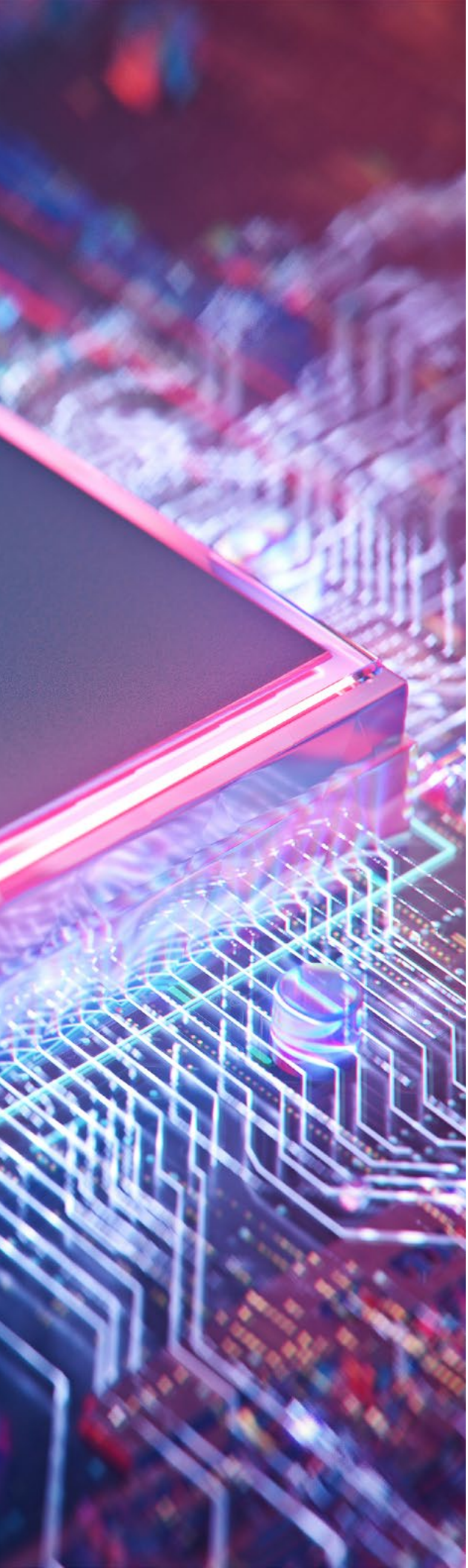
OCTOBER 2020

PREVENTING FINANCIAL CRIMES PLAYBOOK

PYMNTS.com | NICE · ACTIMIZE



PYMNTS.com | NICE · ACTIMIZE

PREVENTING FINANCIAL CRIMES PLAYBOOK

ACKNOWLEDGMENT

The Preventing Financial Crimes Playbook is done in collaboration with NICE Actimize, and PYMNTS is grateful for the company's support and insight. PYMNTS.com retains full editorial control over the following findings, methodology and data analysis.

WHAT'S INSIDE

Financial crime is a constant worry for banks, credit unions, FinTechs, other financial institutions (FIs) and businesses around the world — and for good reason.

Total fraud losses clock in at $1.45 trillion a year, with almost half of organizations worldwide reporting such losses in 2018. A financial fraud attack against FIs or businesses occurred every two minutes on average in 2019, summing to 59,627 attacks that year.

This year has been even worse on the fraud front as financial crime stresses FIs that are already confronting the pandemic, economic struggles and an unpredictable political climate. Digital and mobile payments are surging as businesses and consumers transact from home, and this increased digital engagement has opened the door to more financial crime. Twenty-one percent of all fraud attacks were waged on mobile transactions in the first half of the year and 37 percent of them originated from mobile devices.

Peer-to-peer (P2P) payment apps like CashApp, PayPal, Venmo and Zelle are especially popular targets for financial crime as more than 1 billion individuals around the world use these solutions. Fraud attacks against these apps have increased by 733 percent since 2016 and over $2.2 billion more was stolen in 2019 than in 2018. Fraudsters deploy numerous tactics to target these apps, including sophisticated hacks like account takeovers (ATOs) and old-fashioned confidence schemes that trick users into sending them money directly.

Securing P2P apps as well as other financial accounts will require banks to upgrade their security protocols and customers to take their security more seriously. Just 37 percent of bank customers use separate passwords for different accounts, for example, and 22 percent use two to five passwords across all their online profiles. This means that even one compromised account could threaten all others that rely on the same credentials, potentially costing victims a fortune in stolen money and data.

Financial crime will almost certainly never be stopped entirely, but consumers and banks that make it harder for fraudsters to crack their defenses are likelier to hold criminals off. This could ultimately lead bad actors to seek out easier targets or even abandon their schemes altogether.

GLOBAL FINANCIAL CRIME DEVELOPMENTS

One illicit activity plaguing FIs and their customers is impersonation fraud, in which cybercriminals pose as trusted officials and trick victims into sending them money. The United Kingdom experienced an 84 percent increase in this fraud type in 2020, mostly due to bad actors impersonating police, government officials or victims' banks to exploit the confusion surrounding the pandemic. This tactic has been used to steal more than £58 million ($74.9 million USD) this year.

FIs have had some success in halting fraud, however. U.K. banks managed to reduce their fraud losses by £374.3 million ($483.4 million

USD) during the first half of 2020 compared to the same period last year, blocking £853 million ($1.1 billion USD) from being stolen. This accounted for approximately 70 percent of all fraud attempts, though experts warn that this assessment may be preliminary because of the lag that often occurs between when cybercriminals steal victims' personal data and use it for profit.

Consumers are willing to go along with bank security measures, but only to a point. A recent study found that almost 70 percent of bank customers are willing to share email addresses, birthdays and other standard data for security purposes, but only one-third are comfortable handing over biometric data like voiceprints or fingerprints. Approximately 30 percent of consumers say they would be more at ease doing so if banks explained why sharing such details was necessary, however.

For more on these stories and other financial crime prevention developments, read the Playbook's News and Trends section (p. 12).

Executive Insight

The number of P2P payments fraud victims has shot up by 733 percent since 2016. What factors are contributing to this increase, and how can FIs prevent bad actors from taking advantage of their customers?

"When it comes to scamming consumers, fraudsters tend to capitalize on the unknowns. Whether that be the learning curve of new technology, or, as seen in recent events, the unknowns of a global pandemic — fraudsters will prey on these opportunities. One of the challenges of P2P technology is the immediacy of the payment. While that may seem to be a benefit for consumers, it can be a double-edged sword. This immediacy means that, once initiated, the payments are virtually irrevocable.

We are seeing fraudsters use P2P payment services as the final steps in larger, more traditional fraud attacks — such as check fraud [and] social engineering. … Therefore, as payments services evolve to meet customer demand, so must a financial service organization's fraud controls. It's important for [financial service organizations] to a take real-time, cross-channel, cross-payment holistic approach when it comes to their fraud controls. At Actimize, we use behavioral analytics to detect and prevent fraud across multiple payments products and servicing channels to allow organizations a single view of the customer. Consolidated account and customer-level alerts, cross-channel investigations and robust reporting and query tools reduce false positives and enhance investigations, enabling a frictionless customer experience for the [financial service organization's] customers."

YUVAL MARCO

general manager of fraud and authentication at NICE Actimize

HOW P2P PAYMENT APPS LEVERAGE AI TO FIGHT SCAMS AND FRAUD

P2P payment apps face a double-edged cybercrime threat: technological fraud schemes, like ATOs, as well as scams targeting their users. These threats require a dual approach that leverages both artificial intelligence (AI) and customer awareness, according to Jamie Armistead, vice president and business line leader for banking app Zelle. This month's Feature Story (p. 8) explores how apps like Zelle work with their bank partners to identify suspicious transactions and provide their customers with the knowledge they need to spot scammers.

DEEP DIVE: HOW P2P PAYMENT APPS FIGHT FRAUD

P2P payment apps have become commonplace around the world, with more than 1 billion individuals globally and 70 percent of Americans using them in some capacity. These apps are vulnerable to bad actors, who perpetrate schemes like ATOs or social engineering fraud against their users. In this month's Deep Dive (p. 17), PYMNTS explores the fraud threats these apps face as well as how firms are deploying multifactor authentication (MFA) to keep fraudsters at bay.

FIVE FAST FACTS

84%

Increase in impersonation fraud in the U.K. in 2020

£374.3M

Reduction in fraud losses by U.K. banks in first half of 2020

61%

Share of Chinese seniors who have been victimized by fraud

67%

Share of banks that offer mobile P2P payment services

41%

Portion of attacks against FIs since 2017 that leveraged credential stuffing

FEATURE STORY

How Zelle Protects Users Against Scams And Fraud With AI, Analytics

P2P payment apps have gained ubiquity over the past decade, supplanting or replacing cash transactions, personal checks or wire transfers for payments between individuals or sometimes even small businesses.

Gone are the days of diners handing waiters a stack of credit cards to split a bill, with consumers instead making seamless money transfers that occur in a matter of seconds. Payment apps like CashApp, Venmo and Zelle are used by more than 70 percent of Americans.

These apps are not without danger, though, and fraudsters are looking to cheat and scam their way to paydays from innocent users. Venmo users alone lost more than $40 million in 2018. Meeting this fraud threat will not only require in-depth knowledge of fraudsters' techniques but also advanced technology and customer vigilance, according to Jamie Armistead, vice president and business line leader for banking app Zelle.

"We split out scams and frauds," he explained in a recent interview with PYMNTS. "Fraud means someone is trying to access your device, while scams consist of people being tricked into sending money."

Armistead recently offered PYMNTS an inside look into the different techniques that fraudsters leverage as well as the initiatives Zelle undertakes to protect itself and its users.

THE SCAMS AND FRAUD FACING P2P PAYMENT APPS

Zelle largely categorizes the threats it faces into two broad categories: scams that swindle users into sending bad actors money and fraud that utilizes more technical means to infiltrate users' accounts. The former encompasses a wide range of different schemes, and fraudsters will go to great lengths to hide their identities and present sympathetic faces to their victims.

"There are extremely elaborate scams with puppies for sale, for example," Armistead explained. "There are really elaborate but completely bogus websites of puppies, with pictures of the puppies, links to bogus pet transport services, et cetera. Unfortunately, they're highly effective at getting people to pay hundreds of dollars for a puppy that doesn't exist."

Scams have taken on a new life amid the COVID-19 pandemic, according to Armistead, with scammers impersonating tax officials, personal protective equipment (PPE) sellers or bank personnel to trick victims into sending them money. The economic anxiety associated with the pandemic has made victims especially vulnerable.

Fraud typically involves perpetrators infiltrating users' accounts directly. Cybercriminals deploy a variety of tactics to do so, with phishing being the most popular. Fraudsters send out mass emails and trick users into surrendering their app login details, which they then use to take over accounts and either send money to their own bank accounts or steal personal data.

Securing both of these risk avenues is a difficult undertaking that Zelle does not conduct alone. The app relies on both in-house analytics systems and its FI partners' security systems to fight these scams and fraud attempts.

LEVERAGING AI TO FIGHT CYBERCRIME

Fraudsters often work together in organized crime rings, so it makes sense for payment apps and their bank partners to collaborate, too. Zelle's first line of defense against fraudsters is its bank partners' security systems, meaning that any potential bad actor has to first clear the onboarding system of the bank associated with a given Zelle account.

"It starts at the financial institution level, as they already have a number of tools and technologies in place," Armistead explained. "But as you go through that enrollment process, we are doing a number of things behind the scenes to validate [that] you are who you say

you are. We can access and look at the risk profile of an email address, for example."

Zelle also relies on its AI-based pattern recognition system to locate suspicious transactions that could indicate fraud. These anomalies vary by customer type, location and numerous other variables, all of which the system takes into account.

"We try to identify patterns associated with fraud or scams because we see all the transactions at the network level," he said. "Maybe they're using one account to run a scam and using another account to move the money, or they're just temporarily holding the funds and they're liquidating it once they get it to a third point in that equation. That's the type of stuff that we would sometimes use AI to try to examine."

Scams are a little trickier as they can often appear legitimate to automated systems. Identifying scams relies much more on customer awareness, though arming users with as much information as possible significantly reduces risk.

"We do things to help people ensure they're sending money to the right place; for example, making sure that when they enter a phone number, it comes back with a name prompt to let them know who they're sending money to," Armistead said. "We also have warning messages that remind people to only send money to people they know and trust."

Payment apps like Zelle ultimately rely on a combination of customer vigilance and prevention measures to prevent scams. Fraudsters work together on cybercrime and banks and payment apps collaborate on fraud prevention, and so too can apps and their customers cooperate to drive down fraud attempts and scams to manageable levels.


NEWS &
TRENDS

Financial crime trends

RISE IN CONTACTLESS PAYMENTS LEADS TO INCREASED FEARS OF CNP FRAUD

Contactless payments are becoming more popular because they can enable quicker transactions than traditional credit cards, especially for payments between individuals. One recent survey found that 67 percent of banks provide some form of mobile P2P payment service — a 13 percent rise since 2016. These solutions are also offered by 39 percent of credit unions and 26 percent of banks, and 29 percent of credit unions that do not currently offer them plan to do so by next year.

There are still some concerns regarding these payments, bank executives say, including card-not-present (CNP) fraud. Such incidents involve hackers using victims' payment information rather than their physical payment cards, making the schemes particularly well-suited online marketplaces. Thirty-nine percent of executives cited CNP fraud as their top concern for contactless payments while 29 percent were most concerned about a lack of security best practices among their customers.

IMPERSONATION FRAUD INCREASES BY 84 PERCENT IN UK

U.K. banks and their customers are also facing impersonation fraud, in which fraudsters pretend to be trusted officials and trick victims into sending them money. These schemes have increased by 84 percent this year as bad actors exploit the confusion surrounding the ongoing COVID-19 pandemic. U.K. Finance members reported 15,000 cases of impersonation fraud between January and June of this year, and 8,200 of the cases involved fraudsters impersonating police or victims' banks. Most of the remaining cases involved cybercriminals pretending to be utility companies or government officials.

More than £58 million ($74.9 million USD) was stolen using these tactics between January and June. Experts say banks should be responsible for stopping these scams as they can identify suspicious transactions and reverse them if they are deemed fraudulent.

U.S. TREASURY DEPARTMENT SAYS BUSINESS LOAN FRAUD REPORTS SKYROCKETED IN AUGUST

The U.S. government's pandemic response has included significant aid to businesses, including the Paycheck Protection Program (PPP), which promised loan forgiveness for businesses that did not lay off any employees. This wave of federal aid coincided with a spike in business loan fraud, however, and the Treasury Department's Financial Crimes Enforcement Network (FinCEN) said it received 1,922 reports of such activities in August alone. The department did not specifically say the two were correlated, but it has warned of fraud schemes related to aid programs such as the PPP and the Small Business Administration's (SBA's) Economic Injury Disaster Loan program.

61 PERCENT OF CHINESE SENIORS HAVE BEEN VICTIMIZED BY FRAUD, STUDY FINDS

Digital banking's global popularity boost has extended even to seniors, who have historically been averse to new technologies. One recent study found that 49 percent of seniors in China leverage mobile banking, as do 24 percent of those in Hong Kong and 19 percent of them in Singapore. The study determined that mobile banking apps and budget management tools were especially popular.

These seniors' adult children are concerned about their parents' risk of financial crime, however. Eighty-three percent of the adult children reported being confident in seniors' abilities to recognize and prevent financial crime, but 61 percent of seniors have been victimized — a rate 30 percentage points higher than the worldwide average. Chinese seniors may be cognizant of the dangers now, but additional education could be necessary to prevent them from falling prey to new fraud schemes.

> 83% of Chinese adult children reported being confident in seniors' abilities to **recognize and prevent financial crime.**

FBI WARNS AGAINST INCREASE IN CREDENTIAL STUFFING ATTACKS

Fraudsters deploy many schemes when attacking banks and their customers, wielding techniques as diverse as social engineering, identity theft and phishing. One tried-and-true tactic is credential stuffing, in which hackers algorithmically enter huge numbers of acquired username and password combinations to access accounts. The FBI recently stated that 41 percent of financial industry attacks from 2017 to 2020 were conducted via the method, and many of these incidents harnessed botnets to conduct their schemes.

This increase was due to two factors: the vast amount of stolen credentials circulating on the dark web — with some reports pegging the current total at 5 billion — as well as poor security hygiene such as password recycling and a lack of MFA. The FBI said bank customers should sign up for MFA and avoid repeating passwords to limit the damage hackers could do with stolen credentials.

P2P PAYMENT FRAUD HAS INCREASED BY 733 PERCENT, STUDY FINDS

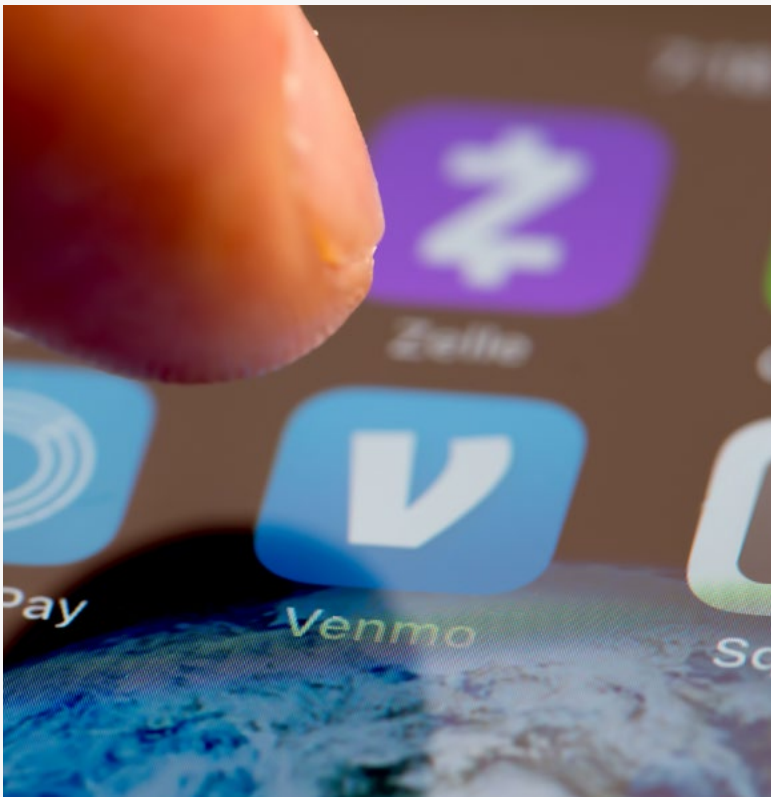
P2P payment apps like Venmo and Zelle have seen their popularity skyrocket in recent years, with 71 percent of Americans using them as of April 2020, for example. Almost two-thirds of U.S. adults use them on at least a semiregular basis, but these apps could put users at risk of financial crime unless adequate safeguards are in place. The number of P2P payment fraud victims has increased by 733 percent since 2016, and fraudsters have leveraged numerous techniques for their schemes. Some stage ATOs while others use stolen identities to start accounts and drain victims' linked bank accounts. Many of these apps also cannot recover stolen or mistakenly sent funds, even though more than half of users believe they can.

Fraud prevention trends

U.K. BANKS REDUCE FRAUD LOSSES BY £374.3 MILLION IN FIRST HALF OF 2020

Many banks' financial crime prevention measures seem to be paying off, despite recent increases in cybercrime, with U.K. FIs reducing their fraud losses by £374.3 million ($483.4 million USD) during the first half of 2020 compared to the same period last year. These banks blocked £853 million ($1.1 billion USD) in attempted fraud during this period, totaling approximately 70 percent of all financial crime attempts. Experts warn that these numbers may be only preliminary, however, as there are often delays between when cybercriminals steal victims' personal data and when they use it for profit.

Contactless card fraud fell by 20 percent, marking the first decrease in this fraud type since reporting on it began in 2013. The decline in check fraud losses was even more dramatic, falling by 78 percent. Investment scam losses rose by 27 percent, however, meaning banks may need to step up their fraud prevention efforts in that area.



CONSUMERS ARE MORE WILLING TO SHARE PERSONAL INFORMATION FOR SECURITY PURPOSES

Ensuring that customers are who they say they are during onboarding is key to keeping fraudsters from infiltrating banks' systems. A recent study found that almost 70 percent of consumers are willing to share their email addresses, birthdays and other data for authentication purposes, but this willingness has a limit. Only one-third of consumers would be comfortable providing biometric data such as fingerprints or voiceprints when accessing their bank accounts, for example.

Banks can take steps to make customers more amenable to sharing this data, however. Approximately 30 percent of consumers say they would be more at ease with biometrics if FIs explained why it was necessary to provide them.

Almost **70% of consumers** are willing to share their email addresses, birthdays and other data for **authentication purposes.**

FIs take on new security measures

FINTECH MODULR BECOMES FIRST NONBANK TO ADOPT CoP

CoP is being leveraged by more than just traditional banks in the U.K., with FinTech Modulr recently adopting the system to protect its clients. Modulr's solution, much like those of its bank counterparts, will warn users if the names they enter do not match those of their intended recipients to reduce fraud over payment apps. The widespread adoption of CoP is being led by Pay.UK, the country's retail payments authority, amid rising authorized push payment fraud. Modulr's adoption of the system follows its other recent payments initiatives, including offering access to the Faster Payments and Bacs payment schemes in 2019.


DEEP
DIVE

Fighting Back Against **The Fraud Plaguing P2P Payment Apps**

P2P payment apps — including third-party solutions like Venmo and CashApp as well as first-party banking apps — allow users to seamlessly pay each other for informal services and goods and have recently become incredibly popular. Some retail establishments are also adding P2P-enabled payments to their repertoire of contactless payment apps, like Apple Pay or Google Pay.

A report predicted that 1 billion individuals around the world would use some sort of payment app this year and projected this number to grow to 1.31 billion by 2023. This group includes more than 70 percent of Americans, according to the American Association of Retired Persons (AARP).

The ubiquity of these apps belies serious security concerns, however. Fraudsters utilize numerous schemes to intercept these payments or trick app users into paying them directly, and the problem has worsened as the apps have gained popularity. The number of P2P payment fraud victims has increased by 733 percent since 2016 and the total amount of money stolen has likewise risen. There were 1.4 million fewer fraud victims in 2019 than in 2018, for example, but the total cost of these incidents rose by $2.2 billion.

The following Deep Dive explores the fraud methods P2P payment apps and their users face as well as the security measures app providers are deploying.

PAYMENT APP FRAUD THREATS

Account takeovers are one of the most pervasive threats payment app users face. Fraudsters perpetrating these schemes seize control of customers' accounts and use them to access credit card data or steal funds. Cybercriminals can leverage methods like phishing or brute force botnet attacks to

access users' accounts, but one of the most common strategies involves purchasing stolen credentials in bulk online. Researchers have found 15 billion such credentials circulating the dark web, and because individuals typically use similar passwords and usernames for multiple logins, this stolen information can be applied to even greater numbers of accounts.

Other fraudsters forgo infiltrating accounts in favor of tricking payment app users into paying them directly, posing as friends or trusted authorities. These scams have become more sophisticated as app users grow more aware of the practice, and fraudsters are getting more creative. The Better Business Bureau (BBB) recently warned users about a new scam that is gaining popularity. Users receive seemingly innocuous messages asking for the return of accidental payments, at which point victims notice deposits of several hundred dollars in their accounts and return the money in good faith. These funds come from stolen credit cards, however, and after scammers send money to victims, they switch out the stolen credit card details with their own and link them to their P2P accounts. The stolen money then goes into the scammer's bank accounts while funds are removed from the victim's, costing them that amount when the owner of the stolen credit card seeks reimbursement.

The ongoing pandemic is allowing such scams to become even more pervasive, and fraudsters are capitalizing on consumers' fears and economic uncertainty by posing as people in need, businesses selling personal protective equipment or government officials promising stimulus checks. The AARP estimated that Americans had lost $13.4 million to COVID-19-related payment app scams as of April.

HOW APPS FIGHT FINANCIAL CRIME ON THEIR PLATFORMS

Protecting payment apps from crime thus falls on payment apps as well as their users. One of the most effective tools that apps can deploy against account takeovers is MFA, which requires users to enter secondary validation measures — such as emailed security codes or biometric fingerprint scans — in addition to their passwords. These authentication methods can stop potential bad actors cold, making the passwords they steal from data breaches useless on their own. Studies have found that using MFA can prevent more than 99.9 percent of attacks that utilize stolen credentials.

Payment app users also have to take security into their own hands. The first step is often fixing poor password hygiene. A recent study from data analytics firm FICO found that only 37 percent of bank customers use separate passwords for different accounts, for example, while 22 percent use two to five passwords across all their online profiles. This represents a massive security risk as a data breach that compromises a single account could give fraudsters access to any other account using the same password. App users should also be wary of transferring funds to strangers and report suspicious transactions to the apps' security teams.

P2P payment apps are revered for enabling the convenient and seamless transfer of funds, despite security worries. App developers and users therefore need to up their security games to ensure that these apps retain their usage well into the future.

ABOUT

PYMNTS.com is where the best minds and the best content meet on the web to learn about "What's Next" in payments and commerce. Our interactive platform is reinventing the way companies in payments share relevant information about the initiatives that make news and shape the future of this dynamic sector. Our data and analytics team includes economists, data scientists and industry analysts who work with companies to measure and quantify the innovations at the cutting edge of this new world.

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.

Stay current with NICE Actimize webinars at actimize.nice.com/events.

We are interested in your feedback on this report. If you have questions, comments or would like to subscribe to this report, please email us at feedback@pymnts.com.

PREVENTING FINANCIAL CRIMES PLAYBOOK