MONETIZING DIGITAL INTENT TRACKER®

JUNE 2022

PYMNTS.com | neuroID

Read the previous edition

MAY 2022

Monetizing Digital Intent Tracker®

MONETIZING DIGITAL INTENT

TRACKER®

PYMNTS.com | neuroID

ACKNOWLEDGMENT

The Monetizing Digital Intent Tracker® was produced in collaboration with NeuroID, 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.

TABLE OF CONTENTS

EDITOR'S LETTER

Digital fraud continues to wreak havoc on the economy despite banks', businesses' and consumers' best efforts to stop it. The Federal Trade Commission (FTC) reported $5.8 billion lost to fraud last year, an increase of more than 70% since 2020. Some of the most common schemes include impostor scams, which caused more than $2.3 billion in losses, and online shopping fraud, which shot to $392 million in 2021, up from $246 million in 2020. More than 2.8 million consumers submitted fraud reports to the FTC last year, although the true number of victims is likely far higher.

Businesses primarily rely on "post-submit data" — including passwords, personal identification numbers (PINs) and biometrics — to counter these security threats. Many of these methods have proven ineffective at stopping fraud, however. At least 65% of consumers recycle passwords among several accounts, so a data breach at any single account could potentially compromise them all. Biometrics and multifactor authentication (MFA) may be much safer, but fraudsters are becoming increasingly sophisticated in devising ways to fool facial recognition scans and intercept text messages from verification systems.

Businesses are leaning increasingly on behavioral analytics to keep their customers safe, combining the above post-submit data with "pre-submit data," which analyzes how customers enter this information. Legitimate customers enter their own names quickly and with few errors, for example, while fraudsters might introduce misspellings or copy and paste names from other forms — both red flags of fraud. Behavioral analytics systems can reduce rates by up to 35%, according to a recent study.

Pre-submit data reaches its true potential when used in concert with post-submit data, resulting in a security solution greater than the sum of its parts. Systems such as these can reduce total fraud volume by 71% and bring the cost of fraud 12% lower — largely by presenting such a daunting target that bad actors take their schemes elsewhere.

This edition of the Monetizing Digital Intent Tracker®, a PYMNTS and NeuroID collaboration, delves into why post-submit security systems are ineffective at dealing with digital fraud. It also examines how behavioral analytics can reduce fraud by augmenting these systems. Companies are leveraging both pre-submit and post-submit data in tandem to keep themselves and their customers safe.

Thought Leadership Team

PYMNTS.com

Feature Story

How Wave Financial Leverages Pre- And Post-Submit Analytics To Prevent Fraud

DIGITAL FRAUD IS A CLEAR AND PRESENT DANGER TO BANKS, BUSINESSES AND ORGANIZATIONS OF ALL KINDS.

Bad actors deploy stolen identities, synthetic identities, account takeovers, botnets, denial of service attacks and numerous other techniques against any target they deem vulnerable, all in the name of stealing customers' funds or personally identifiable information (PII).

Preventing a variety of fraud types is a full-time job, but even with the very best efforts, subpar authentication systems can let companies down. Some of the most effective techniques involve leveraging both post-submit authentication data and pre-submit behavioral data, as exemplified by software company Wave Financial.

"Our models take into account behavioral data, like how users navigate our sites, combined with the hard production metadata, such as PII of the cardholder and geographic information of their devices," said Angie Dobbs, vice president of fraud and risk for Wave.

In a recent PYMNTS interview, Dobbs offered an inside look at the dangerous fraud threats facing organizations today and why a multilayered authentication system combining pre- and post-submit data is one of the most effective fraud prevention methods available.

PRESSING FRAUD THREATS

The most pressing type of fraud facing the financial industry on a daily basis is new account fraud, according to Dobbs. Fraudsters steal or develop new identities out of whole cloth and attempt to create fake accounts, bypassing traditional verification checks, such as Social Security numbers, because they already possess the information.

“The majority of fraud we experience is new account fraud, consisting of stolen or synthetic identities used to create payments accounts which are then used to process stolen card data,” she explained. “We also experienced your typical account takeover fraud, but by and large, it’s a new account fraud problem.”

These bad actors are primarily attempting to drain customers’ accounts of funds, either by hijacking their accounts directly or tricking them into sending money into their fake accounts. Stopping this fraud after it occurs is difficult, as the money is already gone from victims’ bank accounts and fraudsters shut down fake ones as soon as they hit paydirt.

“They steal an identity or create an identity of a business owner and a fake, fictitious business,” said Dobbs. “They generate invoices for those businesses and charge the stolen credit cards on those. So if we don’t detect it, then they take the funds, and once they charge back, we’re at a loss.”

Preventing this type of fraud requires ironclad customer verification, but it cannot scare away legitimate customers in the process. Wave employs behavioral data to augment post-submit data, such as passwords, to strike this balance.

LEVERAGING BEHAVIORAL DATA TO AUGMENT EXISTING POST-SUBMIT DEFENSES

Multiple defensive layers are vital to stopping fraud, as an enterprising bad actor armed with a workaround for a single defensive system can run rampant within companies’ systems. Fraudsters constantly innovate new techniques, potentially developing countermeasures for existing authentication systems with zero warning.

“There is no silver bullet,” said Dobbs. “There are varying types of data breaches, and our identities are becoming more complex. Physical data is being compromised and less reliable as a verification method. Devices are playing a bigger part — we’ve always got our phones by our side — but even those are being doctored or phone numbers being forwarded.”

The most effective method to shore up existing post-submit defensive layers is by leveraging behavioral data, she said. Wave’s technique involves observing how users navigate its website and determining their likelihood of being legitimate users or fraudsters.

“A real user is going to peruse, they’re going to click around, they’re going to try to understand what they’re here for,” said Dobbs. “But a fraudster, typically, is familiar with our site, and they know exactly how to go for the goods.”

Leveraging this pre-submit behavioral data and the post-submit data in tandem will be vital in preventing bad actors from gaining access to valuable funds and personal information. Either deployed in isolation will be far less effective.

> “Devices are playing a bigger part — we’ve **always got our phones by our side** — but even those are being doctored or phone numbers being forwarded.”

Q&A

JACK ALTON
CEO
neuroID

What are some of the flaws inherent in relying on post-submit data, such as passwords and biometrics for user authentication?

The goal of every user-authentication process is to answer the question, 'Is this user who they say they are?' Historically, that has been done by simply asking the user for unique information such as a password, username, email, Social Security number and, more recently, some sort of biometrics such as a finger scan. These pieces of data are called personally identifiable information, or PII. This PII is reviewed and analyzed after the user hits the submit button and is run through a fraud or identity stack for verification, which is why it's known as 'post-submit data.'

This is where the industry has been for years: running post-submit checks against PII. The problem is that PII is not a reliable indicator of users' identities. Research shows that billions of records containing consumer PII have been stolen, leaked, compromised or otherwise exposed and used to attempt to steal products, services and cash. If we continue to rely on the same compromised data, we will continue to get the same unreliable results. This is the biggest fly in the fraud-fighting ointment causing false positive/decline rates to increase and driving stagnant, single-digit conversions.

As this method of verification became less reliable, we moved to two-factor authentication, which again relied on many of the same PII data points. We have now moved to multifactor authentication and fraud or identity orchestration platforms while continuing to assume that if we simply add more of the same PII data points together and throw in some machine learning or artificial intelligence, we'll be OK.

Behavioral analytics systems can reduce fraud by up to 35%, according to recent research. How do these systems analyze pre-submit data to do so?

Unlike PII and multifactor authentication that relies on post-submit data, behavioral data is pre-submit. It is tracked before a user enters the fraud stack, so it doesn't add any friction to their experience — it's already there, just waiting to be captured. And because behavior is truly unique to each user, it is impossible to fake. Analyzing the behavior of users, both across the crowd and individually, provides very accurate indications as to their intentions and helps answer the critical question 'Are you who you say you are?'

By monitoring the crowd of users coming to an organization's 'front door' through an application, behavioral analytics can see indicators of fraudulent activities such as fraud rings or bots as they interact with the form, even before the submit button is hit. They may have obtained all the correct PII, but behavior analysis can determine if they are familiar with that PII. If they are not familiar with the PII they are entering, the odds that the user is not who they claim to be and the risk of fraud dramatically increases.

By alerting and flagging users who are not familiar with the PII they are entering, fraud and identity teams see for the first time how the actions or behavior of the user can help them determine the best approach to take. That could range from a straight decline to an escalated verification process or a fast-tracked approval. This simple approach has been used by major online brands to flag more fraud earlier and avoid costly fraud operations and reviews, as well as to increase conversion rates.

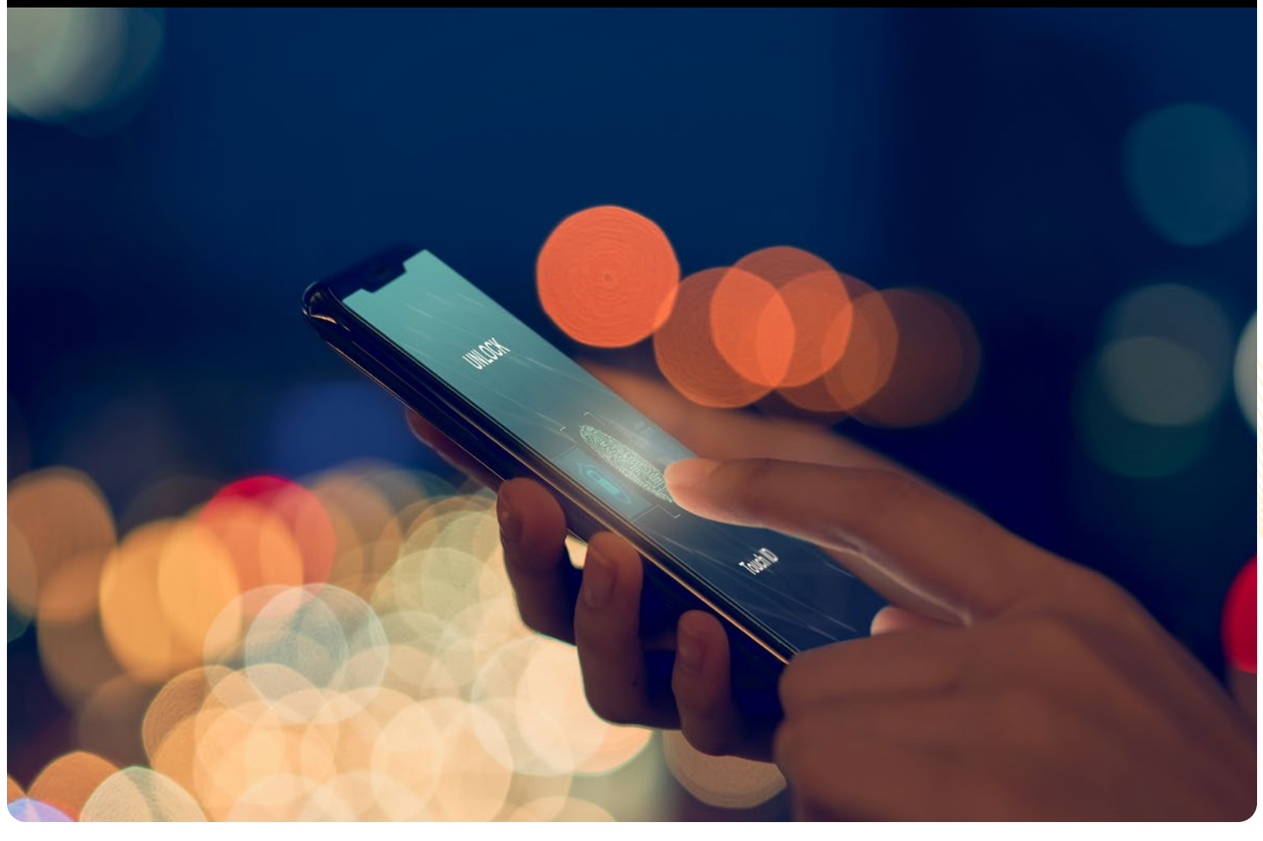
What is the best way to combine post-submit and pre-submit data to keep companies and their customers safe from fraud?

Essentially, the process is to add the ability to monitor behavior at the top of the onboarding funnel and at various areas of authentication. This early, pre-submit warning system alerts a company's current fraud stack to the looming presence of fraud, fraud rings, bots, etc., so their system can take appropriate action rather than running every user through the same process. Post-submit data can be used for appropriate step-ups rather than blunt-force rejections.

While the integration can be as simple as a JavaScript installation, the enhanced view of users on their site can lead to lower fraud rates, lower false positives/declines, lower fraud operational cost, lower underwriting expense and, ultimately, higher conversion rates.

PYMNTS Intelligence

Combining Pre-Submit And Post-Submit Data To Stop Digital Fraud



IDENTITY FRAUD IS A GROWING PROBLEM IN THE UNITED STATES.

Losses due to identity fraud were up 79% year over year in 2021 to a total of $52 billion, while the number of victims rose 50% to 42 million adults. Identity fraudsters leverage a wide variety of techniques, ranging from identity theft to the creation of synthetic identities compiled from various scraps of actual identity data.

With fraudsters constantly innovating ways to circumvent popular security measures such as MFA, biometrics and other forms of verification, cybersecurity providers are scrambling to catch up. Relying on this post-submit data can potentially let fraudsters through to steal funds or valuable information, damaging companies' reputations in the process. Pre-submit data — such as how users swipe, type and behave during data entry — is also a valuable tool for stopping bad actors. This month, PYMNTS Intelligence explores how companies can use pre- and post-submit data in tandem to halt identity fraud and other forms of cybercrime.

POST-SUBMIT DATA FOR FRAUD PREVENTION

Post-submit data primarily consists of PII that verifies the user's identity, such as biometrics, passwords, PINs or other data points. These methods have variable efficacy, with passwords being a particularly weak security method. Upwards of 65% of consumers recycle passwords among several accounts, so a data breach at any account could potentially compromise them all. Biometrics and MFA are less vulnerable to compromise, but fraudsters have been known to intercept verification codes or use printed pictures to fool facial recognition scans.

Post-submit data is also prone to be exposed via data breaches. A recent study found that 83% of data leaked in data breaches within the financial industry was personal data, for example, including login credentials, Social Security numbers and email addresses, all of which bad actors can exploit.

Relying on post-submit data is also decidedly inconvenient for customers. An estimated 65% of consumers abandon websites when asked to create a username and password, and 92% of users said they would rather leave a website entirely than try to recover or reset forgotten login credentials.

Post-submit data on its own thus poses significant risks of security incidents and customer abandonment. Only when combined with pre-submit data through behavioral analytics can post-submit data adequately protect customers against fraud with minimal friction.

LEVERAGING BEHAVIORAL ANALYTICS TO HARNESS PRE-SUBMIT DATA

A more effective way to authenticate customers is to look at how they enter their data rather than the data itself. These "swipes and types" are known as pre-submit data and can contain valuable tells as to whether a user is legitimate. Genuine customers typically enter their names quickly and without error, for example, while fraudsters might introduce misspellings while typing unfamiliar names or might copy and paste them from other forms — both warning signs of fraud. More than 65% of users enter post-submit data abnormally, meaning that an unusually smooth entry pattern could also be a sign of fraud. Analyzing pre-submit data in this way can reduce fraud rates by 35%, studies have found.

Pre-submit data reaches its maximum efficacy only when combined with post-submit data, however. A clever fraudster could dupe each type of data independently, but making it past both methods would require much greater effort. Deploying both pre-submit and post-submit authentication checks is a classic example of MFA, which can result in a 71% reduction in total fraud volume and a 12% decrease in lost revenue. The mere presence of a multilayered security stack can be enough to convince bad actors that an organization is not worth their time and prompt them to move on to softer targets.

Fraudsters are constantly innovating ways to circumvent common security solutions, with passwords, biometrics and SMS codes all demonstrating security vulnerabilities in recent years. Combining this post-submit data with the pre-submit patterns of entry could be the key to staying ahead of bad actors and keeping both organizations and customers safe from fraud.

NEWS & TRENDS

DIGITAL **FRAUD TRENDS**

$43 BILLION LOST TO BUSINESS EMAIL COMPROMISE FRAUD IN THE PAST FIVE YEARS, FBI REPORTS

Fraudsters leverage countless methods to scam businesses, but one of the most dangerous is business email compromise (BEC) fraud, in which bad actors pose as a company's supplier and dupe accounting teams into paying them rather than their actual vendors. The Federal Bureau of Investigation reports that businesses have lost $43 billion to this scam between 2016 and 2021, a 65% increase from the previous five years. This includes 241,206 separate incidents in the U.S., with 116,401 different victims reporting this crime to the FBI's Internet Crime Complaint Center.

BEC fraud is tough to correct after the fact because it is technically a legitimate transaction, just one that a fraudster tricked an accountant into making. Some variations of this scheme steal employees' PII or tax information instead of funds, making behavioral analytics a crucial step in mitigating further incidents of fraud that leverage this stolen data.

CONCERNS GROW OVER BIOMETRIC IDENTITY THEFT, STUDY FINDS

Biometrics have long been heralded as a silver bullet for identity verification, but fraudsters are developing ways to spoof these systems, and consumers' attitudes surrounding them have cooled significantly. A recent survey of Canadian consumers found that 50% said they were concerned that fraudsters could steal their biometric data. They also raised other concerns that were not security-related, with 49% saying they were worried about organizations misusing their biometric data and 45% saying that biometrics could potentially compromise their privacy.

Biometrics are still a popular verification tool, regardless of these concerns. More than half of Canadians use their fingerprints to unlock their phones, and 32% use facial recognition for the same purpose. Fourteen percent of biometric users started leveraging these methods for the first time during the pandemic, the study found.

55% OF INDIVIDUALS RELY ON MEMORY FOR PASSWORD MANAGEMENT

Biometrics may be under scrutiny, but password security loopholes have been known for decades. A recent study revealed that individuals largely eschew password managers, with 55% relying on memory, 32% writing passwords down on paper and 23% keeping them in text files on their computers. Just 30% of individuals leverage password managers, which are the most effective solution for such vulnerable systems. These managers help limit the amount of password recycling, which 85% of Americans do on a regular basis. Relying on post-submit data such as passwords is unreliable at best, but combining them with pre-submit data such as behavioral analytics can significantly improve their efficacy.

FRAUDSTERS EXPLOIT **SECURITY LOOPHOLES**

GENERAL MOTORS HIT WITH CREDENTIAL STUFFING ATTACK

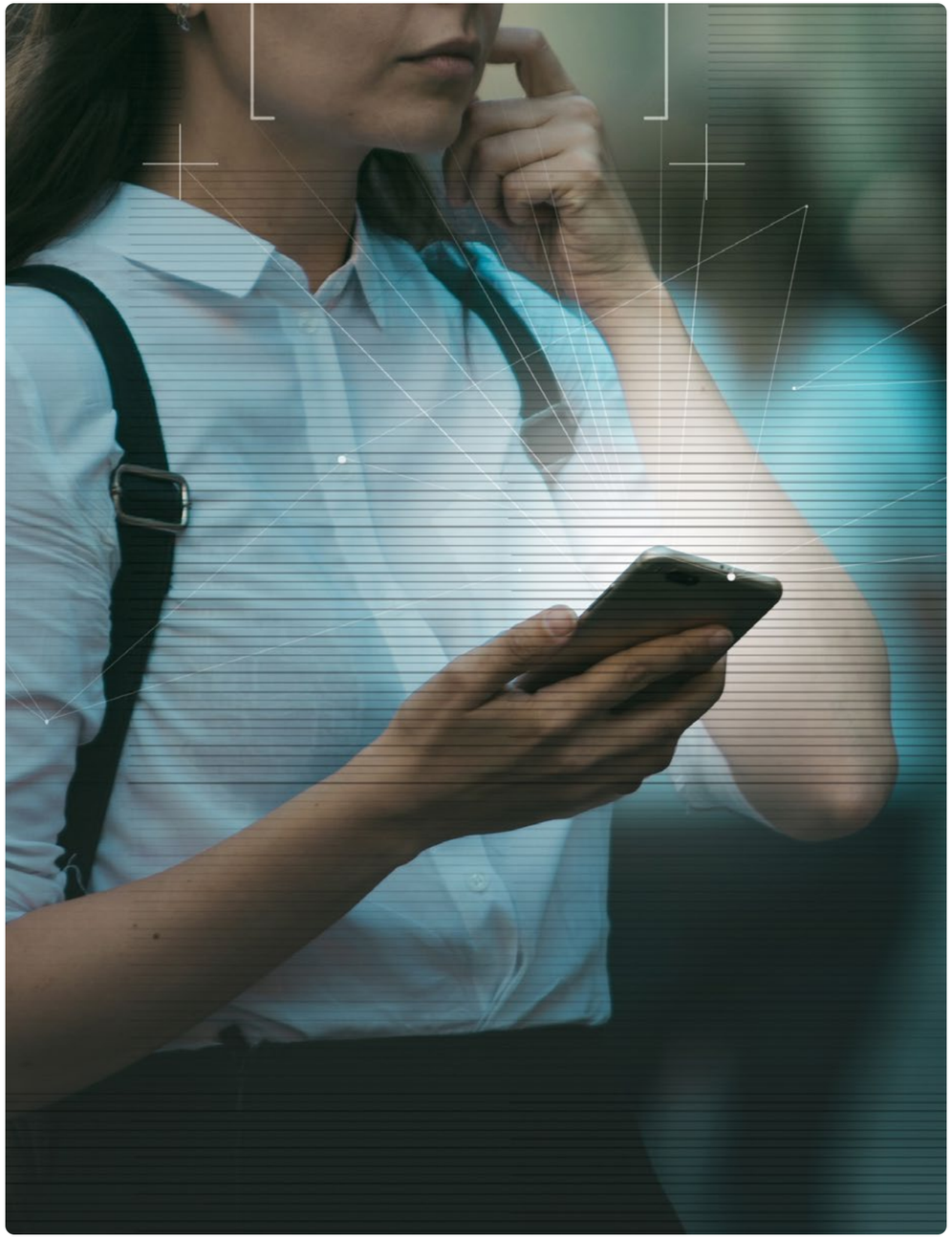
Credential stuffing is a popular fraud method, consisting of hackers obtaining stolen login credentials and deploying them en masse to break into customer accounts. Car manufacturing giant General Motors recently suffered one such example, sending a warning to 5,000 California residents that the hacker had potentially leaked their personal information. This warning was compulsory under a California law that mandates public notification in the event of a data breach affecting more than 500 people. GM said the attack occurred between April 11 and 29 of this year.

Credential stuffing attacks often result from phishing and password recycling, with bad actors stealing user passwords and then using them on other accounts owned by the same person. Behavioral analytics could potentially catch these data breaches by noticing automated data entry rather than traditional typing.

FBI WARNS THAT FRAUDSTERS ARE SELLING LOGIN CREDENTIALS FOR COLLEGE NETWORKS

A new target for fraudsters is higher education, with the FBI warning that cybercriminals are selling login credentials for college networks. Bad actors largely obtained these passwords and usernames through phishing, according to the FBI, as well as large-scale data breaches at other organizations that held recycled passwords. The fraudsters are currently selling these credentials for up to thousands of dollars.

The FBI recommends that universities implement training programs so that students and employees can identify and avoid phishing attempts, as well as adopt brute-force protection measures. Behavioral analytics can also be valuable, as it limits the efficacy of these stolen login credentials by identifying whether a bad actor is entering them using an automated system.



MONETIZING DIGITAL INTENT

TRACKER®

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.

neuroID

NeuroID is solving the global Digital Identity Crisis. The industry-redefining behavioral analytics company applies patented neuroscience technology to measure how familiar users are with their inputted PII before they click ‘submit’ and enter a company’s fraud stack. NeuroID analyzes this pre-submit data in real time and determines if users are genuine or risky without adding any friction. This proprietary process enables deep visibility into a user’s unique digital interactions and helps optimize identity verification orchestration, yet never collects customer data. NeuroID’s dynamic behavioral intelligence is fully compatible with all anti-fraud software and is endlessly scalable against any advances in fraud technology. Visit neuro-id.com to learn how FinTechs, insurers, eCommerce, traditional banks and others use ID Crowd Alert™ and ID Orchestrator™ to help safeguard their most valuable asset: the customer onboarding funnel.

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.

DISCLAIMER