PYMNTS INTELLIGENCE | INGO Payments

March 2025

Speed and Security: How Faster-Payments Providers Are Reducing Fraud Risks

Money Mobility Tracker® Series

Real-time payments are coming to the fore as a powerful tool for faster, more transparent transactions. While their instantaneous nature raises concerns about fraud, payment security is also emerging as real-time transactions' underrated strength.

Read the previous edition

February 2025

The Instant Remedy for Healthcare Payments' Pain Points

Money Mobility Tracker® Series

Despite advances in digital payment technologies, healthcare payments remain a complex landscape for patients and providers. The persistent use of outdated methods underscores the urgent need for digital and instant solutions that can meet the evolving demands of modern healthcare billing and patient expectations.

FEBRUARY 2025

Money Mobility Tracker® Series

What’s Inside

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

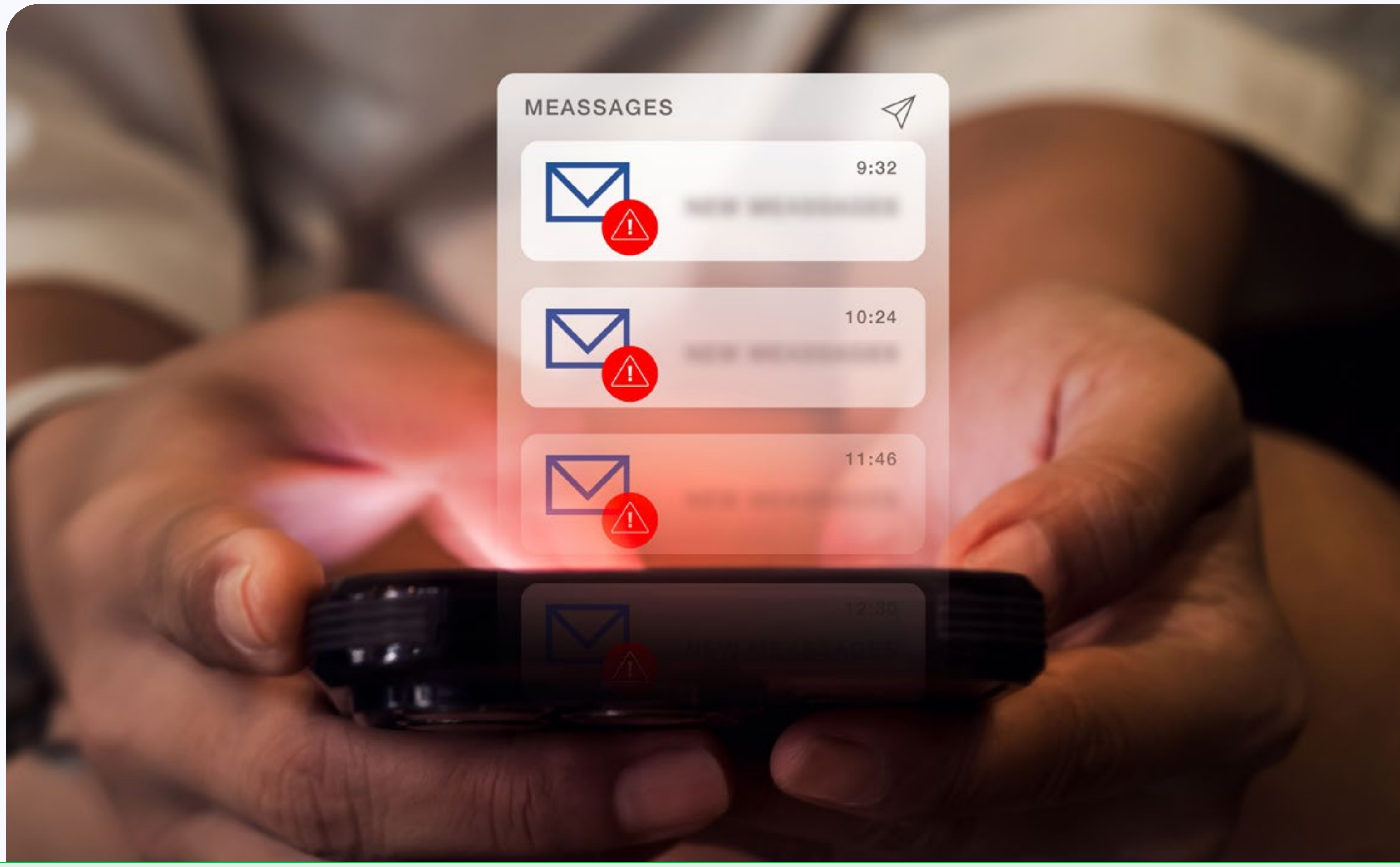
Fraud remains a persistent challenge for financial institutions (FIs), businesses and consumers, costing them money, data and peace of mind. PYMNTS Intelligence reports that the percentage of FIs experiencing increased fraud-related dollar losses rose from 29% to 40% year over year in 2024. These attacks range from simple scams to sophisticated digital hacks that leverage advanced botnets. In addition to financial losses, FIs and businesses that fail to protect against these escalating threats risk losing their customers to competitors.

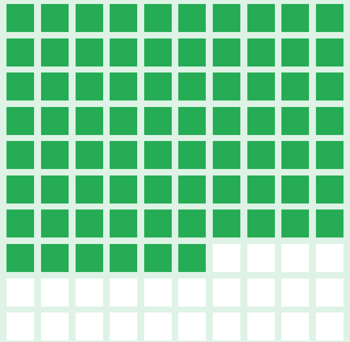
Instant payments have emerged as one of the most important innovations in financial services in recent years, offering benefits like improved cash flow control, smoother operations and the ability to move money anytime. However, the speed of these transactions also heightens fraud concerns for both consumers and providers. While many consumers view real-time rails as more vulnerable due to their irreversible nature, instant payments can be more secure than traditional methods when banks and businesses implement advanced security and real-time fraud detection to mitigate risks.

Fraud Concerns

Consumers Balance Convenience and Caution With Faster Payments

With both fraud and instant payment usage on the rise, consumers are increasingly concerned about fraud in faster payments.





76%

of U.S. consumers in 2024 received unsolicited communications via text, email or phone that they suspected to be scam attempts.

Fraud Concerns

The CFPB alleges that inadequate protection cost Zelle users $870 million in fraud losses.

The Consumer Financial Protection Bureau (CFPB) filed a lawsuit against Early Warning Services, the operator of Zelle, and its partner banks Bank of America, JPMorgan Chase and Wells Fargo. The suit charged them with failing to protect consumers from fraud on the peer-to-peer (P2P) payment network, costing users $870 million over seven years. The CFPB alleges that the banks rushed Zelle to market to compete with other P2P payment networks such as Venmo without implementing sufficient fraud prevention measures or security guardrails. The suit also claims that the banks failed to address hundreds of thousands of fraud complaints from consumers, providing neither proper assistance nor reimbursement.

For its part, Zelle has denied the claims, accusing the CFPB of exaggerating the impact of fraud on its customers. Zelle states consumers conducted $481 billion in transactions on its network during the first half of 2024 alone, emphasizing that fraud losses represent a small fraction of overall payment volume.

Consumers are becoming increasingly aware of payment fraud risks.

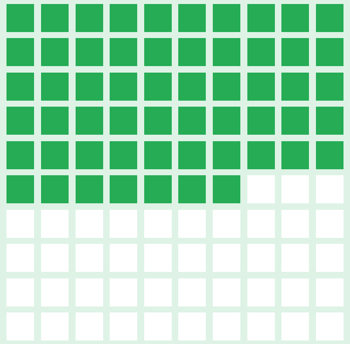
According to a recent survey, 76% of consumers in the United States last year reported receiving unsolicited communications via text, email or phone that they suspected to be scam attempts. This represents a 4% rise from 2023, indicating a growing awareness of fraud among consumers. In addition, 51% of U.S. consumers reported having friends or family members who were scammed in 2024, up 8% from 2023, surpassing the global rise of 5%. This personal connection to scam victims has resulted in heightened vigilance regarding digital payment risks, scams and overall security concerns.

This awareness extends to real-time payments as these channels grow in popularity. By 2028, an estimated 70% to 80% of all FIs in the U.S. will have the ability to receive real-time payments, while an estimated 30% to 40% will have the ability to send them. Use cases include high-dollar transactions such as government payouts, gambling and online banking, making these payments prime targets for fraudsters. Consequently, FIs must invest heavily in security measures to keep their customers safe on these new real-time payment networks.

Anti-Fraud Technologies

Instant Payments Serve as Catalysts for Strong Fraud Prevention

As real-time payment systems gain popularity, fraudsters are employing increasingly sophisticated techniques, prompting FIs to adopt advanced technologies for real-time fraud detection and prevention.



57%

of consumers said better fraud detection was the most or second-most important measure their banks could implement.

Anti-Fraud Technologies

Consumers want stronger payment fraud protections from their banks.

A recent survey found that 57% of consumers said better fraud detection was the most or second-most important measure their banks could implement. Additionally, 47% of consumers said receiving more alerts about known or emerging scams would be among the most effective measures their FIs could take. Furthermore, 75% of bank customers indicated they would view their bank favorably if it preemptively declined a payment identified as fraudulent — a 4% increase from 2023. These findings underscore shifting customer expectations regarding payment priorities, which are evolving from convenience and speed to security as consumer awareness of fraud threats increases.

Anti-Fraud Technologies

Fraud rates on real-time rails are much lower than for traditional payment systems.

Instant rails, meanwhile, would seem to be offering the reassurance consumers need. According to experts with the BAI, fraud rates on real-time rails such as the RTP® network and the FedNow® Service are substantially lower than those for traditional payments such as automated clearing house (ACH), wire transfers and checks. Instant payment systems tend to rely on tokenized processing, in which random strings of characters or “tokens” replace sensitive payment details during transactions. Because of this, they provide better security than legacy payment methods. As banks work to improve fraud detection and prevention for faster payments, signs thus far indicate that strong access management and consumer education offer powerful tools for risk reduction.

AI is proving effective in protecting against frauds and scams.

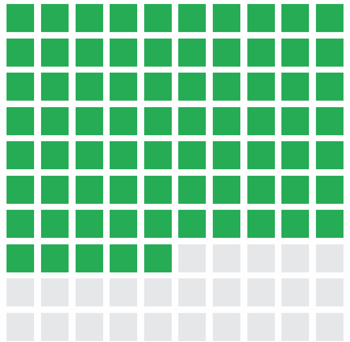
Nearly three-quarters (73%) of global FIs are also actively employing artificial intelligence (AI) for fraud detection, while 74% are using the technology to sniff out other forms of financial crime. These systems typically monitor customer behavior, flagging deviations that may indicate fraudulent activity. For example, a customer who normally withdraws small amounts from their bank account but suddenly makes a large withdrawal might trigger a fraud investigation. Ninety-four percent of organizations surveyed leverage AI and machine learning (ML) techniques to identify risks based on user behavior.

AI’s benefits extend beyond fraud detection. Sixty-nine percent of FIs believe that AI will result in greater revenue — through enhanced customer interactions and decreased time spent on investigating false positives — compared to the losses incurred from fraud and breaches.

Reassuring Customers

Consumers Value Payment Security More Than Ever

Consumers have traditionally prioritized speed in payments, but security is becoming increasingly important. FIs can enhance customer trust and loyalty by implementing advanced real-time fraud detection systems that safeguard faster payment methods without compromising transaction speed and convenience.



75%

of consumers would switch FIs due to inadequate fraud protection.

Reassuring Customers

Consumers are increasingly prioritizing transaction security over speed.

More than 70% of consumers are willing to dedicate more time to identity verification if it means greater security. This figure rises to 77% among financial services customers, who are growing more aware of the importance of transaction security. A significant majority of consumers — 75% — said they would change FIs if they discovered inadequate fraud protection measures. The same proportion also believes that their bank is responsible for preventing fraud and cybercrime and reimbursing customers for any stolen funds.

Seamlessness and speed are becoming less critical. Another survey found that fewer than 15% of consumers rated quick, seamless account openings as extremely important, compared to the roughly 54% and the more than 55% who ranked security and privacy, respectively, as extremely important. The lesson for FIs is that their customers are willing to tolerate some friction in everyday processes if it means having greater protection from fraud.

Reassuring Customers

Customers reward banks that take fraud prevention seriously.

According to a recent J.D. Power survey, 92% of bank customers are likely to continue using their bank if a fraud issue is resolved satisfactorily. This retention of customer trust and engagement can offset the potential cost of implementing anti-fraud systems.

Conversely, poor handling of a fraud incident can damage customer relationships. In this instance, more than half of customers (57%) would file a complaint with their banks, and 8% would escalate their complaints to government regulators. Most troubling, however, is that 19% of customers would switch FIs due to dissatisfaction with how their bank handled a scam incident. This underscores the importance of preventing fraud whenever possible and resolving incidents promptly.

Call to Action

Safely Leveraging Real-Time Payments

> Fraudsters are always adapting — but with AI and real-time transaction monitoring, financial institutions have powerful tools to protect instant payments and maintain customer confidence.

DREW EDWARDS
CEO

INGO Payments

Despite consumer worries, real-time payments actually offer many advantages over traditional transactions in the fight against fraud. Real-time rails often employ enhanced security measures and data capabilities, supporting more robust verification processes and real-time risk assessments. These features can help banks identify and block suspicious transactions before they are completed, limiting overall fraud losses.

However, the instantaneous nature of real-time payments presents new challenges. Once a transaction is completed, it is largely irreversible, leaving little time for traditional fraud detection methods. To address these risks, banks should implement multilayered fraud prevention strategies that combine advanced analytics, AI and ML algorithms capable of detecting anomalies in real time. Additional measures such as transaction limits, dual approvals and multifactor authentication for high-value transfers can further enhance security. Customer education is essential, helping individuals recognize and avoid real-time payment fraud risks.

About

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 and Writer

Joe Ehrbar
Content Editor

Augusto Solari
Senior Research Analyst

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").