PYMNTS INTELLIGENCE | INGO Payments

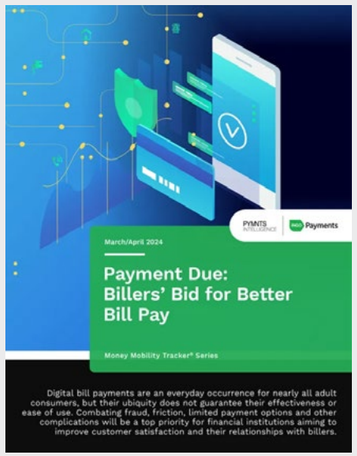
April 2024

Protecting Accelerated Disbursements From Fraud

Money Mobility Tracker® Series

Faster disbursements are a boon for companies, employees and customers alike, but — like all payments — they are not immune to bad actors, and their speed complicates the issue. Fortunately, a range of robust strategies are available to ensure that faster disbursements remain secure.

■ Read the previous edition



MARCH/APRIL 2024
Money Mobility Tracker® Series

What's Inside

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.

© 2024 PYMNTS Intelligence All Rights Reserved

Introduction

Disbursements are a critical part of the modern economy, with more than 170 million consumers in the United States receiving at least one disbursement within the past year. These payments come in a multitude of flavors, including Social Security payments, insurance claim payments and retail refunds. For consumers, these payments all share one feature: They could be faster. According to a PYMNTS Intelligence survey, roughly half of U.S. consumers who receive disbursements would choose to obtain them via instant payment rails if they could, with faster payments providing not just convenience but also a powerful advantage in cash flow transparency and money management.

Accelerated payments are not invincible, however. Faster transactions are susceptible to the same social engineering techniques fraudsters have employed to target legacy payment systems — but with the added twist that funds intercepted via faster payments are often irrecoverable due to their speed. Fortunately, real-time solutions are rising to meet the challenge. Companies can confidently offer their customers the convenience of faster disbursements while proactively keeping them secure from fraud.

Fraud Meets Faster Payments

Faster Payments Demand Faster Fraud Tools

While faster payments offer increased ease and convenience for consumers and businesses, accelerated funds lost to fraud are seldom retrievable, as opposed to slower payment methods that allow for more time to reverse the transaction. This makes prevention paramount.

27%

of firms that use real-time payments reported seeing an increase in fraud affecting these payments in 2023.

Fraud's threat to faster payments is complicated by their speed — and hence irrevocability.

With 78% of financial institutions (FIs) and businesses calling faster payments a "must-have" for their organizations, enthusiasm has never been higher for instant payments adoption. Nearly nine in 10 FIs say they plan to adopt the FedNow® Service or The Clearing House's RTP® network within the next two years. Meanwhile, 76% either already offer or plan to implement instant payments network Zelle. With so many financial players moving toward faster payments, implementing best practices for protecting these payments from fraud is an essential step in that process.

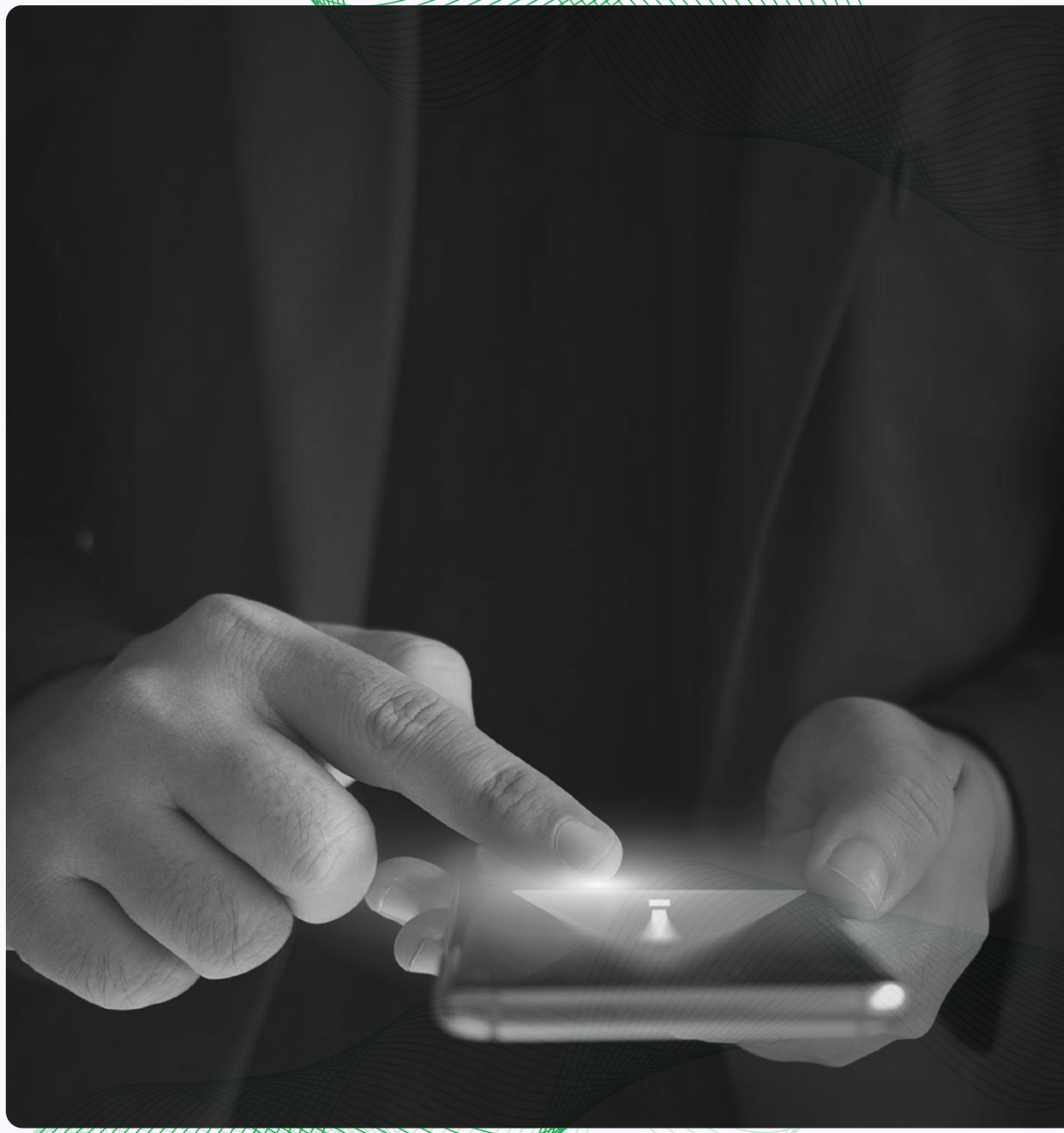
As consumers have learned through the growing popularity of peer-to-peer (P2P) payment apps, however, fraud protection of faster payments is complicated by the fact that, once sent, these payments cannot be "clawed back." Instead, speed of fraud detection and prevention are key.

© 2024 PYMNTS Intelligence All Rights Reserved

Fraud Meets Faster Payments

Real-time payments require real-time fraud-fighting.

Although only 27% of industry participants reported seeing an increase in fraud related to their faster payments operations in 2023, this figure has more than doubled from 13% in 2020. The types of fraud most often cited as a concern by the faster payments industry match those of the payments industry in general, including account takeover (ATO) fraud at 52%, synthetic identity fraud at 47%, and authorized push payment (APP) fraud at 34%. APP fraud involves tricking payers into directing payments to the fraudster rather than the intended recipient, often through tactics such as identity theft or social engineering. Faster payments' vulnerability to such tactics is not unique, but the payments' speed raises the stakes of having immediate and powerful fraud protection, preferably in the form of real-time payments monitoring.



© 2024 PYMNTS Intelligence All Rights Reserved

Faster Fraud Combatants

Advanced Technologies Effectively Curb Disbursements Fraud

Technologies such as AI and ML are highly effective at securing faster transactions by identifying minute account and transaction discrepancies and patterns that would evade human detection.

71%

of FIs are leveraging AI and ML for fraud detection and prevention.

Emerging technologies are being used to curtail payments fraud.

Artificial intelligence (AI) and machine learning (ML) offer a range of capabilities, one of the most notable of which is the detection of payments fraud. AI systems can continuously monitor financial transactions from end to end in real time to identify fraudulent login attempts, anomalous transactions and suspicious or fake accounts. By validating users and analyzing data much faster than human analysts can, these technologies can speed decision-making in faster payments environments. In addition, through their capacity to learn, the technologies' ability to spot unusual payment behaviors or account usage is always improving over time, making these tools especially useful in applications for detecting ATO fraud — the top risk in faster payments fraud.

A recent PYMNTS Intelligence study found that 71% of organizations are leveraging AI and ML to detect and prevent fraud — up from 66% in 2023, which, in turn, was up from 34% in 2022. Moreover, as these technologies continue to gain ground, their impact on decreasing fraud rates in faster payments is becoming evident.

Faster Fraud Combatants

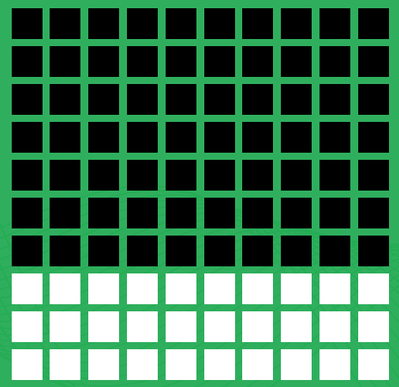
New technologies are already making an impact in countering fraud for some faster payments.

Coincident with the near doubling of the share of FIs using AI and ML to detect and prevent fraud between 2022 and 2023, the incidence of Venmo fraud in FIs with more than $5 billion in assets fell significantly from 50% in 2022 to just 34% in 2023. Fifty-six percent of these FIs reported plans to initiate or increase their use of ML and AI to improve existing fraud solutions. Another study reports that 65% of FIs believe AI will be instrumental in detecting social engineering and APP scams. Although ATO, synthetic identity and APP fraud remain the biggest threats, all three have seen a significant drop in their mention by faster payment providers as concerns over the past four years. This likely reflects the shift toward leveraging advanced technology to counter these advanced threats.

Overcoming Implementation Challenges

Third-Party Solutions Yield Faster Security

For FIs finding it difficult to implement AI- and ML-based fraud solutions on their own, third-party offerings can alleviate this burden.



70%

of FIs will ultimately rely on third-party solutions to deliver ML, AI and fraud scores provided by payment processors.

Many FIs lack the technical staff to make advanced fraud prevention a reality.

Recent PYMNTS Intelligence research shows that while many FIs still utilize in-house teams to develop fraud prevention tools, the desire to incorporate more advanced technologies for this purpose has pushed many to consider external providers.

On average, FIs develop 48% of the technologies they use to combat fraud in-house, such as customer transaction alerts. Meanwhile, only 14% of FIs develop fraud-fighting AI and ML technologies in-house due to the substantial costs and expertise involved. The report estimates that as AI and ML become the standard tools for advanced fraud protection, 70% of FIs will rely on third-party solutions to leverage ML, AI and fraud scores provided by payment processors.

Overcoming Implementation Challenges

Form3 and Feedzai joined forces to launch an APP fraud solution in the U.K.

One example of an AI-based faster payments fraud solution is the product of a recent partnership in the United Kingdom. Cloud-based account-to-account (A2A) platform Form3 recently joined with AI fraud solution provider Feedzai to introduce a solution for APP fraud, which is the most common fraud type in that market. Leveraging ML, the new product identifies anomalies in the behaviors of both payment senders and recipients. Understanding the risks surrounding the recipient is key to preventing this type of fraud, as APP fraud involves impersonation and social engineering to manipulate the victim into sending the payment. The solution aims to close the gap in intelligence that fraudsters exploit to receive faster payments.

> The best way to tackle the rise of APP fraud is the use of **collaborative intelligence** and cutting-edge technologies that allow the **real-time identification** of scams within the payment message.
>
> **Mike Walters**
> CEO FORM3

Call to Action

Making Faster Payments Fraud-Free

Reducing fraud in faster disbursements is made both crucial and complex by the irretrievable nature of instant payments theft, but advanced solutions are proving effective.

Some of the most promising technologies in this field include AI and ML, which can offer an ideal blend of security and seamless customer experience. AI-powered anomaly detection systems can analyze vast amounts of transactional data to establish baseline patterns of normal behavior. Any deviation from these norms can trigger alerts for further investigation, allowing organizations to quickly identify potentially fraudulent activity before disbursing funds. ML algorithms, meanwhile, can continuously learn, enabling them to adapt to new fraud patterns and stay ahead of evolving threats.

While the fraud threat to faster payments may seem formidable, FIs have access to all the tools they need to keep their customers safe. Those that effectively deploy technology to protect their customers will find themselves well-positioned as the disbursements field accelerates even further.

© 2024 PYMNTS Intelligence All Rights Reserved

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:

Aitor Ortiz
Managing Director

Andrew Rathkopf
Senior Writer

Alexandra Redmond
Senior Content Editor/Writer

Joe Ehrbar
Content Editor

INGO Payments

Ingo Payments is the money mobility company. Our mission is to give people and businesses instant, digital and secure access to their money. We provide embedded API and iframe-supported payment solutions and deliver fully digital, cloud-based platforms that bridge the gap between legacy payments infrastructure and new payments technologies to deliver modern, bespoke payment experiences. Whether it's instant account funding, payments or payouts, businesses can count on Ingo to tailor our platform and services to meet their needs. Headquartered in Alpharetta, Georgia, Ingo employs more than 240 professionals and serves some of the largest brands in North America.

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