

PYMNTS
INTELLIGENCE

INGO Payments

January 2025

Checks at Risk: How Paper Payments Weaken Fraud Prevention

Money Mobility Tracker® Series

Despite advances in digital payment technologies and cybersecurity, check fraud remains a persistent threat to businesses and consumers, causing significant financial losses. The ongoing prevalence of this age-old crime underscores the critical need for more secure and efficient digital payment alternatives.

■ Read the previous edition



DECEMBER 2024/JANUARY 2025

Money Mobility
Tracker® Series

What's Inside

04 Introduction

The growing prevalence of check fraud underscores the urgent need to reduce businesses' and individuals' reliance on checks as a payment method.

06 Paper Checks Remain Popular for B2B Payments

Despite their well-documented security vulnerabilities, paper checks represent a larger-than-expected share of B2B payments.

10 Check Payments Are Susceptible to Fraud

Even with the growing industry shift toward digital payments, checks remain a critical weak link in the fraud prevention chain.

16 Leveraging Digital Rails to Secure Transactions

Digitizing payments could prove exceptionally useful not only toward reducing check fraud but also accelerating payment speed.

20 Transitioning From Paper Checks to Digital Payments

Digital payment methods offer robust security solutions that significantly reduce fraud risks and enhance financial protection, making it essential to transition away from paper checks as quickly as possible.

22 About

Information on PYMNTS Intelligence and Ingo Payments

PYMNTS
INTELLIGENCE

INGO Payments

Acknowledgment

The Money Mobility Tracker® Series is produced in collaboration with Ingo Payments, and PYMNTS Intelligence is grateful for the company's support and insight. [PYMNTS Intelligence](#) retains full editorial control over the following findings, methodology and data analysis.

Introduction

Check fraud remains a persistent and growing issue for both businesses and consumers. According to a recent survey, nine in 10 bankers have experienced higher levels of [check fraud](#) in recent years, with 28% of banks noting an increase of more than 50% in the past three years. Smaller banks have been hit especially hard. Check fraud takes many forms, including forgery, kiting, physical theft, counterfeiting and overpayments. Alarming, this surge in check fraud comes at a time when overall check use is declining, increasing the odds that any given check payment will encounter fraud.

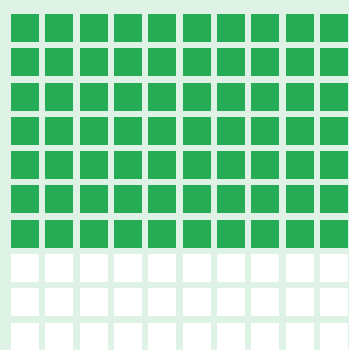
The most effective way to bring the check fraud crisis to heel is to reduce businesses' and individuals' reliance on paper checks as a payment method. Newer digital payment options not only allow for more secure transactions but also facilitate faster and more convenient payments. Therefore, financial leaders must prioritize adopting digital payment systems to mitigate check fraud and prevent an erosion of consumer trust in their ability to safeguard transactions.



Paper Payments Persist

Paper Checks Remain Popular for B2B Payments

Despite their well-documented security vulnerabilities, paper checks account for a significant share of business-to-business (B2B) payments. Current trends suggest that their use is unlikely to decline meaningfully in the near future.



70% of organizations using check payments have no plans to discontinue their use in the next two years.



Paper Payments Persist

Most companies continue to use checks for B2B payments.

In 2023, 68% of companies in the United States used checks for [B2B payments](#), up slightly from 65% in 2022. Among very small businesses, this figure was even higher, reaching 79%. All told, checks account for nearly 40% of all U.S. [B2B payment volume](#). This trend shows little sign of changing. Of the 75% of organizations using check payments, 70% reported having [no plans](#) to discontinue them in the next two years.

Despite advances to digital payment methods like real-time rails, businesses tend to stick with what they know rather than adopt new and perceived-to-be-untested alternatives. While this approach helps them avoid expensive digital overhauls in the short term, the persistent risk of check fraud could drive a shift in attitudes down the line.

Checks are not as cost-effective as many businesses believe.

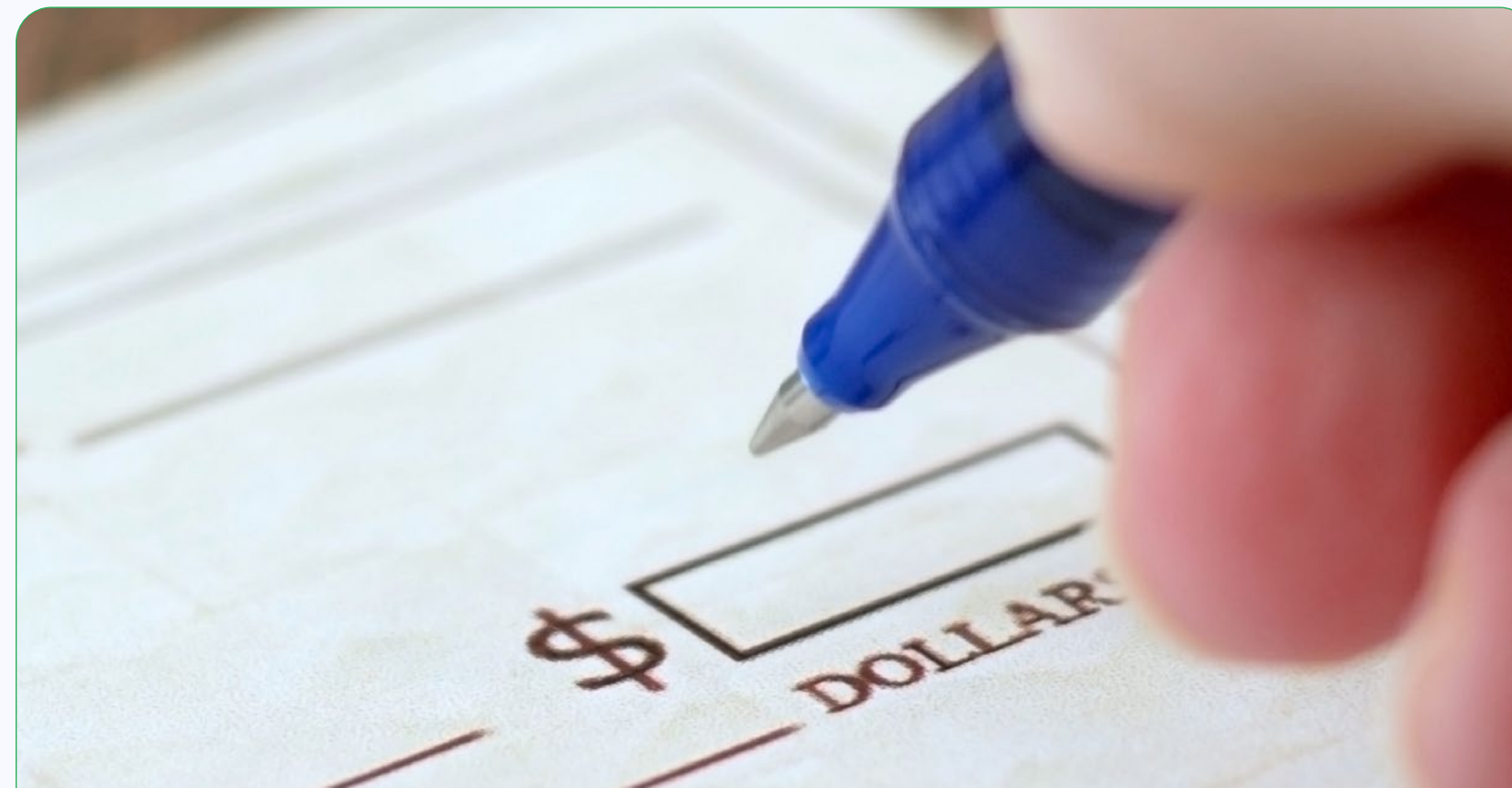
Many businesses rely on checks under the assumption that they are free or inexpensive to process, obviating the need for costly system upgrades to support digital payments. However, this is a misconception. According to Rebecca Schultz, Chief Marketing Officer at Boost B2B Payment Solutions, [manual check processing](#) often incurs hidden costs, including time, labor and delayed payment cycles — not to mention losses from potential check fraud.

Furthermore, manual processes — such as those associated with paper checks — can also hinder digital systems if digitization is not embraced fully. If any part of the process remains manual, such as suppliers physically cashing checks, then the advantages of digital transformation and the value of the data exchange are diminished. As Schultz explained in an interview with PYMNTS Intelligence, “You can digitize the payment, but if the receiver is turning it into cash and manually entering the data, then the value of that exchange has ended.”

Check Fraud Runs Rampant

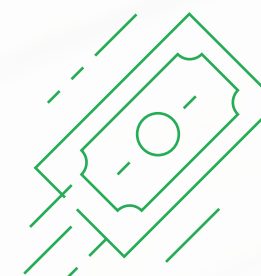
Check Payments Are Susceptible to Fraud

Despite a growing industry shift toward digital payments, checks remain a critical weak link, leaving businesses vulnerable to significant financial losses from fraudulent transactions.

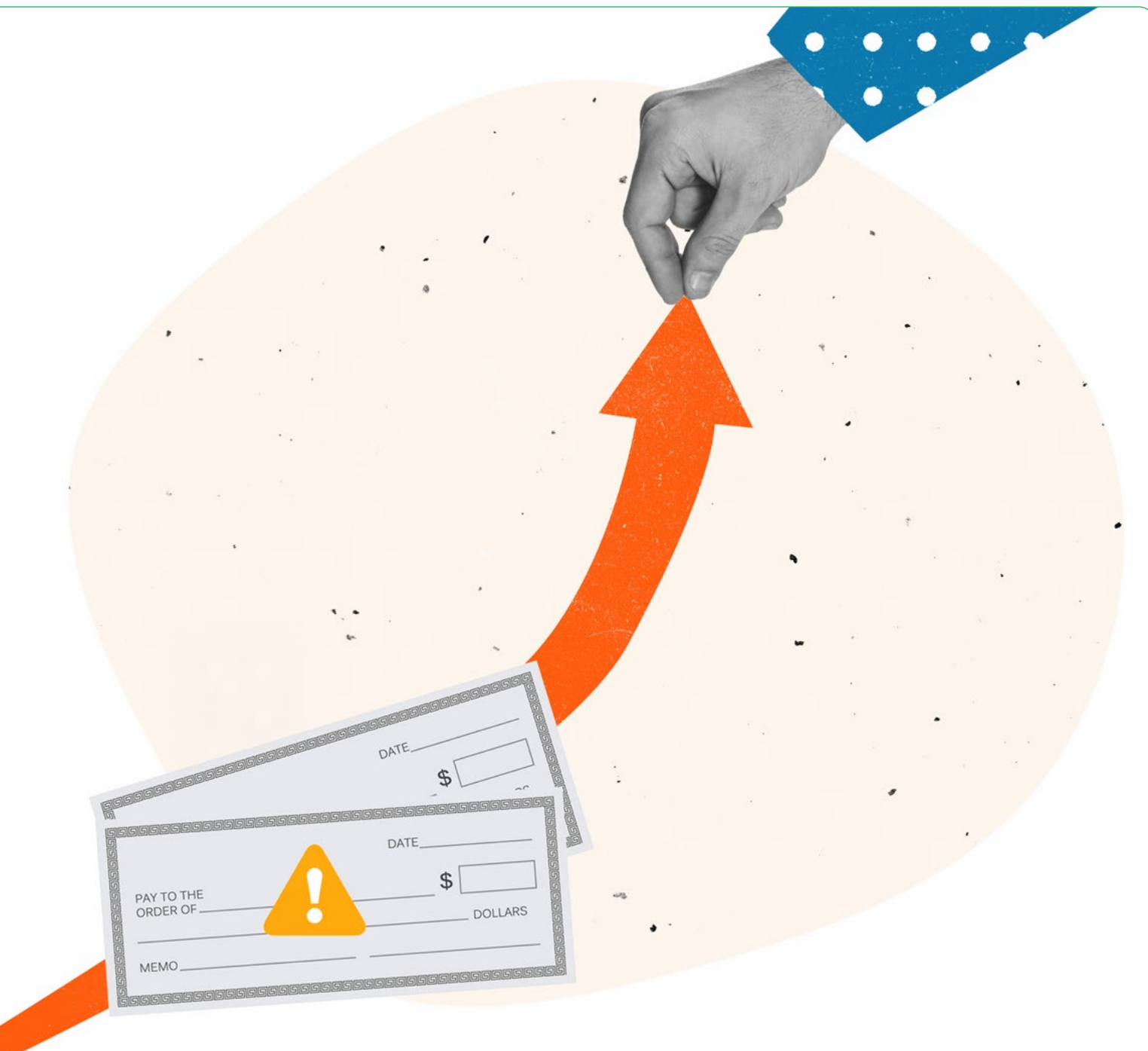


\$24B

Estimated losses from **check fraud** in 2023



Check Fraud Runs Rampant



Check fraud is a booming business.

A September 2024 study by the [Financial Crimes Enforcement Network](#) (FinCEN) revealed that an alarming 15,417 Bank Secrecy Act (BSA) reports filed over a recent six-month period in 2023 were linked to mail theft-related check fraud, representing \$688 million in transactions. One expert estimated that total losses from [check fraud](#) could reach \$24 billion in 2023 — roughly twice the amount recorded five years before. This surge is due in large part to the ease with which checks can be exploited and the [difficulty of detection](#). In many instances, committing check fraud is as simple as stealing checks from mailboxes or physically altering their amounts. Fraudsters also counterfeit checks or post stolen check details to online platforms notorious for facilitating criminal activity, such as Telegram, enabling other bad actors to exploit victims' personal information.

Check fraud is difficult to detect due to the lack of a [centralized system](#) for tracking checks. Banks have no way of determining whether a specific check has been accepted or deposited elsewhere, which makes it challenging to prevent duplicate check fraud, for example. Detecting check fraud often requires visible examinations and manual comparison to identify forgeries. Given the [hundreds of millions](#) of checks processed annually, banks lack the resources to inspect each check individually. As a result, it can be quite some time before fraud is discovered.

Check Fraud Runs Rampant

SMBs are more likely to be affected by check fraud.

According to a 2024 survey, nearly one quarter of small to mid-sized businesses (SMBs) fell victim to [check fraud](#), compared to just 15% of the general population. The stakes are also higher for SMBs, as they often deal with larger sums of money relative to their size and spend more time resolving fraud cases. Roughly 86% of SMBs spent at least one hour addressing fraud issues in 2024, surpassing the 75% rate among general consumers. For SMBs with limited staff, this time commitment can be especially detrimental, potentially bringing operations to a standstill and forcing owners to focus on resolving the fraud instead of running their businesses.

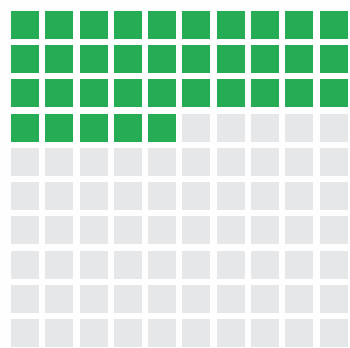


SMBs' higher reliance on checks may contribute to their increased vulnerability to fraud. Half of SMBs write six or more checks annually, compared to just 32% of the general population. However, it should be noted that SMBs demonstrate a greater awareness of check fraud prevention technologies, with 66% being knowledgeable in this area. They also show more initiative in educating themselves about check fraud prevention, with half participating in educational sessions or workshops offered by their financial institutions (FIs).

Securing Transactions

Leveraging Digital Rails to Secure Transactions

As check fraud continues to rise, risk reduction has become a top priority for financial leaders. Digitizing payments offers the dual advantage of enhancing security and accelerating payments.



35%

of firms use AI for identity verification on digital payments.



Securing Transactions

Digital payments enable advanced security measures.

While paper checks are only as secure as the mailbox to which they are delivered, digital payment methods leverage a host of advanced security technologies. Artificial intelligence (AI) has proven to be one of the most promising cybersecurity technologies, with 35% of firms using it for [identity verification](#) to reduce the risk of payment fraud. These systems can also analyze payment patterns and identify anomalies that could be the result of fraud, such as an unusual payee or payment amount.

Given these capabilities, it is no surprise that enhanced security features rank highly among payment leaders' priorities. In fact, more than 13% of heads of payment cite [enhanced security features](#) as the most valued characteristics when selecting a payment option for supplier transactions. Beyond improved security, digital payments offer additional benefits, including real-time cash flow monitoring and more effective vendor management.

Digital treasury processes can unlock a host of benefits for businesses.

While paper-based payment methods remain prevalent among businesses, treasury executives are increasingly recognizing the benefits of digitization. Almost all respondents in a recent survey reported that [digital treasury processes](#) improved cash flow forecasting (97%), enhanced financial visibility and control (96%), and boosted profits (91%). Despite these advantages, concerns about fraud and security risks continue to deter some companies from fully embracing digitization, even though paper payments are far more vulnerable to fraud.

The adoption of instant payments, however, has seen a significant uptick among companies, with 77% of respondents utilizing this technology in 2024, up from 62% the previous year. Among the companies using instant payments, this growth is evident in the widespread use of both the RTP® network and the FedNow® Service, with 92% and 77% of respondents reporting usage, respectively. While paper check usage has yet to see a meaningful decline, businesses may be more willing to phase out this legacy method as they gain confidence in the security and efficiency of more advanced payment technologies.

Call to Action

Transitioning From Paper Checks to Digital Payments

To address the escalating risks of check fraud and financial vulnerability, businesses should prioritize transitioning from paper checks to digital payments. Paper checks are inherently susceptible to various risks, including physical theft, fraud, forgery and mail interception. Criminals can easily steal checks from mailboxes, alter recipient names and amounts, or create counterfeit checks using sensitive banking information like routing and account numbers. Some bad actors even target mail carriers' [universal access keys](#), allowing them to steal checks from hundreds of mailboxes.

“

By replacing checks with secure digital payments, businesses can protect against fraud, lower expenses and ensure funds reach the right account faster.

”

DREW EDWARDS
CEO

 INGO Payments



Digital payment methods offer robust security solutions that significantly minimize fraud risks while enhancing financial protection. These advanced systems incorporate multiple layers of security, including encryption, multi-factor authentication and real-time transaction monitoring powered by AI. In addition, digital payments reduce human error, lower processing costs and provide businesses with improved transaction visibility and operational efficiency.

About

PYMNTS INTELLIGENCE

[PYMNTS Intelligence](#) is a leading global data and analytics platform that uses proprietary data and methods to provide actionable insights on what's now and what's next in payments, commerce and the digital economy. Its team of data scientists include leading economists, econometricians, survey experts, financial analysts and marketing scientists with deep experience in the application of data to the issues that define the future of the digital transformation of the global economy. This multilingual team has conducted original data collection and analysis in more than three dozen global markets for some of the world's leading publicly traded and privately held firms.

The PYMNTS Intelligence team that produced this Tracker:

John Gaffney
**Chief Content
Officer**

Andrew Rathkopf
Senior Writer

Alexandra Redmond
**Senior Content
Editor**

Joe Ehrbar
Content Editor

Mariano Soler
Research Analyst

INGO Payments

[Ingo Payments](#) enables banks, FinTechs, and enterprise brands to deliver innovative financial experiences through its full-service embedded finance platform. Designed to be bank-grade and compliance-first, the platform offers money mobility capabilities on a modern money stack, providing the foundation for account funding, transfers, mobile deposits, payouts, digital wallets, bank account creation, card issuing, PFM, and rewards solutions across diverse industries and use cases. By vertically integrating issuing, payment processing, and risk underwriting services, we help clients reduce third-party risk, operational complexity, and costs, while accelerating time to market.

Disclaimer

The Money Mobility Tracker® Series may be updated periodically. While reasonable efforts are made to keep the content accurate and up to date, PYMNTS Intelligence 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 Intelligence 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 Intelligence is the property of PYMNTS and cannot be reproduced without its prior written permission.

The Money Mobility Tracker® Series is a registered trademark of What's Next Media & Analytics, LLC ("PYMNTS Intelligence").