REAL-TIME PAYMENTS TRACKER®

The Clearing House | PYMNTS.com

JANUARY 2021

REAL-TIME PAYMENTS® TRACKER

TABLE OF CONTENTS

Acknowledgment
The Real-Time Payments Tracker® is done in collaboration with The Clearing House, 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

Real-time payment services can give businesses and consumers more control over their cash flows and reassure them that funds will reach their recipients on time. These transactions' irreversible natures can reassure retailers that have previously been stung by friendly fraud and are looking to avoid such problems in the future. Rapid disbursements delivered over real-time networks also satisfy consumers who want to receive funds that are immediately ready to spend.

Fraudsters are also turning their attentions toward real-time payment systems, however. Bad actors capitalize on such transactions' immediacy and irreversibility to make off with victims' funds. They know that the money rapidly settles in recipients' accounts and that financial institutions (FIs) have little time to intervene and prevent real-time transactions from completing once they have been initiated. FIs thus need to modernize their fraud-fighting approaches when they adopt real-time payment services, and robust technologies can help. Advanced learning tools and abundant data troves can help banks proactively detect red flags and deal with potential fraud before schemes are perpetrated.

Around the world of real-time payments

Real-time payments are becoming more and more popular among consumers and businesses alike, but some FIs are finding it challenging to safeguard such systems. These struggles are leading many to examine cutting-edge tools that can help them better protect these transactions from fraud. A recent study found that 78 percent of FIs surveyed in the Asia-Pacific region reported rises in fraud losses after debuting real-time payments services. Tools that help banks quickly analyze consumers' behaviors for suspicious activities could help banks level up their defenses and ferret out bad actors before fraudsters pull off their scams.

Security upgrades could also usher in significant changes across the payments space. Recent surveys found that 38 percent of United States financial executives cite

EXECUTIVE INSIGHT

"cybersecurity attack" and "payments fraud" fears among the factors that impede the greater use of digital payments. Survey respondents did not specify the kinds of cyberthreats they envisioned, but many potential risks could come into consideration. Companies that accept digital transactions must create safe payment environments, preventing eSkimming attacks that use malware to steal card data that is entered at checkout. Businesses may also need to ensure they can securely store clients' sensitive payment details and block attempted data breaches. Companies that practice good security hygiene, which includes regularly monitoring and updating third-party codes to prevent or catch malware, may be more eager to modernize their payment flows.

Promoting better education regarding faster payments options and their implications for businesses and consumers could also encourage greater adoption, and Nacha, which sets the rules for the Automated Clearing House networks in the United States, appears to be invested in these efforts. The association's Faster Payments Project Team is currently working on a resource to familiarize companies with the latest faster payments developments and inform their strategies. The team is expected to debut its corporate-focused playbook within the next six months.

For more on these stories and other recent real-time payments headlines, read the News and Trends section (p. 12).

FIs that adopt immediate payment services may need to take new fraud-fighting approaches to keep transactions safe. What key security strategies should they implement?

"Customers have made it clear that they want real-time payment options, and we are already seeing the important role they play in commerce and the economy — especially during the pandemic. Ensuring the payments rails are secure has been a priority for FIs and will continue to be moving forward, as we know fraudsters will attempt to scam customers, especially as the number of FIs and transaction volumes continue to grow on the RTP® network. The security measures FIs need to deploy to take advantage of real-time payments include techniques that are well-known in the information security space, such as multifactor account authentication, identity confirmation, fraud-monitoring tools and encouraging account holders to use strong passwords and safeguard usernames and account information."

Transactions made over instant payment rails are irreversible, making it important for banks to detect potential payment issues before money leaves an account. What kinds of tools and processes can help FIs address this issue?

"Emerging fraud-fighting methods, such as ones powered by artificial intelligence (AI), can add additional layers of fraud monitoring. The RTP network is also deploying tokenization for accounts on the network, where a token is used for account numbers. Tokenization increases security without harming the user experience — tokenization happens behind the scenes — because the unique token is transmitted during the transaction, not a customer's account details. These measures will also help avoid payments made by mistake. Account authentication, for example, will make sure the account holder is the one sending the payment, not a fraudster. This is important because payments on the RTP network are credit transfers and are irreversible in most cases. (It's worth noting that most fraud involves debits, not credits.)"

How do you expect faster payments security and fraud trends to evolve in the coming year?

"During the next year, these multilayered security and fraud detection techniques will continue to evolve. We also expect to see more AI algorithms in use to identify potential fraud before it takes place."

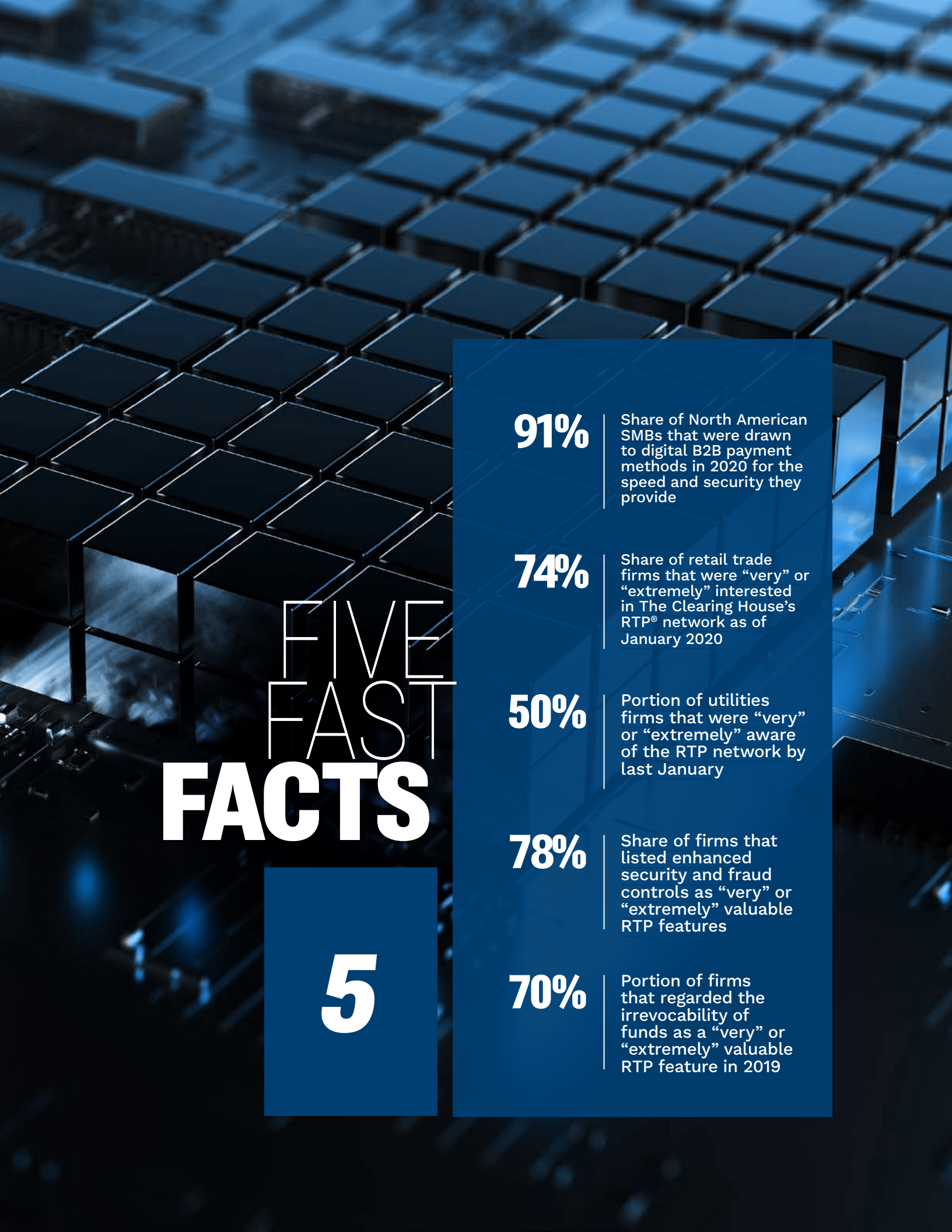
Steve Ledford
senior vice president of products and strategy at The Clearing House

Westlake Financial on designing for a secure RTP rollout

Financial services companies that send disbursements over the RTP® network can give customers the convenience of immediate funds access. Adopting such a system requires upgrading security and risk strategies, however, because money sent over real-time rails cannot easily be reclaimed if delivered to the wrong person due to fraud or human error, according to Raul Alvarez, director of accounting operations at auto financing provider Westlake Financial. In this month's Feature Story (p. 9), Alvarez explained the contingency planning and onboarding procedures that went into ensuring a smooth launch for sending disbursements over the RTP network.

Deep Dive: Thwarting P2P payments app fraud

Peer-to-peer (P2P) payment apps like Venmo and Zelle have become more popular during the pandemic, but bad actors have also been ramping up their attacks against them. Fraudsters often try to trick users into sending them money, and victims have few recourses once criminals make off with their funds. Other attackers launch account takeovers (ATOs) to seize control of legitimate customers' P2P app accounts and steal funds they hold or make charges to the linked payment cards or bank accounts. These app providers must therefore build strong defenses to prevent ATOs, help users detect scams and prevent bad actors from onboarding to begin with. This month's Deep Dive (p. 17) examines how cybercriminals launch these schemes as well as the key strategies app providers can use to combat them.



FIVE FAST FACTS

5

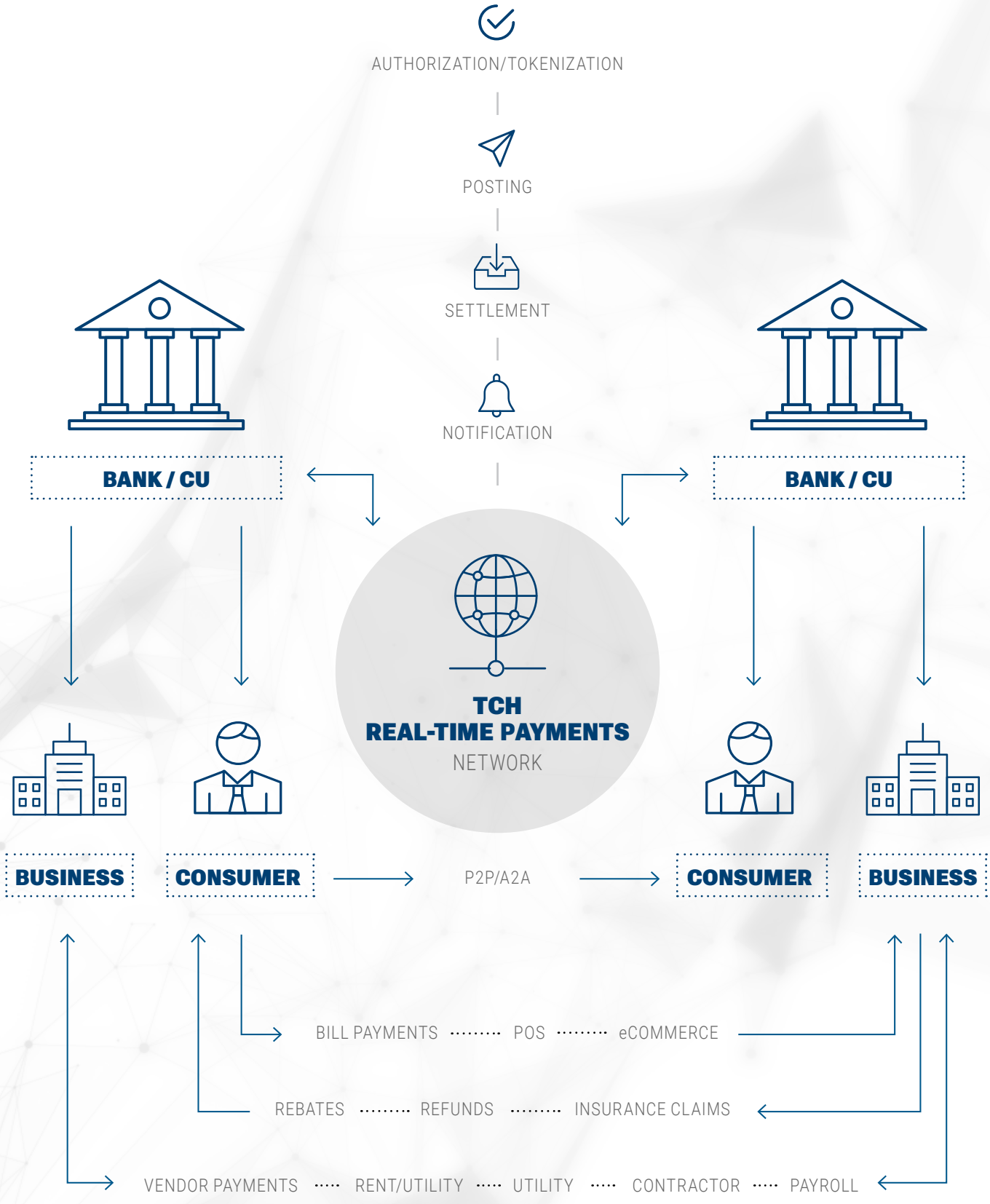
91% Share of North American SMBs that were drawn to digital B2B payment methods in 2020 for the speed and security they provide

74% Share of retail trade firms that were “very” or “extremely” interested in The Clearing House’s RTP® network as of January 2020

50% Portion of utilities firms that were “very” or “extremely” aware of the RTP network by last January

78% Share of firms that listed enhanced security and fraud controls as “very” or “extremely” valuable RTP features

70% Portion of firms that regarded the irrevocability of funds as a “very” or “extremely” valuable RTP feature in 2019


AUTHORIZATION/TOKENIZATION
POSTING
SETTLEMENT
NOTIFICATION
BANK / CU
BANK / CU
TCH
REAL-TIME PAYMENTS
NETWORK
BUSINESS
CONSUMER
P2P/A2A
CONSUMER
BUSINESS
BILL PAYMENTS ..... POS ..... eCOMMERCE
REBATES ..... REFUNDS ..... INSURANCE CLAIMS
VENDOR PAYMENTS ..... RENT/UTILITY ..... UTILITY ..... CONTRACTOR ..... PAYROLL

FEATURE STORY

Westlake Financial Securely Raises **The Speed Limit For Auto Financing Disbursements**

Consumers are going online to complete their shopping during the pandemic — even for major purchases typically done in person, such as buying a car. Consumers who have become accustomed to quick-moving digital transactions may find it all the more painful when their auto financing disbursements take days to arrive, however. Those who were happy to wait days for checks in the mail or for ACH transactions to settle are now likely to regard these delays as unnecessary frictions in their car-buying journeys.

Many consumers are therefore eager for auto financing to be as swift as possible, and companies like auto financing provider Westlake Financial see disbursements delivered over the RTP® network as the future of the industry. Westlake has already sent several million dollars over the RTP network during the pandemic, according to Westlake's director of accounting operations, Raul Alvarez.

Accelerating auto financing disbursements to real-time speeds takes careful planning and preparation, however. As with any payment method, fraud attacks and human errors can upend customer experiences unless companies have strong security strategies in place. Alvarez explained in a recent PYMNTS interview how effectively securing real-time transactions requires thorough contingency planning and advanced customer verification methods.

Contingency planning

The RTP network is a powerful tool, but any tool needs to be wielded properly to have its desired effect. Westlake spent a month and a half testing use cases and troubleshooting fraud scenarios before employing the network. The company was well aware that immediate payments could bring reduced administrative costs, rapid speeds and 24/7 year-round availability, but such transactions are also nearly irreversible, adding complexity. Payments sent to the wrong account by mistake or as a result of a fraudster's scam cannot simply be cancelled before the funds settle.

"We know that real-time payments are a type of payment that's more of a wire — it's very tough to get the funds back," Alvarez said. "We can't pull them back as you would do with ACH or anything else. You can't put a stop payment [like] on a check. The level of risk is higher."

That made it essential for Westlake to ensure it had all of its security measures in place to block fraudsters. It also had to prepare contingency plans for how to respond should bad actors slip through or technical difficulties or human errors interrupt smooth use of the faster payments network.

"There was a lot of risk assessment: 'What happens if this happens? What if that happens?' And making sure we had contingencies in front of us before it really happened," Alvarez said.

The thorough risk assessment required envisioning possible problematic scenarios, such as funds being delivered to the wrong customer account. Alvarez gave a hypothetical example in which auto financing loans were sent to a married couple but delivered into the wrong spouse's account. The company, through an arrangement with its bank, Wells Fargo, can now examine potentially misplaced RTP transactions, reclaim the funds out of the incorrect recipients' accounts and return them to Westlake, Alvarez said.

"If the funds go out over RTP [with] incorrect [account] information, Wells Fargo goes back and looks at the information we provided," Alvarez said. "If, by chance, it went to the wife's bank account instead of the husband, who was the primary account member, it actually goes back to us and we can send the funds again."

Other contingency plans considered what to do should Westlake lose access to the RTP network. The firm accesses the real-time payment system via integration with an application programming interface (API) from its bank, and it had to consider what it would do in the unlikely scenario that it lost this connection mid-transaction, for example. That led to Westlake preparing internal systems so that an interrupted transaction would be switched over to customers' preferred alternate payment methods, like ACH or MoneyGram.

Early intervention

Heading off problems before they happen is ideal, of course, and Westlake and Wells Fargo set up various protections to help anticipate potential issues. Westlake now uses an RTP pre-confirmation system through its bank that compares the account details that the FI has in its records for a given customer against those that Westlake staff enter at the point-of-sale (POS) before allowing the transaction to clear. This is intended to catch mistyped account digits at the POS and prevent those payments from going through.

"If I'm buying something on Amazon and put in my credit card number incorrectly by one number, it doesn't let me do the transaction. We had to get that for RTP," Alvarez said.

Good security also requires preventing RTP transactions from being delivered to scammers, as fraudsters that receive immediate funds can quickly vanish with them. Robust onboarding methods are therefore critical, and Westlake requires users to confirm their identities through a variety of official documents and details, like Social Security numbers or passports. It has even reached out to personal references in some cases.

The company also examines historical data about applicants, such as their bank account balance histories and records of overdue bill payments. Details like these are not used to assess creditworthiness but to instead get a better understanding of whether the behavioral patterns suggest legitimate customers or fraudsters. Artificial intelligence (AI) tools also help assess the many customer data points collected to determine the likelihood of fraud, Alvarez said. Should anything still go wrong, Westlake and Wells Fargo will work to quickly rectify the problem, and the issue will become another data point that the AI can use to make its fraud assessments more robust, he said.

Adopting new payments technologies is a powerful way to usher in more compelling customer experiences, but businesses must also innovate their troubleshooting and anti-fraud strategies to keep everything safe. Advanced intelligence tools, robust contingency planning and strong onboarding checks can be essential steps that pave the way for swift, secure payments.

NEWS & TRENDS

Fraud fighting

New study spotlights need to address real-time payments fraud with robust solutions

Real-time payments are compelling to consumers and banks, but some FIs in the Asia-Pacific region are concerned about how they can best secure such services. Securing real-time payments often requires different security approaches than those banks typically use to protect other types of transactions, and recent findings offer a wake-up call that reveals the importance of investing in such security upgrades. Analytics firm FICO recently released a study revealing that 78 percent of banks in the Asia Pacific believe their fraud losses increased after they introduced real-time payments platforms. Fifty-eight percent of respondents anticipated that fraud would rise "moderately" during the next 12 months, while 22 percent expected such increases to be "significant."

The crux of the issue is that banks that enable funds to move in real time are generally unable to interrupt transactions between payors and recipients once the transactions are initiated, said Dan McConaghy, FICO's Asia-Pacific president. He explained that securing real-time transfers will therefore require FIs to adopt more robust authentication measures and leverage tools like artificial intelligence (AI) to more rapidly analyze users' behaviors and detect red flags. He recommended that banks move beyond primarily authenticating customers via passwords and one-time codes and instead incorporate biometrics and device telemetry for a more thorough approach.

38 percent of finance officials say security, fraud fears inhibit greater use of digital payments

Payment fraud is also a concern in the U.S., where the pandemic has forced businesses to seriously consider digitizing at least some of their payment flows. Recent surveys of 300 high-level financial executives at U.S. firms assessed their interest in digital payments alongside barriers to greater usage. Respondents primarily hailed from firms that took in $100 million or more in annual revenues and were asked about the pandemic's impacts on their financial strategies as well as how the pandemic would affect their approaches in the new year. Delivering payments via paper check can be challenging when many employees are working from home, as it is more cumbersome for payers to print, approve and mail checks and for recipients to collect and process them. The study found that more firms are digitizing their B2B payments, but checks still hold sway in the space. Half of all respondents said that 50 percent to 89 percent of the payments they receive are digital, for example, but only 34 percent said that at least 90 percent of their client payments are digital.

38% of U.S. financial executives say fraud and cybersecurity concerns prevent greater digital payments use.

Paper-based payments are maintaining their hold in the B2B space partly because some clients are incapable of sending or receiving electronic payments. Thirty-two percent of the study's respondents said that their clients' reluctance to send money electronically prevented more robust use of digital payments, while 38 percent highlighted fraud and cybersecurity concerns. Technologies and strategies that can allay businesses' concerns about using digital payments could thus pave the way for greater uptake.

How centralized databases, ML can secure India's digital payments

India is focusing on detecting and tackling digital payments fraud as it pushes to reduce cash use and boost its Unified Payments Interface (UPI) instant payments system, which reportedly facilitated a record 1.6 billion transactions in August 2020. The nation's banks must also adequately safeguard these real-time transactions from bad actors. This could mean adapting their

fraud-fighting approaches as new payment trends — such as using UPI to facilitate low-value, everyday payments — emerge, according to Damon Madden, principal fraud consultant in payments risk management at payments system provider ACI Worldwide.

FIs often tap tools like machine learning (ML) to catch schemes, and Madden **urged** banks to share fraud-fighting information among themselves and with relevant agencies in real time. This could help FIs stay up to date about new threats and improve the data they use to train their ML tools. Madden's recommendations align with the Reserve Bank of India's (RBI's) ongoing efforts to launch a registry to gather digital payments fraud data. Banks currently **inform** the RBI's Central Fraud Monitoring Cell about fraud threats, and the bank announced in 2019 that it aimed to create a Central Payment Fraud Registry focused on payments-related crime as part of its Payment System Vision 2021 plans. Madden **encouraged** continuing and expanding such initiatives.

New and forthcoming systems

Brazilians see faster options in new PIX rail and anticipated WhatsApp Pay launch

Brazil's recently launched PIX real-time payments system is reportedly gaining traction, having been **rolled out** on Nov. 3 and amassing 100 million **registered** user accounts within a month. Users appear largely satisfied with the system as well, with a late November **study** of 2,000 Brazilians finding that 60 percent **believed** they would prefer using PIX instead of using two of the country's other transfer services that provide only same-day and next-day settlement. The PIX 24/7 year-round, real-time payment system is also likely to **appeal** to Brazil's many unbanked and underbanked consumers, who can use it to make transactions from mobile wallets without needing to have bank accounts, said Ralf Germer, CEO and co-founder of PagB."asil, a payments processing provider that serves international eCommerce platforms and retailers selling into Brazil.

The pandemic could also prompt growth in the adoption of other mobile payment forms in Brazil. The nation's consumers are warming to the use of digital wallets, and the country's launch of WhatsApp Pay — originally expected to go live in June 2020 — is expected to be underway soon.

Barbados' Finance Ministry plans rapid digital payment system for late 2021

Not all countries have rapid payment systems, but some nations are looking to change that. The pandemic has made digital payments and banking options must-haves in Barbados, according to recent statements from its finance minister Ryan Straughn. Stakeholders have been working on a digital payments system for two years, and the service is expected to debut later this fall. Straughn described the service as an automated clearing house (ACH) that would operate in real time and stated that all eight of the country's major FIs are expected to participate. The island also aims to modernize its financial system by launching a credit reporting system that will help small to mid-sized businesses (SMBs) better demonstrate their creditworthiness to banks. Straughn said a third initiative would support digital banking, which could make it easier for SMBs and microbusinesses to transact with FIs and government entities and grow their operations.

Making greater use of instant payments

Partnership between FinTech and payments provider helps Australian merchants accept real-time payments

Businesses and payment processors are also looking for ways to get more use out of existing rapid payment methods. A new partnership aims to help Australian shoppers purchase from eTailers via the country's real-time payments system, the New Payments Platform (NPP). The collaboration would ensure that consumers can shop without keying in payment card details at checkout and enable merchants to receive payments that settle instantly and are safe from chargebacks. AzuPay — a FinTech that facilitates consumer-to-business (C2B) payments via the NPP — teamed up with Asia-focused digital payments solutions provider AsiaPay on the initiative, with the latter

helping to expand the former's merchant base. AzuPay will provide the necessary PayID credentials that allow customers to send merchants funds using the NPP while also giving retailers new, single-use PayIDs and QR codes for each transaction.

Why 2021 could be the year real-time disbursements go mainstream

Disbursements are also undergoing a faster payments upgrade, one disbursements platform CEO said in a recent PYMNTS interview. Most consumers would choose to receive disbursements immediately if given the chance, said Ingo Money CEO Drew Edwards, and banks and large businesses have begun embracing this need. This marks a major shift from the days in which sending funds to consumers involved staff calling up customers to request their debit card details and then processing refunds onto those cards, the CEO said. This left many consumers waiting vigilantly for funds to show up, and they would have to call companies back within a day or two if the money did not arrive.

These trends are changing as more FIs and businesses collaborate with FinTechs to make their disbursements digital and rapid. The CEO predicted that firms are likely to accelerate their disbursements this year and that immediate payments will become widespread as more companies regard convenient disbursements as a competitive necessity.

Nacha team to release resources helping corporates understand, react to real-time payments

The ever-increasing number of payments modernizations can be confusing for FIs and businesses, and some need help keeping pace with the space's many changes. Nacha — the entity that sets the rules for the Automated Clearing House networks in the U.S. — has worked in recent years to help FIs and businesses determine which faster payments methods are available to them, and it has recently begun developing a new set of resources to boost this effort. FIs and corporates may struggle to determine whether they would benefit from using Same-Day ACH, The Clearing House's RTP® network or other options to suit their needs, and Nacha aims to assist.

The Payments Innovation Alliance group — a Nacha organization that comprises stakeholder representatives from across the finance and payments industries — debuted the Faster Payments Project Team in 2018 to clear up confusion surrounding rapid payment methods. The team has been charged with delivering resources to help FIs and companies better plan their payment strategies. It has released an information packet geared toward familiarizing small and mid-sized FIs with faster payments options, for example, and it offers online resources to assist FIs of all sizes with learning and planning. The Faster Payments Project Team recently turned its educational efforts toward non-FIs and is reportedly working on a resource to help companies better understand how the space is changing and how these shifts may affect them. The team plans to release the Faster Payments Playbook for Corporates during the first half of this year.

DEEP DIVE

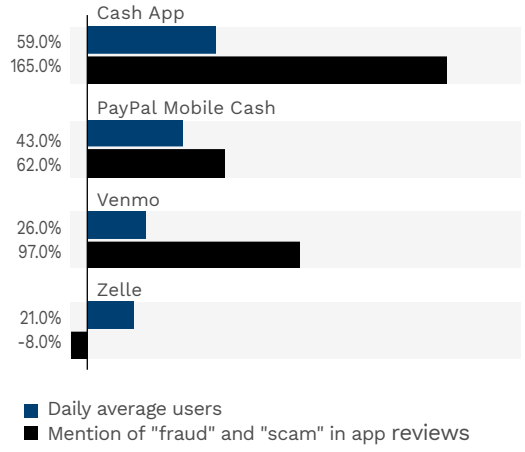
How P2P Payment App Providers Can Tackle Rising Fraud

More consumers are turning to digital methods to pay friends and retailers during the global health crisis. Shoppers are looking to avoid exchanging cash and cards in person and are instead choosing contactless transactions or remote purchase options. This trend has created myriad opportunities for P2P payment apps like Venmo and Zelle, which allow consumers to quickly, simply and digitally transfer funds to merchants and friends.

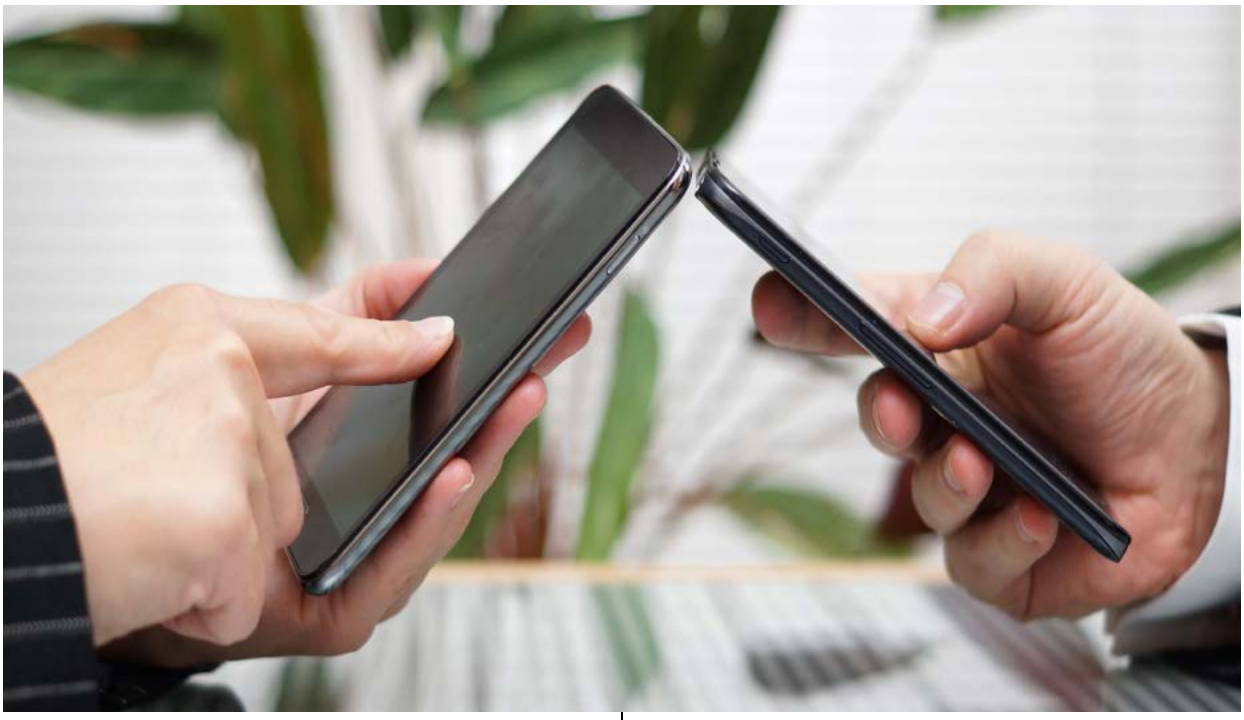
These app-based transactions must be adequately secured to enable consumers to take full advantage of their benefits, however. P2P payments providers have their work cut out for them in this regard as cybercriminals have ramped up their attacks during the pandemic. This month's Deep Dive examines the fraud challenges that real-time P2P payment apps face and the strategies these services can use to mitigate such threats.

P2P scams

Shoppers are leaning more heavily on P2P apps during the pandemic, prompting fraudsters to do the same. *The New York Times* recently reported that, even as Venmo's daily user count rose 26 percent over the past year, the number of customer reviews that included the words "fraud" or "scam" rose at almost four times that rate. These two trends suggest that such payment services are continuing to draw attention from both legitimate users and bad actors.



Source: Apptopia - Note: Change from 2019 to 2020. *The New York Times.*



Many P2P app providers are thus highly concerned with finding ways to serve consumers while thwarting bad actors, but the security challenges present in these payment services are no small issue. More than 70 percent of U.S. adults in a recent **survey** said that they use such apps, partly because the apps allow them to **send** funds immediately — an appealing option compared to transactions that take several days to complete. These quick transfers give payments services providers smaller time frames during which they can review and stop the movement of funds if something is amiss, however. Scammers often seek to capitalize on real-time payment services' irreversibility, typically by setting up P2P app accounts and tricking victims into sending funds that are impossible to reclaim. Consumers who use these apps to send money to people they do not know risk routing the funds to fraudsters.

Cybercriminals take advantage of consumers' trust by soliciting funds under dishonest pretenses. Some **pretend** to be tax officials and insist that their targets must send funds via the apps, for example. Other scams occur when fraudsters post Craigslist ads claiming that they are selling items and demanding upfront payment via P2P apps. They then abscond with the funds without delivering the goods. Consumers who fall prey to these schemes are unable to file chargebacks and receive refunds, unlike with credit cards. Many consumers do not know that they should avoid sending money to unfamiliar parties with the apps, and 47 percent of respondents in a 2019 **survey** said they had used P2P apps to send money to strangers in response to classified ads on Craigslist and other sites. Fifty-three percent reported using such apps to pay unknown sellers they met on bidding platforms like eBay.

P2P app providers are striving to get ahead of these problems by educating consumers about the risks involved in such transactions. Some apps now feature pop-up alerts that warn users of the risks they face when sending funds to recipients they do not know, for example. Other app providers have moved away from enabling one-click transactions and instead prompt users to review their payments before hitting send, giving customers time to examine their choices, check for errors and confirm the details.

Keeping fraudsters from using real-time payment services to con legitimate customers can entail preventing bad actors from entering the space in the first place. App providers must be able to detect when users might be leveraging false identities during onboarding. Scammers often try to create accounts using stolen credentials or synthetic IDs that have been cobbled together using personally identifiable information lifted from multiple victims. Payments providers can lean on banking partners to vet customers while also boosting their efforts to catch bad actors who slip through by leveraging AI-powered tools to detect abnormal user behaviors that could indicate fraud.

ATOs, and how P2P apps can fight back

Real-time payments providers also need to safeguard honest customers from cybercriminals who might seize control of their accounts. Fraudsters who gain access to these accounts can steal the funds they store on the apps or siphon off money from any bank or card accounts linked to them. Some cybercriminals may try to leverage usernames and passwords that were stolen in data breaches or purchased on the dark web to log into customers' apps. Others apply brute force techniques that rely on malicious bots to automatically plug various usernames and passwords into login screens and hope they hit the correct combinations.

P2P app providers are far from powerless when it comes to stopping ATO attacks, however. A simple first step is to encourage customers to use unique passwords when signing up, reducing the likelihood that their account details will be compromised should a different company fall victim to a data breach. A recent study found that only 37 percent of Canadian bank customers use different passwords for each of their accounts, with 22 percent recycling two to five passwords across various accounts. Reusing passwords is risky because hackers can use compromised login details from other breaches to access additional accounts. App providers may therefore need to put in dedicated effort to educate customers about the importance of changing their habits.

Payment companies can also monitor for sudden and rapid rises in unsuccessful login attempts, which could indicate that brute force attempts are underway. P2P app providers could even take security a step further and implement multifactor authentication (MFA) to ensure that stolen password and username combinations alone would not be enough to give criminals access to customers' accounts. P2P apps that implement MFA require customers to present at least one additional layer of authentication to validate their identities.

Many consumers recognize that real-time P2P payments can remove frictions from their transaction experiences and make paying swift and easy. Enabling customers to enjoy the benefits of such offerings also requires app providers to ensure that security is top-notch. The right fraud-frighting approaches can help P2P payments providers keep transactions moving quickly while halting fraud.

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

ABOUT

PYMNTS.com

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 in which companies in payments share relevant information about the initiatives that shape the future of this dynamic sector and make news. Our data and analytics team includes economists, data scientists and industry analysts who work with companies to measure and quantify the innovation that is at the cutting edge of this new world.

The Clearing House

The Clearing House operates U.S.-based payments networks that clear and settle funds through ACH, check image, the RTP® network and wire transfers. The RTP network supports the immediate clearing and settlement of payments along with the ability to exchange related payment information across the same secure channel.

Learn more at **www.theclearinghouse.org**.

REAL-TIME

PAYMENTS TRACKER®

DISCLAIMER

The Real-Time Payments Tracker® may be updated periodically. While reasonable efforts are made to keep the content accurate and up to date, PYMNTS.COM: MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, REGARDING THE CORRECTNESS, ACCURACY, COMPLETENESS, ADEQUACY, OR RELIABILITY OF OR THE USE OF OR RESULTS THAT MAY BE GENERATED FROM THE USE OF THE INFORMATION OR THAT THE CONTENT WILL SATISFY YOUR REQUIREMENTS OR EXPECTATIONS. THE CONTENT IS PROVIDED" "AS IS" AND ON AN "AS AVAILABLE" BASIS. YOU EXPRESSLY AGREE THAT YOUR USE OF THE CONTENT IS AT YOUR SOLE RISK. PYMNTS.COM SHALL HAVE NO LIABILITY FOR ANY INTERRUPTIONS IN THE CONTENT THAT IS PROVIDED AND DISCLAIMS ALL WARRANTIES WITH REGARD TO THE CONTENT, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT AND TITLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES, AND, IN SUCH CASES, THE STATED EXCLUSIONS DO NOT APPLY. PYMNTS.COM RESERVES THE RIGHT AND SHOULD NOT BE LIABLE SHOULD IT EXERCISE ITS RIGHT TO MODIFY, INTERRUPT, OR DISCONTINUE THE AVAILABILITY OF THE CONTENT OR ANY COMPONENT OF IT WITH OR WITHOUT NOTICE.

PYMNTS.COM SHALL NOT BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND, IN PARTICULAR, SHALL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE, OR LOSS OF USE, ARISING OUT OF OR RELATED TO THE CONTENT, WHETHER SUCH DAMAGES ARISE IN CONTRACT, NEGLIGENCE, TORT, UNDER STATUTE, IN EQUITY, AT LAW, OR OTHERWISE, EVEN IF PYMNTS.COM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME JURISDICTIONS DO NOT ALLOW FOR THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, AND IN SUCH CASES SOME OF THE ABOVE LIMITATIONS DO NOT APPLY. THE ABOVE DISCLAIMERS AND LIMITATIONS ARE PROVIDED BY PYMNTS.COM AND ITS PARENTS, AFFILIATED AND RELATED COMPANIES, CONTRACTORS, AND SPONSORS, AND EACH OF ITS RESPECTIVE DIRECTORS, OFFICERS, MEMBERS, EMPLOYEES, AGENTS, CONTENT COMPONENT PROVIDERS, LICENSORS, AND ADVISERS.