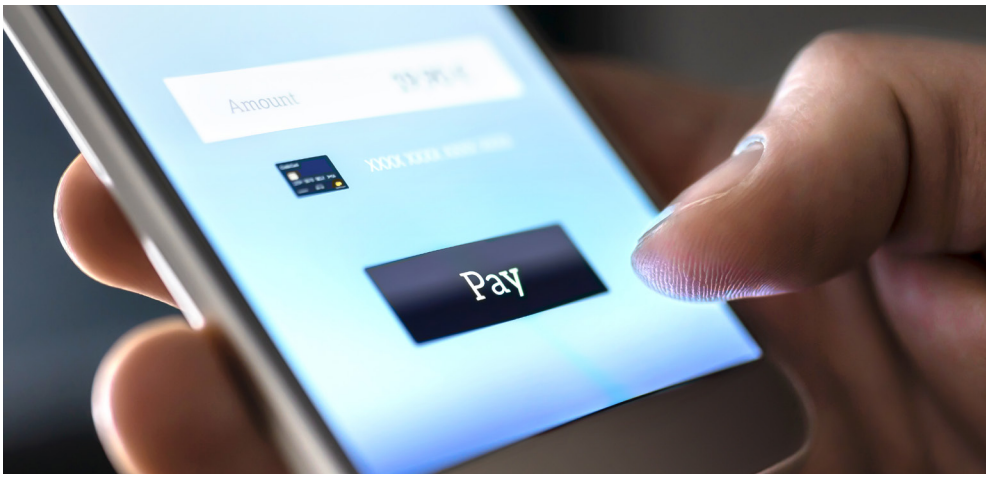
Treliant®

From THE PULSE

SUMMER 2024

The Underestimated Threat: Zelle Fraud's Impact on Regional Banks in the United States

By Daniel Lane and Justin Duquella



In recent years, the landscape of financial transactions has undergone a significant transformation with the rise of digital payment platforms. Among these platforms, Zelle has emerged as a top player, offering users a convenient and seamless way to send and receive money directly from their bank accounts. As of 2023, Zelle processed over $806 billion in transactions, reflecting a 28% increase from the previous year.[1] However, alongside the benefits of convenience and accessibility, Zelle also presents a significant challenge in the form of fraud, particularly for regional banks in the United States. This is discussed in greater detail below. Despite the platform's widespread adoption, Zelle fraud remains a pressing concern, posing substantial risks to financial institutions and their customers.

[1] Zelle. (2024). *Zelle Soars With $806 Billion Transaction Volume, Up 28% From Prior Year*

(continued on next page)

Launched in 2017, Zelle quickly gained popularity as a peer-to-peer payment platform backed by major banks. Its integration with banking apps and instantaneous fund transfers made it a preferred choice for millions of users seeking quick and hassle-free money transactions. By 2023, Zelle had over 2,100 participating financial institutions, representing nearly 80% of all U.S. bank accounts, and facilitated more than 2.9 billion individual transactions.[2] However, the speed and convenience that Zelle offers also make it an attractive target for fraudsters and cybercriminals looking to exploit vulnerabilities in the system.

The prevalence of Zelle fraud has raised significant concerns among regional banks, which may lack the resources and infrastructure of larger financial institutions to effectively combat this evolving threat. According to a 2023 report by the Federal Trade Commission (FTC), complaints related to Zelle scams have surged by 86% year-over-year, highlighting the increasing sophistication of fraud tactics.[3] Unlike big banks with dedicated cybersecurity teams and sophisticated fraud detection systems, regional banks often struggle to keep pace with the rapidly evolving tactics employed by fraudsters. As a result, they face an increased risk of monetary loss, reputational damage, and loss of customer trust in the event of a security breach or fraudulent activity on the Zelle platform.

Regional banks face an increased risk of monetary loss, reputational damage, and loss of customer trust.

The Evolution of Digital Payment Platforms

Before delving deeper into the impact of Zelle fraud on regional banks, it's helpful to understand the broader context of digital payment platforms and their evolution over the years. The advent of the internet and mobile technology has revolutionized the way people conduct financial transactions, enabling them to send and receive money with unprecedented speed and convenience. Traditional payment methods, such as cash and checks, have gradually been supplanted by digital alternatives, offering users greater flexibility and accessibility.

Among the myriad digital payment platforms available today, Zelle has emerged as a leading player in the peer-to-peer (P2P) payments space. Launched in 2017, Zelle was developed as a collaborative effort among several major banks, with the aim of providing users with a seamless and secure way to transfer money directly from their bank accounts. Unlike third-party payment apps like Venmo or PayPal, which require users to maintain a separate account balance, Zelle operates within the existing infrastructure of participating banks, allowing users to send and receive funds directly from their checking or savings accounts. Zelle's real-time transfer feature sets it apart from other P2P payment platforms, allowing users to send and receive funds instantaneously, even outside of regular banking hours.

[2] Zelle. (2024). *Zelle Soars With $806 Billion Transaction Volume, Up 28% From Prior Year.*.
[3] Federal Trade Commission (FTC). (2023). *FTC Reports Increase in Complaints Related to Zelle Scams.*

(continued on next page)

Zelle fraud encompasses a variety of tactics and schemes employed by cybercriminals to exploit vulnerabilities in the platform and defraud unsuspecting users.

However, the same features that make Zelle so convenient for users also make it an attractive target for fraudsters looking to exploit vulnerabilities in the system. Unlike traditional payment methods, such as checks or wire transfers, transactions made through Zelle are instantaneous, meaning that once a transfer is initiated, it cannot be undone. While this feature enhances the speed and efficiency of money transfers, it also leaves users vulnerable to fraud, since there is limited recourse for recovering funds in the event of unauthorized or fraudulent transactions. Zelle member banks have begun to process refunds on a claim-by-claim basis.[4]

Types of Zelle Fraud

Zelle fraud can take many forms, ranging from simple phishing scams to sophisticated account takeover schemes. The list below outlines some of the more common methods fraudsters employ while using Zelle.

- **Phishing Schemes:** Phishing remains one of the most common tactics employed by fraudsters to exploit banking customers. In these schemes, perpetrators impersonate legitimate entities, such as banks or government agencies, through deceptive emails, text messages, or phone calls. These communications typically contain urgent messages prompting users to provide sensitive information, such as account credentials or personal details. Once obtained, fraudsters use this information to access victims' bank accounts and initiate unauthorized Zelle transfers.

- **Account Takeover:** Account takeover represents another prevalent form of Zelle fraud, wherein cybercriminals gain unauthorized access to a user's bank account through various means, such as malware or social engineering. Once inside the user's bank account, fraudsters may change account settings, including email addresses or phone numbers associated with the account, to prevent users from receiving notifications of suspicious activity. Subsequently, they exploit Zelle's instant transfer feature to quickly move funds out of the compromised account to their own, making it challenging for banks to trace and recover the stolen funds.

- **Social Engineering:** Social engineering tactics involve manipulating individuals into divulging confidential information or performing actions that compromise their security. In the context of Zelle fraud, social engineering techniques may include impersonating friends or family members and requesting money transfers under false pretenses. For example, a fraudster might pose as a relative in distress, claiming they

[4] Zelle Begins Refunding Impostor Scam Victims — How To Get Your Money Back If Scammed.

(continued on next page)

need urgent financial assistance and requesting funds to be sent via Zelle. Unwitting victims may fall prey to these emotional appeals and transfer money without verifying the identity of the requester, resulting in monetary loss.

In summary, Zelle fraud encompasses a variety of tactics and schemes employed by cybercriminals to exploit vulnerabilities in the platform and defraud unsuspecting users. From phishing and account takeover to fake seller/buyer scams and social engineering, these fraudulent activities pose significant challenges to both users and financial institutions, highlighting the need for robust security measures and vigilant risk management strategies.

Challenges Faced by Banks

Regional banks in the United States are increasingly grappling with a range of challenges posed by the rise in Zelle fraud. One significant issue is the increased workload for their fraud departments. As fraud attempts via Zelle become more prevalent and sophisticated, these banks must allocate additional resources to detect, investigate, and mitigate fraudulent activities. According to a 2023 report by the Federal Reserve, financial institutions reported a 30% increase in Zelle-related fraud cases compared to the previous year.[5] This often means hiring more staff, investing in specialized training, and deploying advanced fraud detection technologies. Such measures, while necessary, can strain the limited budgets of regional banks, diverting funds and staff attention from other crucial areas of operation.

As fraud attempts via Zelle become more prevalent and sophisticated, banks must allocate additional resources to detect, investigate, and mitigate fraudulent activities.

Another critical challenge is maintaining customer service and trust. Incidents of Zelle fraud can erode customer confidence in the bank's ability to protect their assets. For regional banks, which often rely on close relationships with their customers and a reputation for personalized service, this loss of trust can be particularly damaging. Addressing fraud-related issues requires not only efficient case resolution but also clear and compassionate communication with affected customers. A survey conducted by Javelin Strategy & Research in 2022 found that 15% of consumers reported switching banks after experiencing fraud, underscoring the potential impact on customer retention.[6]

Compliance with financial regulations adds another layer of complexity. As regulatory bodies update guidelines to address emerging threats, regional banks must continuously adapt to remain compliant. This includes implementing robust security protocols, maintaining accurate records, and staying abreast of regulatory changes. For regional banks, the costs associated with compliance can be substantial, in terms of time, money, and headcount. A study by the American Bankers Association indicated that regulatory compliance costs for regional banks can amount to up to 10% of

[5] Federal Reserve. (2023). *Annual Report on Financial Fraud and Cybersecurity.*
[6] Javelin Strategy & Research. (2022). *Consumer Fraud Survey.*

(continued on next page)

their non-interest expenses.[7] While those costs clearly include much more than just Zelle fraud-fighting capabilities, the need to balance regulatory requirements with operational efficiency and customer service excellence presents an ongoing challenge.

Lastly, regional banks must navigate the technological and security landscape to stay ahead of fraudsters. Implementing cutting-edge security measures, such as multifactor authentication and real-time transaction monitoring, is crucial but often comes with prohibitive costs and technical challenges. Regional banks must also keep pace with innovations in fraud prevention, ensuring that their systems are resilient against increasingly sophisticated attacks. The rapid evolution of fraud tactics means that staying one step ahead is a continuous battle, requiring ongoing investment and strategic planning. According to a report by Aite-Novarica Group, financial institutions are expected to increase their spending on fraud detection and prevention technologies by 15% annually through 2025.[8]

By leveraging new technologies, banks can analyze vast amounts of transaction data, identify patterns indicative of fraudulent activity, and intervene swiftly to stop fraudulent transfers.

Mitigation Strategies

Mitigating the impact of Zelle fraud requires a comprehensive approach that combines technological solutions, customer education, and collaboration with industry stakeholders. Regional banks must proactively invest in advanced fraud detection systems and employ innovative technologies, such as artificial intelligence and machine learning (AI/ML) algorithms, to enhance their ability to detect and prevent fraudulent transactions in real-time. By leveraging these technologies, banks can analyze vast amounts of transaction data, identify patterns indicative of fraudulent activity, and intervene swiftly to stop fraudulent transfers before they occur. If fraudulent activity can be detected and thwarted before a loss is incurred, the customer base will be more likely to continue banking with their institutions and the bank will be able to protect both their assets and reputation.

Additionally, addressing headcount and staffing issues is crucial for maintaining operational efficiency and customer trust. Banks should utilize predictive analytics for workforce planning to ensure they have the right staff in place during peak periods and to quickly adjust staffing levels based on demand. Cross-training employees can provide operational flexibility, while investment in AI-driven recruitment platforms can streamline the hiring process and improve candidate matching. To retain talent, banks should foster a positive work environment through regular feedback, recognition programs, and career development opportunities.

Navigating the regulatory environment is another critical aspect. Banks should establish dedicated compliance teams to stay updated on regulatory changes and ensure all legal requirements are met. Regular compliance training for employees

[7] American Bankers Association. (2022). *Cost of Compliance for Regional Banks.*
[8] Aite-Novarica Group. (2023). *Trends in Fraud Detection and Prevention Technologies.*

(continued on next page)

and frequent audits will help identify and rectify compliance gaps. Utilizing regulatory technology (regtech) solutions can automate compliance processes, making it easier to manage compliance requirements.

Furthermore, banks should prioritize customer education and awareness initiatives to empower users to recognize and avoid common scams and security threats associated with Zelle. Providing clear guidance on security best practices, such as safeguarding account credentials, enabling multifactor authentication, and avoiding sharing sensitive information online, can help users protect themselves from falling victim to fraudulent schemes. Banks can disseminate educational materials through various channels, including online banking portals, mobile apps, and email newsletters, to reach a wide audience and ensure that users are equipped with the knowledge and tools they need to safeguard their financial assets.

Additionally, collaboration among banks, regulatory agencies, and law enforcement is essential to combatting Zelle fraud effectively. By sharing information about emerging threats and fraudulent schemes, banks can stay ahead of cybercriminals and coordinate their efforts to investigate and prosecute offenders. Moreover, collaboration with Zelle's parent company and other industry stakeholders is crucial to developing and implementing standardized security protocols and best practices that enhance the overall security posture of the Zelle platform.

Financial regulatory bodies are likely to introduce stricter guidelines and compliance requirements to protect consumers and ensure the integrity of digital payment systems.

Future Outlook of Zelle Fraud and Related Impacts

The future outlook of Zelle fraud presents both challenges and opportunities for regional banks in the United States. As digital payment platforms like Zelle continue to grow in popularity, fraudsters are likely to develop more sophisticated techniques to exploit vulnerabilities. This evolving threat landscape will require banks to stay vigilant and proactive in their security measures. According to a recent study by Juniper Research, the total value of digital payment fraud losses globally is expected to exceed $200 billion between 2024 and 2028, with peer-to-peer payment platforms like Zelle being significant contributors to these losses.[9]

One of the critical areas of focus for regional banks will be the enhancement of their fraud detection and prevention technologies. The adoption of advanced technologies such as AI/ML is expected to play a crucial role in identifying and mitigating fraud attempts in real-time. AI/ML can analyze vast amounts of transaction data to detect unusual patterns and flag potentially fraudulent activities with greater accuracy and speed. A report by Gartner forecasts that by 2026, over 60% of financial institutions will have integrated AI/ML into their fraud detection systems, significantly reducing the incidence of successful fraud attempts.[10]

[9] Juniper Research. (2023). *Global Digital Payment Fraud Report.*
[10] Gartner. (2023). *The Future of AI and Machine Learning in Financial Services.*

(continued on next page)

Banks should develop a targeted action plan that addresses identified weaknesses, optimizes existing processes, and sets the foundation for a robust fraud prevention framework.

In addition to technological advancements, regulatory developments will shape the future landscape of Zelle fraud. Financial regulatory bodies are likely to introduce stricter guidelines and compliance requirements to protect consumers and ensure the integrity of digital payment systems. Regional banks will need to stay updated with these regulatory changes and invest in compliance infrastructure to avoid legal repercussions and maintain customer trust. The increased regulatory scrutiny may also lead to more robust industry standards and best practices for fraud prevention, further enhancing the security of digital payment platforms.

Industry trends indicate a growing emphasis on collaboration within the banking sector and with external stakeholders to combat fraud. Regional banks can benefit from sharing information and resources through industry consortiums and partnerships, such as the Financial Services Information Sharing and Analysis Center (FS-ISAC), Financial Action Task Force (FATF), and Bankers Association for Finance and Trade (BAFT). By collaborating with larger banks, fintech companies, and cybersecurity firms, regional banks can access cutting-edge technologies and abilities that might otherwise be out of reach. This collective effort can help create a more secure digital payment ecosystem and reduce the overall incidence of fraud.

Next Steps

To mitigate the impact of Zelle fraud, as indicated above, banks should adopt a multifaceted approach that combines:

- Technology solutions
- Customer education
- Collaboration with industry stakeholders

To ensure their fraud program is robust and efficient, banks should begin with a comprehensive independent initial program assessment. This assessment will evaluate the current state of fraud detection and prevention measures, identify gaps, and prioritize areas for improvement. Conducting an initial program assessment is crucial, since it provides a clear baseline of the bank's existing capabilities and vulnerabilities. This step enables the bank to tailor its strategies to its specific needs and ensure that resources are allocated effectively.

The assessment should include a thorough review of the bank's current fraud detection technologies, such as the efficacy of AI/ML-based systems in identifying suspicious activities. Additionally, it should evaluate the adequacy of staffing levels and training programs, ensuring that employees are well-equipped to recognize and respond to fraud attempts. The assessment must also scrutinize the bank's compliance with regulatory requirements and the effectiveness of its RegTech solutions.

(continued on next page)

By conducting this initial program assessment, banks can develop a targeted action plan that addresses identified weaknesses, optimizes existing processes, and sets the foundation for a robust fraud prevention framework. This proactive approach not only enhances the bank's defenses against Zelle fraud but also demonstrates a commitment to maintaining customer trust and retention by prioritizing their security.

Conclusion

Zelle fraud poses a significant threat to regional banks in the United States, jeopardizing their financial stability, reputation, and most importantly, the trust of their customers. As the popularity of digital payment platforms continues to grow, so does the need for robust security measures and proactive risk management strategies. The rise of Zelle fraud underscores the importance of understanding the evolving threat landscape and implementing effective mitigation strategies to protect users and financial institutions alike.

The impact of Zelle fraud is particularly pronounced for regional banks, which may lack the resources and expertise of larger financial institutions to combat this evolving threat effectively. Beyond the direct financial costs of reimbursing affected customers and investigating fraudulent transactions, banks also face reputational damage and loss of customer trust. In an increasingly competitive banking landscape, characterized by shifting consumer preferences and growing reliance on digital banking services, maintaining customer trust and confidence is paramount to long-term success.

Investing in advanced fraud detection systems and AI/ML algorithms can help banks identify suspicious transactions in real-time and prevent fraudulent transfers before they occur. Moreover, prioritizing customer education and awareness initiatives can empower users to recognize and avoid common scams, thereby reducing their susceptibility to fraud.

In conclusion, Zelle fraud represents a complex and evolving challenge that requires a coordinated and proactive response from financial institutions, regulators, and law enforcement agencies. By leveraging technology, education, and collaboration, regional banks can mitigate the impact of Zelle fraud on their bank, protect their customers' financial assets, and uphold the integrity of the financial system. Ultimately, safeguarding the security and trust of users is paramount to ensuring the continued success and sustainability of digital payment platforms like Zelle in an increasingly interconnected and digitized world.

Zelle fraud represents a complex and evolving challenge that requires a coordinated response from financial institutions, regulators, and law enforcement agencies.

(continued on next page)

Daniel Lane

Dan Lane, a Director in Treliant's Global Financial Crimes Compliance practice, is an accomplished professional in corporate accounting, financial auditing, forensic accounting, regulator-directed monitorship, and financial crimes compliance. He has a history in financial crimes compliance stemming from his experience at global consulting and financial advisory firms and has conducted extensive financial and risk control audits for financial institutions, energy providers, and publicly traded companies. **DLane@treliant.com**

Justin Duquella

Justin Duquella is a Senior Manager with Treliant. With over 10 years' experience in the financial services industry, Justin has held fraud and Anti-Money Laundering (AML) compliance roles in both the banking and fintech sectors. He has extensive knowledge of fraud risk assessments, remediation action plans, suspicious activity report (SAR) writing, know your customer/know your business (KYC/KYB) obligations, account investigations, and other financial crimes compliance essentials. **JDuquella@treliant.com**

Treliant, an essential partner to financial services companies globally, brings to you *The Pulse*, a quarterly newsletter offering insights and information regarding pertinent issues affecting the industry. This article appeared in its entirety in the Summer 2024 issue. Other articles that appeared in this issue include:

- Resolution and Recovery Planning: New Requirements and the Importance of Credible Challenge
- Risk Data Aggregation and Risk Reporting: Where Did It All Go Wrong?
- New Repo Reporting Rule: Get Ready for NCCBR Data Collection

To subscribe to our quarterly newsletter, *The Pulse,* visit **Join Our Newsletter - Treliant.**

Treliant®