



PYMNTS

The Clearing House

April/May 2023

# Fighting Fraud in Real-Time Payments

Real-Time Payments Tracker® Series

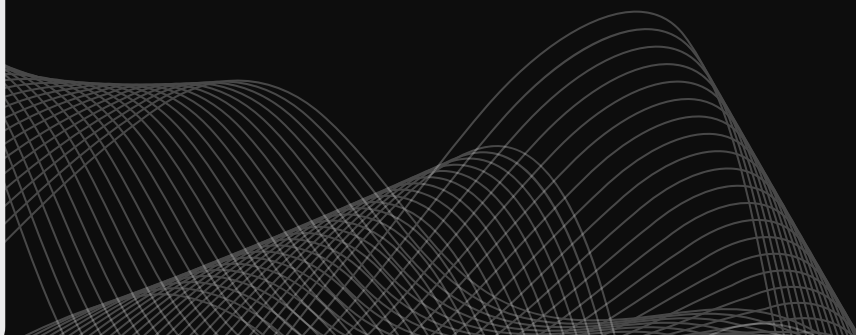
Read the previous edition



APRIL 2023

Real-Time Payments Tracker® Series

- Real-Time Payments' Unique Fraud Prevention Portfolio **P. 04**
- PayPal Data Breach Exposes 35,000 Users' Data **P. 10**
- How Fraud Damages P2P Payment Organizations **P. 14**
- Fraud Not Hindering Real-Time Payments' Growth **P. 28**



# What's Inside

## 04 Real-Time Payments' Unique Fraud Prevention Portfolio

The FTC reported the amount lost to fraud in 2022 at \$8.8 billion, an increase of more than 30% from the year before.

## 10 Attempted Fraud Transactions Spiked by 92% Last Year

The number of attempted fraud transactions skyrocketed by 92% between 2021 and 2022, with attempted fraud dollar amounts spiking by a massive 142%.

## 14 How Fraud Damages P2P Payment Organizations

PYMNTS examines the economic and reputational harm fraud can wreak on P2P applications and how technological solutions can keep fraud to a minimum.

## 20 Organizations Face Challenges in Combating Fraud

Complex regulatory requirements were the top challenge, cited by two-thirds of FIs, according to a recent PYMNTS study.

## 22 An Insider Details the Best Protections Against Push Payment Fraud

Lee Kyriacou, vice president of real-time payments at The Clearing House, discusses how a mix of technology and consumer education can effectively fight push payment fraud.

## 26 PayPal Introduces Passkeys for Android Smartphones

User authentication is critical to improving cybersecurity, but most companies rely on weak, knowledge-based verification measures.

## 28 Real-Time Payments to Grow by More Than 31% Annually Through 2027

The looming threat of fraud is doing little to hinder the long-term outlook for real-time payments.

## 30 About

Information on PYMNTS and The Clearing House

PYMNTS



### Acknowledgment

The Real-Time Payments Tracker® Series is produced in collaboration with The Clearing House, and PYMNTS is grateful for the company's support and insight. PYMNTS retains full editorial control over the following findings, methodology and data analysis.

## Need to Know

---

# Real-Time Payments' Unique Fraud Prevention Portfolio

Fraud is top-of-mind for payment providers as well as the businesses and consumers they serve — for the simple reason that the cost of ignoring it is too much to bear. A recent report from the Federal Trade Commission (FTC) [pegged](#) the amount lost to fraud in 2022 at \$8.8 billion, an increase of more than 30% from 2021.

Not all types of fraud are created equal, however, and one of the most important differentiators is the type of payments they target. Consumers or businesses entering into relationships with payment providers must be aware of the types of fraud to which they may be exposed so they can hold their providers accountable for fraud prevention.

Payments fraud is a serious threat to consumers and businesses alike.



**\$8.8B**

Consumer [losses](#) to fraud in 2022



**2.4M**

Number of consumers who [submitted](#) fraud reports to the FTC in 2022


## Need to Know

---

# Credit push payments are inherently safer than debit pull payments.

The core difference between the two methods is that credit push transactions involve payers instructing their banks to send money from their accounts to recipients' accounts, whereas debit pull transactions have recipients' banks extract money from payers' accounts. Common types of pull payments include debit cards and paper checks, while push payments are used for peer-to-peer (P2P) services and direct deposits.

Push payments are largely considered far safer than pull payments and are the type used by real-time payment systems around the world, including the RTP® network in the United States and the Faster Payment System in the United Kingdom. Unlike pull payments, they often do not require payers to disclose sensitive information such as bank account numbers to recipients.



**Push payments are widely used by customers via P2P payment apps.**

**84%**

Share of customers who have used P2P services

**44%**

Portion of consumers who use P2P services at least once per week

## Need to Know

---

# Push payments are not invincible, however.

Push payment customers are still potentially vulnerable to social engineering scams, in which bad actors trick users into sending them money by posing as trusted confidants or companies with which the victim does business. A recent [survey](#) found that half of companies have reported fraud related to faster payments, largely due to social engineering.

Push payments can limit the damage caused by social engineering schemes, however, as customers must still approve every payment rather than giving bad actors unrestricted access to their accounts. Nevertheless, both payment providers and customers must remain vigilant to protect against the existing threat.

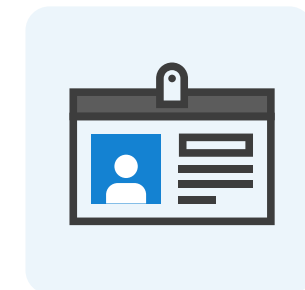
Faster payment providers have experienced many types of fraud.



**45%**  
Account takeover/  
social engineering



**27%**  
Scams



**18%**  
Stolen  
credentials

## News and Trends

---

# Attempted Fraud Transactions Spiked by 92% Last Year

Fraud is a massive problem in the payments industry, and the threat level is only rising. A recent [report](#) found that the number of attempted fraud transactions skyrocketed by 92% between 2021 and 2022, with attempted fraud dollar amounts spiking by a massive 142%. This fraud was not limited to a single channel, instead affecting a variety of different payment methods.

Some of the most pressing threats were account takeover fraud, attempted authorized payment fraud and new account fraud. Experts attribute this rise in fraud to the increasing popularity of digital payments, which offer a greater opportunity to remote bad actors than traditional cash transactions.



## News and Trends

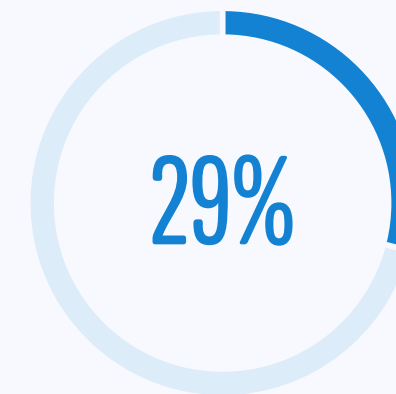
### PayPal data breach exposes 35,000 users' data

Data breaches are one of the worst fears of any company. P2P payment app PayPal recently [admitted](#) that it fell victim to a breach in December 2022 that compromised the personal data of more than 35,000 users, with the leaked data including names, bank account numbers and Social Security numbers.

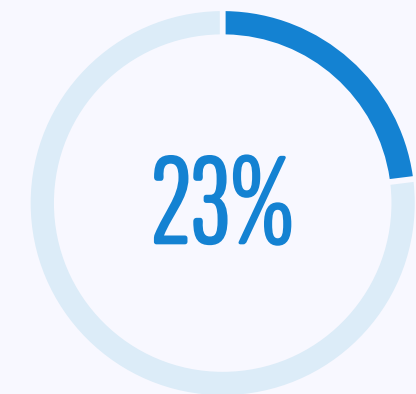
Although PayPal offered free credit monitoring and identity theft protection services to victims, some users filed a class action lawsuit against the company for negligence. The suit also sought unspecified damages for invasion of privacy, unfair business practices and breach of contract and implied warranty.

### Bankers identify P2P fraud and data breaches as top digital threats

Fraud comes in many different forms, but some are bigger threats than others. A recent [survey](#) of bank executives pinpointed P2P and other digital fraud as the top threat, with the four biggest U.S. banks having recently reported more than 190,000 scams in which bad actors tricked victims over Zelle. The second-most widely feared threat was data breaches, which affected more than 9 million consumers last year. Other top threats included ransomware and third-party vendor breaches.



**Portion of bankers that report P2P and digital fraud as top cybersecurity threat**



**Portion of bankers that report data breaches as top cybersecurity threat**

## PYMNTS Intelligence

---

# How Fraud Damages P2P Payment Organizations

Fraud is a constant worry for companies of all types, driven by the sheer variety of different fraud methods that bad actors deploy. Man-in-the-middle attacks, social engineering, account takeovers and botnets are just some of the thousands of different types of fraud that keep CEOs up at night — and the bad actors' techniques are only growing more sophisticated by the day.

The damage fraud can cause is not limited to companies' finances and data: It can also impact their reputations. This month, PYMNTS examines the economic and reputational harms fraud can wreak on P2P applications and how technological solutions can keep fraud to a minimum.





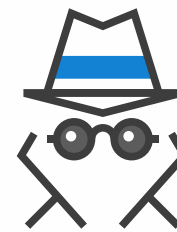
## PYMNTS Intelligence

# P2P fraud costs more than stolen funds

A recent [report](#) filed by U.S. Sen. Elizabeth Warren (D-MA) — based on data from four different banks partnered with P2P payment app Zelle — found that losses to P2P payment fraud hit \$255 million in 2022. These funds were lost due to more than 192,000 cases of scams and represented a massive increase from the \$90 million in fraud reported in 2020.

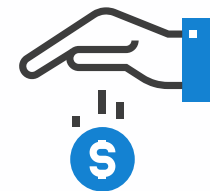
Banks reimbursed the customers in just 3,500 of these cases, the report further [found](#), and only 47% of the funds were returned even when they were withdrawn without customer authorization. This not only forced millions of customers to eat their losses: It also could cost the banks involved much more in the long run than if they had simply compensated the victims.

**P2P payment fraud is a growing problem that costs customers millions.**



## \$255M

**P2P payment fraud losses reported in 2022**



## \$90M

**P2P payment fraud losses reported in 2020**

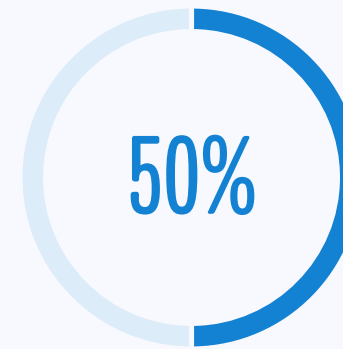
This is because customers are far less likely to do business with an organization with a reputation for fraud. [Studies](#) have found that every dollar lost to fraud ultimately costs companies \$3.75, thanks in part to customers switching to competitors after being victimized by fraud on their platforms. If victims then warn their peers against using the entities involved, the potential opportunity cost in lost business is all but incalculable.

## PYMNTS Intelligence

# Regulation and technology are critical to limiting P2P fraud's impact

The U.S. is exploring several options to tackle this fraud and protect consumers. Lawmakers are [urging](#) the Federal Reserve, the Federal Deposit Insurance Corporation, the National Credit Union Administration and the Office of the Comptroller of the Currency to examine the reimbursement and anti-money laundering policies of P2P networks and impose penalties on companies that do not adequately protect consumers.

Individual businesses need to take the initiative to protect their customers and avoid potential regulatory penalties. Many payment processors have already improved their fraud prevention capabilities, with 50% [increasing](#) their use of real-time fraud decisioning and alerts, 40% investing in artificial intelligence



**Share of payments providers investing in real-time fraud decisioning**



**Share of payments providers investing in artificial intelligence**



**Share of payments providers improving authentication techniques**

and machine learning and 30% improving their customer authentication methods. While fraud will likely never be eliminated, steps such as these go a long way toward protecting customers.

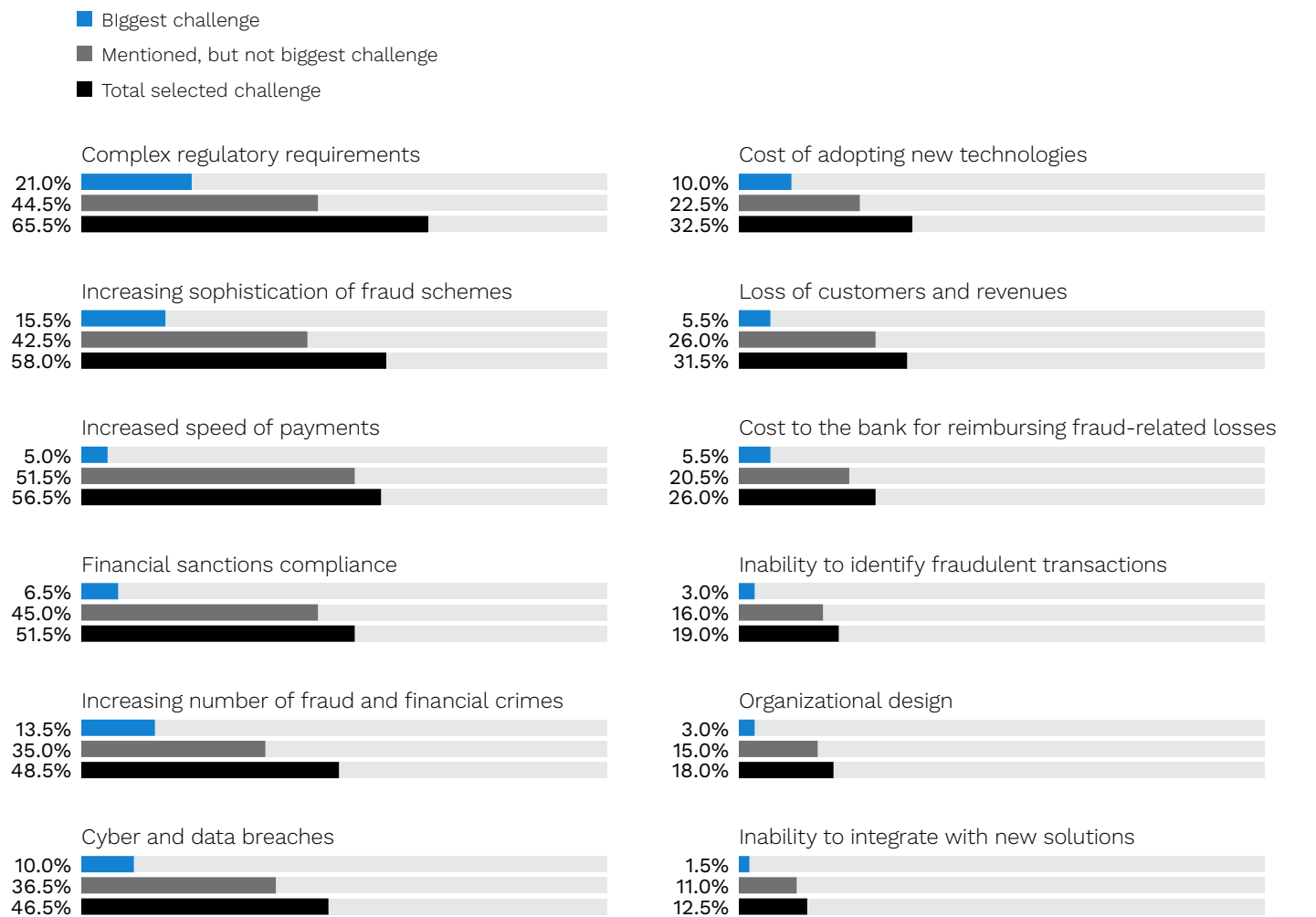
Chart of the Month

# Organizations Face Challenges in Combating Fraud

Nearly every organization can agree that preventing fraud is a good thing, but if it were easy, fraud would barely exist at all. A recent PYMNTS [study](#) detailed the challenges FIs face in their fraud prevention strategies, with complex regulatory requirements the top hurdle cited, at 66%. Government entities have strict regulations surrounding fraud prevention, typically to prevent false positives and ensure that defendants’ legal rights are met, but these can add to the difficulty of fraud prevention as well. Increasing fraud sophistication, increased payment speed and cost of fraud prevention technology were other common factors that complicate fraud prevention.

## Challenges encountered in combating fraud and financial crimes

Share of FIs that reported facing select challenges in the preceding year, by perceived level of challenge



Source: PYMNTS  
 The State of Fraud and Financial Crime in the U.S., September 2022  
 N = 200: Complete responses, fielded April 29, 2022 – June 3, 2022

## Insider POV

---

# An Insider Details the Best Protections Against Push Payment Fraud



**LEE KYRIACOU**  
Vice president of  
real-time payments



“Fraudsters want to get paid in a way that’s fast and final. Well, guess what? Real-time systems are fast and final. So banks and credit unions need to continue to educate customers about account security and use best practices to protect accounts.”

PYMNTS interviews Lee Kyriacou, vice president of real-time payments at [The Clearing House](#), about how a mix of technology, account holder education and security best practices can effectively fight push payment fraud.

Push payments are typically considered much more secure than their pull payment counterparts, but they are far from invincible. While it is much more difficult for bad actors to pilfer funds with stolen information, they can still perpetrate scams and account takeovers to deceive victims into sending payments.

“The payer says, ‘Wait a minute; the payee duped me.’ The biggest problem in push payments is what I call payee scams or receiver scams, where the receiving side has somehow fooled the sender side into making the payment and authorizing that the payment be made.”

## Insider POV

---

**Banks and payment providers looking to combat push payment scams need to deploy data-driven solutions to prevent their customers from being victimized.** Scammers typically operate at high volume when targeting individuals, so having some way of determining which accounts are receiving large numbers of P2P payments will be crucial for identifying these bad actors and shutting them down.

“Banks can look at [things such as] how many times has there been a fraud report for this receiver? How many transactions has this receiver had in the last 24 hours compared to a month ago? When was the first time this receiver got a payment on the network? Then you’re starting to provide them information [from which] a sending bank can then figure out [whether this is] a typical receiver for this customer or not.”

**Regulatory measures also need to be put into place to protect P2P payment providers and their customers from various forms of push payment fraud.** While pull payment scam victims are typically required to be made whole in most jurisdictions, this can be much more of a gray area for push transactions. Although some form of consumer protection is necessary, customers also need to take responsibility for their own fraud awareness.

“Regulation can be helpful, but some amount of liability has to lie [with] the sender of the payment. Banks need to continually educate account holders about account security best practices, such as using complex passwords, two-factor authentication and providing prompts to payers such as ‘Are you making this payment to someone you know? This payment is irrevocable.’”



## Companies to Watch

---

# PayPal Introduces Passkeys for Android Smartphones



User authentication is a critical method for improving cybersecurity, but most companies rely on weak, knowledge-based verification measures. PayPal is taking steps to combat this by [introducing](#) its passkey system to Android devices, which replaces passwords with cryptographic key pairs and digital credentials. These are much more resistant to phishing, credential stuffing and other remote attacks than passwords. PYMNTS research has found that 61% of consumers are willing to use non-password login methods and 45% are very comfortable with using non-password login methods, making the switch to passkeys a natural fit for most customers. PayPal has already introduced passkeys on iOS devices, but it remains to be seen how much fraud levels will drop as these systems grow more widespread.



## What's Next

---

# Real-Time Payments to Grow by More Than 31% Annually Through 2027

The looming threat of fraud is doing little to hinder the long-term outlook of the real-time payments field, with experts [predicting](#) an increase in the market of more than \$55 billion between 2022 and 2027. This equals a compound annual growth rate of more than 31%, spurred by increased adoption of smartphones and high-speed internet around the world. Although fraud has not hampered this growth yet, organizations within the real-time payments industry will nonetheless need to stay vigilant about cybersecurity to ensure that fraud remains in check.

“Prevention of scams involving real-time payments requires ongoing education of payers and putting in ‘friction’ before a payment is made, such as pop-up notices that say ‘Make payments only to those you trust’ or ‘Payments are final.’”

**LEE KYRIACOU**

Vice president of  
real-time payments

 The Clearing House



# About

**PYMNTS** [PYMNTS](#) 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](#) 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](http://www.theclearinghouse.org).

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

# Disclaimer

The Real-Time Payments Tracker® Series may be updated periodically. While reasonable efforts are made to keep the content accurate and up to date, PYMNTS 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 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 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 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 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 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.

Components of the content original to and the compilation produced by PYMNTS is the property of PYMNTS and cannot be reproduced without its prior written permission.

The Real-Time Payments Tracker® Series is a registered trademark of What’s Next Media & Analytics, LLC (“PYMNTS”).