PROTECTING INSTANT PAYMENTS IN THE US:

P2P AND BEYOND

May 2019

Sponsored by:

NICE ACTIMIZE

Independently produced by:

JAVELIN

TABLE OF CONTENTS

TABLE OF FIGURES

FOREWORD

This original report, sponsored by NICE Actimize, examines the fraud threats facing instant payments and charts a path forward for organizations to learn about the challenges and best practices from previous faster payments initiatives in protecting customer accounts.

This research report was independently produced by Javelin Strategy & Research. Javelin Strategy & Research maintains complete independence in its data collection, findings, and analysis.

OVERVIEW

Across both consumer and commercial accounts, payments are accelerating, with customers pushing for funds to post, clear, and settle in minutes, if not faster. This shift offers an opportunity to strengthen relationships with customers, but also brings significant fraud challenges, as instant payments leave little time for organizations to detect and stop fraudulent activity. Early experiments with faster payments offer valuable lessons around the threats facing today's financial innovators and point to best practices that financial institutions and other payments providers can employ to most effectively protect customer accounts.

EXECUTIVE SUMMARY

Key Findings

Payments are getting faster, but not all "faster payments" are created equal. Faster payments come in three flavors: faster (such as same-day ACH), real-time (such as Zelle), and instant (such as TCH RTP), based on their times to post, clear, and settle.

The faster the payment, the more appealing it is to fraudsters. With shorter times between payment initiation and settlement, fraudsters have less risk that their activity will be detected and stopped before they receive the stolen funds. Quick, cheap, and flexible money movement also makes it easier to launder funds through multiple accounts, increasing the complexity of tracing stolen funds back to the perpetrator.

Zelle kicked off rapid P2P growth that shows no sign of stopping. With the launch of Zelle in 2017, the number of digital peer-to-peer (P2P) users leaped from 84 million to 110 million as waves of consumers had P2P payment capabilities integrated into the banking apps already installed on their phone. In 2018, another 15 million users adopted digital P2P payments. While future growth may not be so dramatic, Javelin forecasts that the number of P2P users will reach 173 million by 2023.

P2P schemes are irresistible for fraudsters, whether as a means of cashing out a compromised account or laundering funds to conceal their activities. In 2018, P2P fraud totaled $630 million, up from $549 million in 2017.

Consumers aren't the only ones benefiting from faster payments. Programs like The Clearing House's RTP network will bring instant payments to corporate transactions. The inherent speed and convenience of digital payment offerings built on top of RTP will undoubtedly inspire some of the same types of threats found in today's P2P applications. Disbursements will become higher-profile targets as criminals attempt to manipulate account information to redirect payments, which could include employee paychecks that today are routed via ACH or vendor payments. Or the fraudsters could simply initiate payments to accounts they have taken over with the promise of being able to gain access to those funds immediately.

Successfully rolling out faster payments requires getting fraud controls right from Day 1. Any new financial product is going to be rigorously tested by fraudsters, particularly if it has the potential to move funds. Misaligning fraud controls with risks exposes financial institutions (FIs) to significant jeopardy in the early stages of adoption of new products. For example, early fraud problems around the Zelle rollout were exacerbated by limited integration with pre-existing fraud analytics tools at the implementing banks, inadequate authentication and risk-assessment controls, and insufficient user education.

Recommendations

Hotlist suspicious accounts and attributes. Adding recipients of confirmed fraudulent transactions or scams forces criminals to come up with new names for every scheme. In addition to inconveniencing the perpetrator, it allows FIs to detect potentially fraudulent transactions before the funds leave their institution.

Utilize early account limits to control risk around "gray area" accounts. Until a customer establishes a record of legitimate transactions, early limits can help reduce the potential for fraud in new accounts. However, as overly restrictive limits can significantly impede legitimate users' ability to use the service, these are best applied to accounts flagged as potentially suspicious, such as those held by particularly new-to-bank customers or where there have been recent changes of contact information.

Automatically alert users to all transactions and account maintenance. Notifying customers of every P2P transaction initiated from their accounts as well as account maintenance, such as changes of contact information, engages them in protecting their accounts. It also sends a strong message regarding the degree of oversight in policing transactions for fraud. In the long term, FIs may run the risk of numbing customers to alerts. As the account ages, it may make sense to amend the alert thresholds.

Monitor for changes to contact information or authentication methods. One of the quickest ways to delay the detection of a fraud is to disassociate an account from its owner. Further, when it involves real-time payments, changing contact information is a leading indicator of a fraud in its infancy. Therefore, monitoring for and investigating contact changes, and blocking accounts where appropriate, provides FIs with the ability to detect and prevent real-time payment fraud.

Integrate with fraud analytics platforms. While the host of a payment platform may offer fraud-detection capabilities, it's necessary but not enough to prevent fraud. Similar to the integration of other streams of payment-related data, all payment data must integrate with the FI's fraud platform. Doing so provides additional layers of analysis and protection as well as the people, processes, and technology needed to investigate and make decisions about suspicious transactions, as well as to notify customers.

Analyze memo lines. Ironically, legitimate customers tend not to use the memo line to annotate the purpose of a transaction, whereas fraudsters often add an innocuous description to the memo line to add an air of legitimacy or to help manage the complexity of their own operations. Consequently, the existence of information in the memo line in and of itself can justify additional scrutiny of a transaction. Similarly, looking for patterns in memo lines can help identify groups of malicious users abusing the platform.

Collect threat intelligence to get ahead of emerging fraud schemes. Before an FI can address real-time payment fraud, it must possess a detailed understanding of the types of schemes it will face. By gathering and analyzing the components of a scheme, FIs can test their ability to detect and prevent new and emerging schemes before losses occur. Zelle's early challenges with scams

clearly show the risks of misaligning controls with threats. Since payments in scams are initiated by the legitimate user, unlike in cases of account takeover, they cannot be stopped by better authentication methods and other typical fraud countermeasures.

Monitor for changes in existing payee information. Given criminals' role in legitimate transactions, they may attempt to avoid detection by gathering and altering existing payee information. Monitoring for changes in existing payee information, however subtle, can provide an FI with sufficient justification to contact the account holder to confirm the transaction, or to block it outright.

Connect with contact list. Allowing the app to gather contact information from the user's device reduces the risk of mistyping information such as a phone number or person's name, which could result in a misdirected payment to an unintended recipient. From a fraud perspective, connecting with the contacts stored on an individual's device could limit the potential for phishing by a fraudster purporting to be someone with a phone number or email that doesn't match the stored information.

Monitor user behavior to detect risk early. Users' behavior can provide clues to their intent. Integrating user behavior analytics/ behaviometrics focuses on a person's behavior rather than on their physical characteristics and can lead to the detection of activity that is inconsistent with the true account holder or that is odd in itself. Depending on the solution, this technology can capture and analyze finger size and pressure when selecting keys in an app or the way someone holds a phone, thus generating a unique profile and related score.

Integrate strong, step-up authentication. As the scenario dictates—such as the addition of new payees, the changing of account information, or transactions over a certain limit—FIs can use various levels of authentication to vet the user and approve the activity. Additionally, using intelligence from prior successful interactions with the customer can help identify the safest channel, device, and method for step-up authentication.

Educate customers on fraud risks and their responsibilities. With any new platform, customers must understand the rights and responsibilities when using the platform. They must know how to protect themselves from fraud and what to do should they uncover suspicious activity.

Leverage the collective intelligence of the market to identify fraud. Because fraud rings tend to cross between FIs, consortium data—information shared across organizations about the fraud risk indicators—can give FIs a leg up. Depending on the source, this data can include anything from device profiles associated with fraudulent activity to behavioral cues that help differentiate between legitimate and suspicious users.

INTRODUCTION

Faster payments are markedly changing the payments landscape. Spanning consumer and commercial applications, payments will post, clear, and settle faster than ever before. For consumers and businesses, this is a welcome revolution, one that some would argue is long overdue. For most financial institutions, this new paradigm represents an opportunity to improve the strength of relationships with retail customers and the potential for increased profitability in commercial payments. Yet faster payments are inherently more attractive to fraudsters. Without adequate controls in place, this new world of speed will also prove an incredible avenue for criminals to make their existing schemes far more effective.

Fully grasping the implications of faster payments requires a refinement of the definition that is often used across the industry. In most instances when discussing faster payments, we must clarify the mechanism used to process the payment—and, by extension, how long it takes to complete the transaction. For example, Japan launched its first "faster payments" product in 1973. That approach would not qualify as fast today given the current standard of immediacy; the Japanese processed those transactions at the end of the day.

New, faster payment types that greatly enhance the utility of existing retail and commercial payments are only just starting to be adopted in the U.S. Unfortunately, there have been clear indications that the speed inherent in real-time payment methods, such as P2P payments, are irresistible to fraudsters. With instant payments right around the corner, fraud will continue to rise, complicating the picture for FIs while driving losses and relationship risks ever higher.

P2P PAYMENTS: CANARY IN THE COAL MINE

Before the advent of Zelle, P2P payments were largely the purview of three sets of providers: big banks (ClearXchange), large fintechs via banks (Popmoney, PeoplePay, etc.) and Venmo (eventually acquired by PayPal). By virtue of how they were marketed and the institutions making them available, these new means to pay attracted certain segments of the population.

'Faster Payments' Actually Breaks Into Three Categories: Faster, Real-Time, and Instant

Figure 1. Types of Faster Payment Schemes

Source: Javelin Strategy & Research, 2019

- **Bank P2P solutions** had little support from larger-institution customers (under ClearXchange), nor among those in mid-tier and community banks as the need was underdeveloped and a lack of interconnectivity made the utility limited.
- **Venmo** targeted younger consumers, largely millennials, with its integrated social capabilities. It positioned itself as a payment option for their specific needs, such as splitting lunch, paying bills, sharing rent, etc.

Although the adoption of P2P payment platforms was relatively limited, these solutions were not without fraud risk. For example, bank P2P products saw early cases of activity related to account takeover, leading to unauthorized withdrawals. This development drew the attention of regulators, but the exposure remained relatively limited as the network for transmitting payments reduced the fraudsters' ability to access funds. This was also the case for consumers.

Nonetheless, some Venmo users were manipulated into making payments for goods and services via social engineering or other schemes. Due to the language used when users are notified about the completion of payments, some were led to believe that a transaction was done when it could, in fact, be reversed.

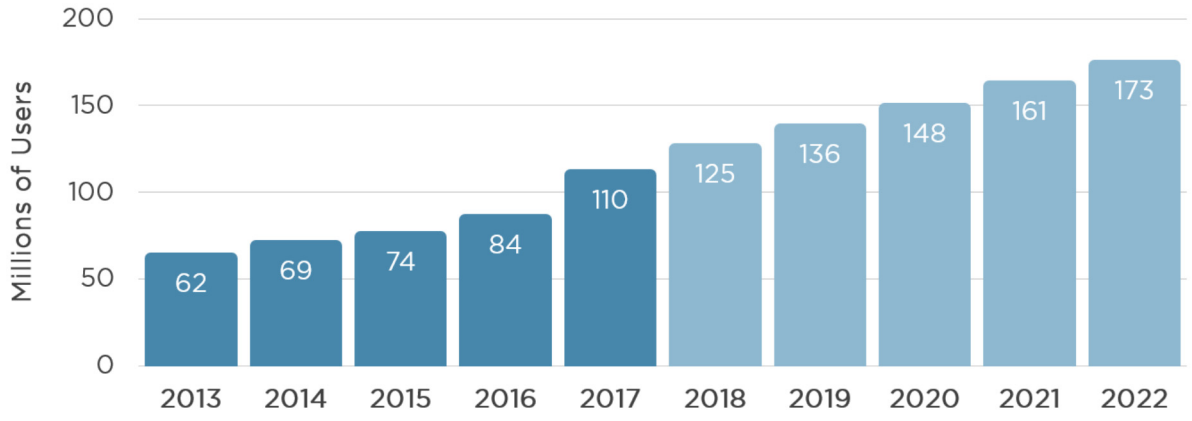
ZELLE: WHEN BIG BANKS STRIKE BACK (FRAUDSTERS LIE IN WAIT)

Not wanting to be left behind as Venmo began to gain momentum, in large part due to its acquisition by PayPal, the large-bank owners of ClearXchange repositioned and rebranded its offering as Zelle. However, the new name didn't change the fact that transactions made via Zelle are a mix of payment types, which can complicate how FIs manage fraud risk. Case in point: Zelle transactions between participating banks are ACH transactions, not true real-time payments, even though they show immediately in a customer's account. Furthermore, transactions between a Zelle bank and non-Zelle bank ride Mastercard Send or Visa Direct rails.

After a significant effort to raise awareness, Zelle has gained considerable momentum,

P2P Payment Adoption Shows No Signs of Slowing Down

Figure 2. Millions of Digital P2P Payments Users (2013-2022, Forecast)



Source: Javelin Strategy & Research, 2019

with 200 banks committed to the platform, of which approximately 60 are now live. With P2P payments now built into the mobile banking apps already installed on consumers' phones, Zelle came ready with a pre-established base of potential users. In 2017, with the public rollout of Zelle, the number of consumers using digital P2P payments jumped from 84 million to 110 million, a significant spike after four years of slow, steady growth.

Yet there were early growing pains. Social engineering, scams, and underprepared customers created a lethal combination, which triggered a series of high-profile incidents highlighting a general lack of awareness among consumers about how Zelle was designed to be used. The fact that consumers did not receive the same liability protections as they did with other financial products, such as cards or PayPal, only compounded the problem.

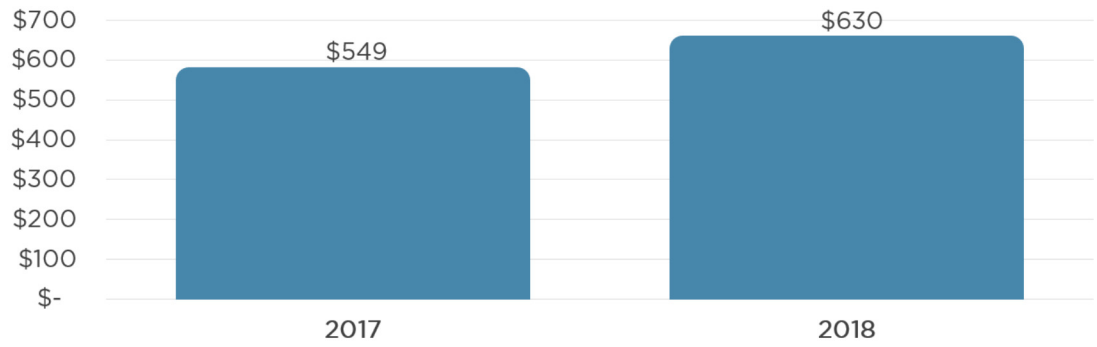
When it came to account takeovers, earlier P2P platforms inspired fraudsters to compromise retail bank accounts, which provided a faster, more convenient (digital) means of draining these accounts. However, the limited networks of these P2P platforms acted as an artificial control that prevented broadscale fraud. Unlike with previous platforms, Zelle was purposely designed to allow transfers to both Zelle network banks and non-network banks, making it much more flexible for legitimate users and for fraudsters—hence its emergence as a driver of account takeover schemes. To underscore the threat, between 2017 and 2018, P2P losses grew from $549 million to $630 million, an increase of 15%.

For the same reasons, quick, cheap, and flexible tools to move funds always run the risk of creating avenues for money laundering. Rapidly moving money between accounts held either by fraudsters or by unwitting money mules makes it much easier to conceal the movement of fraudulent funds than is possible with slower payment methods.

Zelle's value proposition and use cases are sure to grow beyond today's P2P application into business-to-consumer (B2C) payments. In fact, we can see early examples of similar evolutions in the retail space, along with the emergence of Venmo as a means of making

P2P Fraud Losses Climb from 2017

Figure 3. Millions of Dollars in P2P Fraud Losses (2017 and 2018)



Source: Javelin Strategy & Research, 2019

all kinds of P2P payments. Along those lines, we might eventually see disbursements to consumers for things like insurance payments, for example. These new applications will only encourage greater exploration and exploitation by fraudsters looking to manipulate or misuse these capabilities.

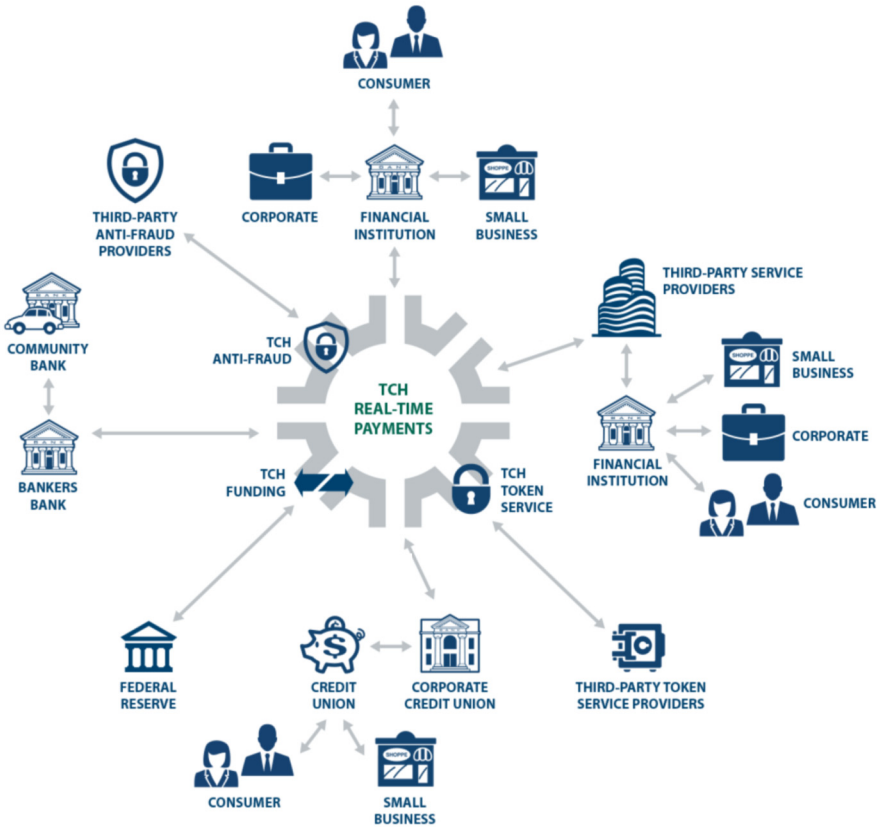
Should Zelle, Venmo, and other P2P schemes, such as Square, accelerate their payment speeds, this will only encourage more fraud and money-laundering activity. This will be especially challenging for smaller banks whose controls generally tend to work best in thwarting simpler schemes. Criminals will undoubtedly shift their attention from larger FIs that generally possess the ability to combat sophisticated frauds to smaller, less-prepared institutions.

A NEW ERA: THE CLEARING HOUSE RTP

A true instant-payment rail, RTP (based on ISO20022) has the potential to do for bill payment, along with disbursements and other commercial payments, what Zelle has begun to do for consumer payments. RTP also has the potential to eventually support P2P payments. And since RTP is owned by 26 of the world's largest commercial banks and has partnerships with leading core providers

The Clearing House's RTP Initiative Brings Instant Payments to Commercial Clients

Figure 4. The Clearing House RTP Network Framework



Source: https://www.theclearinghouse.org/payment-systems/rtp/

FIS, Fiserv, Jack Henry, and Finastra, it should receive broad-based acceptance and an early focus on commercial payment applications.

Nonetheless, the inherent speed and convenience of digital payment offerings built on top of RTP will undoubtedly inspire some of the same types of threats found in P2P applications. As it relates to commercial payment risk, disbursements will become a higher-profile target as criminals attempt to manipulate account information to redirect payments, which could include employee paychecks that today are routed via ACH or vendor payments. Or they could simply initiate payments to accounts they have taken over with the promise of being able to gain access to those funds immediately.

Business email compromise schemes are also likely to increase once instant payments become a reality. The lag between being able to move funds from an organization's account and the detection of a breakdown in internal controls, triggered by compromised email communications, will only work to fraudsters' advantage.

One of the most significant risks in introducing RTP into commercial payments is the potential for it to upend bank relationships with clients. Fraud involving these payments would fall onto the client (under UCC4A), and any significant rise in fraud could lead to significant growth in lawsuits, some perhaps challenging the efficacy of controls that banks put into place, as the inherent risk profile of such transactions will materially change with their speed.

From a retail payment risk perspective, bill payment has been a historical target for fraudsters, who, for example, make small changes to a destination account for an existing payee to redirect funds to an account under their control. Moving these payments to RTP will put a significant strain on FIs that have traditionally managed these as ACH payments, allowing considerable time to identify and stop suspicious transactions.

LEARNING FROM YESTERDAY'S MISTAKES

While Zelle continues to capitalize in the expansion in P2P payments and other projects are expanding real-time payments into corporate payments, there's much to learn from the platform's early challenges with fraud. For financial institutions and other fintech players considering accelerating their current payments features or rolling out new payments technology, a few key considerations should be focused on from Day 1:

- **Integrate tightly with pre-existing fraud detection systems.** While the host of a payment platform may offer fraud detection capabilities, that is necessary but not enough to prevent fraud. Similar to the integration of other streams of payment-related data, all payment data must integrate with the FI's fraud platform. Doing so provides additional layers of analysis and protection as well as the people, processes, and technology needed to investigate and make decisions about suspicious transactions, as well as to notify customers.

- **Build robust initial controls.** Most implementations lacked strong step-up authentication methods to control for risk around high-value transactions, new payees, or indicators of account takeover, such as recently changed account information. In the background, risk assessment tools, such as user behavior analytics, paired with softer restrictions, such as early account limits, could have helped reduce the intensity of fraud on early accounts.
- **Educate users on appropriate use of the platform and the key risks.** While banks and regulators clearly delineate between "fraud" and "scams," consumers expect to receive similar protections from each. This meant that early victims who were deceived into sending funds to scammers received a rude awakening when they were told that they may be liable for the lost funds and not reimbursed as they would be after card fraud.

CONCLUSION

While it took years for P2P payments to take hold in the marketplace, the PayPal acquisition of Venmo changed the landscape, forcing the owners of ClearXchange to reposition and rebrand as Zelle. As the number of P2P payment types grows, we can expect fraudsters to attempt to exploit every platform—both in the retail and commercial spaces.

While speedy payments attract customers, they are also inherently appealing for fraudsters. Any payment platform that wishes to increase its number of retail and commercial users must raise the bar when it comes to fraud prevention and awareness. Tight integration with existing fraud platforms, strong authentication, and engagement with users are all crucial to laying the groundwork for success.

METHODOLOGY

Consumer data in this report is taken from:

- A random-sample panel of 5,000 U.S. adults fielded in November 2018. For questions answered by all 5,000 respondents, the maximum margin of sampling error is 1.41 percentage points at the 95% confidence level.
- A random-sample panel of 3,000 U.S. adults fielded in October-November 2017. For questions answered by all 3,000 respondents, the maximum margin of sampling error is 1.74 percentage points at the 95% confidence level.

ABOUT JAVELIN STRATEGY & RESEARCH

Javelin Strategy & Research, a Greenwich Associates LLC company, is a research-based consulting firm that advises its clients to make smarter business decisions in a digital financial world. Our analysts offer unbiased, actionable insights and unearth opportunities that help financial institutions, government entities, payment companies, merchants and other technology providers sustainably increase profits.

Authors: Kyle Marchini, Senior Analyst, Fraud Management
Al Pascual, Senior Vice President, Research Director
Paul McCormack, Senior Advisor

Contributors: Sarah Miller, Research Manager – Custom Research & Operations
Crystal Mendoza, Production Manager

Publication Date: May 2019

ABOUT NICE ACTIMIZE

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumer and investor assets by identifying financial crime, preventing fraud and providing regulatory compliance. The company provides real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.