECTION

AI-based anti-fraud detection is designed to capture, examine, and identify specific transactional events as they occur. When it detects a possible fraudulent transaction, the AI can be configured to send out immediate alerts, notifying the institution of potential fraud, in real-time.

AI is more than capable of analyzing transactions, to accurately detect fraud, in real time.

TOOLCASE:

PROVIDER OF A COMPREHENSIVE REAL-TIME SUITE OF AI-BASED SOLUTIONS AND SERVICES

ToolCASE LLC has specialized in customized, enterprise-level artificial intelligence and machine learning solutions for more than two decades. Our expertise in deep learning, Ai and remote Oracle Database Administration, Linux/Unix System Administration, and System Storage Administration ranks us as a global leader in business automation, fraud detection, and data interpretation solutions. With our flagship RembrandAi, we provide best-in-class analytics, visualization, and insight to detect and prevent digital transactional fraud and solve complex enterprise challenges. And RembrandtAi does this in real-time.

RembrandtAi *FRAUD DETECTION*

RembrandtAi is an advanced transaction analytics, real-time multi-level AI system that uses analyst and machine learning artificial intelligence. RembrandtAi's expansive, comprehensive API supports effectively limitless data sources, allowing you unprecedented real-time fraud detection and prevention. RembrandtAi also includes extensive data visualization and informative alerting to help fraud and risk teams do their jobs more efficiently, and make informed, accurate decisions.

With RembrandtAi, your fraud detection, cyber security, bank security, P2P and all transactional fraud detection and prevention processes will be easier and more effective at detecting fraud in real-time, than ever before.

ADAPTIVE TO CHANGE

Our world is changing at a fast pace, and nothing can stop it. However, fraudsters and other economic criminals are also evolving and incorporating new strategies into their criminal activities, particularly in P2P fraud. If you want to protect your institution and its members or customers, having a system that can quickly adapt and change with the world and the ever-changing criminal activities of fraudsters should be your top priority.

REMBRANDTAI CAN OUTPERFORM TRADITIONAL, LEGACY AND NON-REAL-TIME FRAUD DETECTION SYSTEMS, AND WORKS AROUND THE CLOCK IN REAL-TIME.

Our AI-based, real-time fraud detection and prevention system utilizes top-of-the-line, customized and adaptive analytics, a type of predictive analytics that collects and analyzes real-time data rather than historical data. While fraudsters are constantly inventing new ways to fool systems, RembrandtAi prioritizes detecting new fraud techniques by analyzing and studying current trends and predicting where new frauds may occur in the future.

It is designed to detect new activities within an organization quickly and accurately, and continually "learns" to get even better. As a result, the adaptive analytics of RembrandtAi can be a powerful tool against modern Zelle fraudsters, and potentially against frauds that have yet to arise. While fraudsters' habits and techniques evolve, AI-based technology in fraud detection and prevention systems evolve and adapt faster than the fraudsters, to counter any new strategies and scams they may have.

REQUEST A DEMONSTRATION OF THE TRULY REMARKABLE REMBRANDTAI

ToolCASE's solutions serve a wide range of industries, including financial services, business services, airlines, oil and gas, retail and online stores, health and medical, government, manufacturing, insurance, and transportation.

If you are a Risk Officer, Fraud Officer, B2B Chief Technology Officer, President, CEO, Data Analyst, Chief Information Security Officer, manager, or director, RembrandtAi is the ultimate solution for your financial institution's fraud detection needs.

RembrandtAi is a set of machine-learning algorithms capable of analyzing a near unlimited number of transactions per second. Its neural networks extend this capability by making decisions in real time. RembrandtAi is highly effective at reducing the overwhelming number of flagged transactions and providing a concise list of those that require further investigation by a human counterpart...

And can be fully automated.

Take a massive step towards greater success and request a demo today to learn more about how ToolCASE's RembrandtAi can take your fraud detection system to the highest level possible.