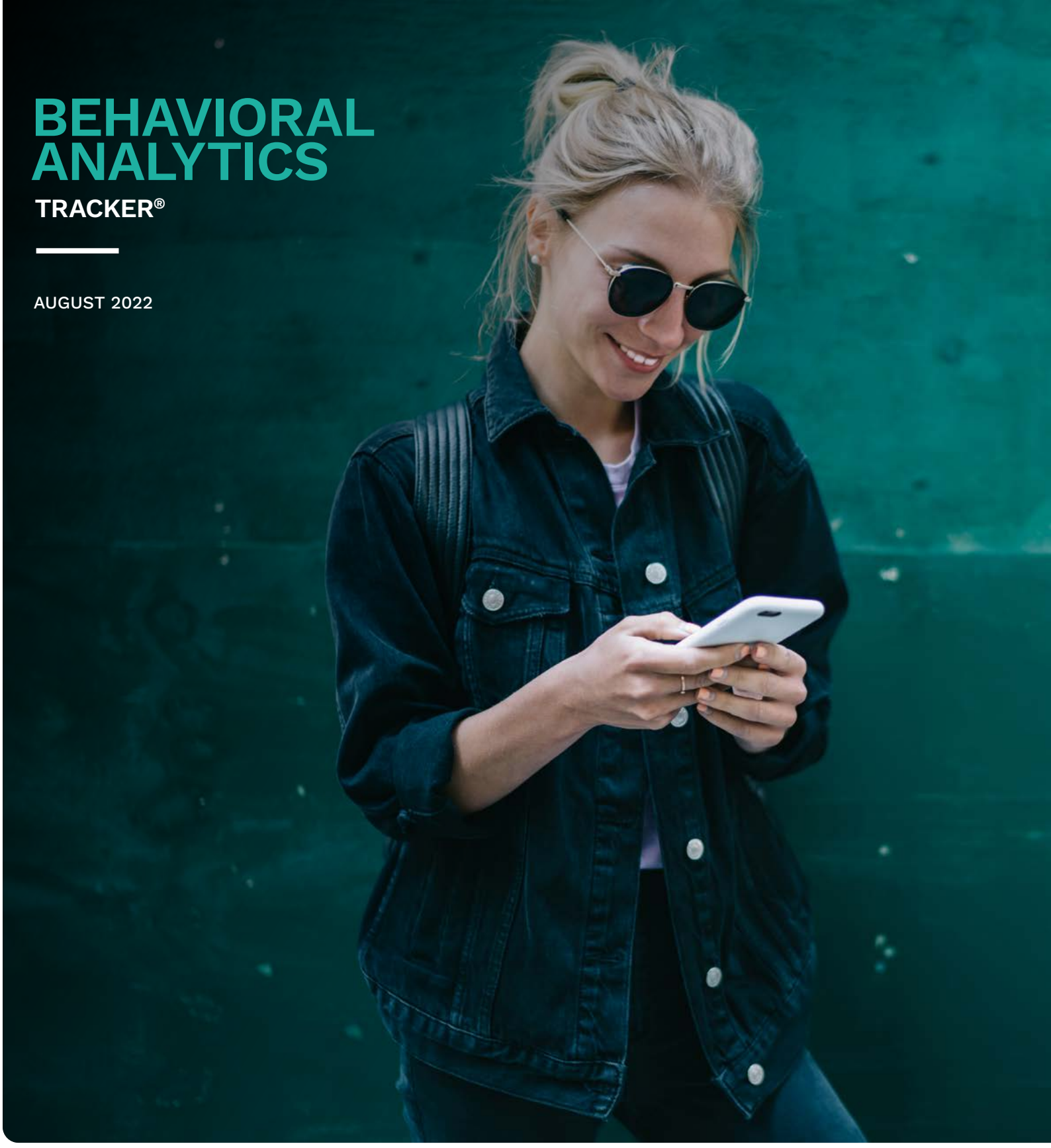
BEHAVIORAL ANALYTICS

TRACKER®

AUGUST 2022



■ FEATURE STORY

Featurespace on how behavioral analytics has changed fraud prevention

PAGE 06

■ PYMNTS INTELLIGENCE

Deploying behavioral analytics to smooth friction points in the customer journey

PAGE 10

BEHAVIORAL ANALYTICS

TRACKER®

PYMNTS.com

TABLE OF CONTENTS

04 WHY BEHAVIORAL ANALYTICS IS A WIN-WIN

A look at how behavioral analytics systems check both the “seamless” and “secure” boxes required for optimal authentication

06 FEATURE STORY

An interview with Roger Lester, account director at Featurespace, on how behavioral analytics is changing the fraud prevention landscape for good

10 PYMNTS INTELLIGENCE

An in-depth analysis of common friction points in the customer journey and how behavioral analytics can identify and fix these frictions while providing ironclad security

14 NEWS AND TRENDS

The latest worldwide behavioral analytics headlines, including why 75% of customers are likely to abandon a transaction due to a subpar digital experience and how shifting to pre-submit data could reduce false positives and customer friction

18 ABOUT

Information on PYMNTS.com

Why **Behavioral Analytics** Is A Win-Win

Customer onboarding is a crucial step in any business relationship. Its most critical task is user authentication, as unprotected onboarding represents an Achilles' heel to fraud for any company. For legitimate customers, onboarding serves an equally crucial purpose: setting the tone for the entire customer journey. Businesses that hope to stay in business must mind both imperatives, ensuring that customers are who they say they are and, if so, providing an easy and seamless experience to welcome them to the fold.

Onboarding regularly fails to check one or the other of the requisite "seamless" and "secure" boxes for authentication. PYMNTS' research found that 55% of auto dealers, for example, said digital authentication processes take too long, and 40% of banks and credit unions said their customers had bad experiences when undergoing these processes. Onboarding can also fail at both tasks, alienating genuine customers while also allowing fraudsters to slip through. Thirty-one percent of peer-to-peer (P2P) lenders complained that their customers suffered bad authentication experiences, yet 54% of lenders discovered these processes also created false identities. Consumers are more than willing to abandon businesses altogether if they feel their experience is subpar. Companies may also wish to abandon subpar authentication processes.

Behavioral analytics offers a solution to both problems, however. This technique is imperceptible to users, making for an effortless authentication experience. The technology relies not on what customers say but on what they do to make its determinations, examining users' digital habits to separate genuine customers from fraudsters based on their behavior. It scrutinizes factors such as typing speed and mouse movement to determine if users are who they claim to be, flagging fraudsters with a high degree of accuracy.

In addition to simply making the authentication process easier, behavioral analytics systems can find the exact friction points customers face by analyzing how long it takes to fill out various forms — including the ones that customers never completed because they found them so onerous that they decided to abandon the process in midstream. One company was able to leverage this data to reduce friction in a specific data field by 20%, for example, thereby cutting cart abandonment rates by 40%.

This edition of PYMNTS' Behavioral Analytics Tracker® takes a closer look at how companies use behavioral analytics to reduce onboarding frictions while honing their authentication security. It also explains why this imperceptible authentication method is proving to be a win-win for businesses and their customers.

Feature Story

Featurespace On How

Behavioral Analytics Has Changed Fraud Prevention

THE CUSTOMER RECEIVED A CALL FROM SOMEONE SAYING HE WAS A REPRESENTATIVE AT HIS BANK.

The representative said someone had warned them that a person at the bank was planning to hack the customer's account. Together, they could catch this crook, but to do this, the representative would need the customer's help, and the best way for him to help facilitate this sting operation was to transfer the entirety of his accounts, both checking and savings, into what the representative called a "suspense account," which they had created just for this purpose, at a different bank.

The supposed bank representative then told the consumer to expect a call from someone posing as a bank employee. This person would cast doubt on everything the supposed representative had told the customer so far — but, the representative assured him, this was all part of the scam. The supposed representative told the customer to tell the person on the other end of the line that he was having work done on his home, which would explain the need to transfer this vast sum of money.

Sure enough, a security analyst at the customer's bank called when the behavioral analytics team flagged these transactions as suspicious. Luckily, the analyst making the call had a gut feeling when talking to the customer that something was not right and was able to ask questions about the person supposedly doing work on the customer's home, such as his name and where the customer had found him. When the customer hesitated to give a name — because he did not have one to give — the analyst knew something was wrong and asked if someone pretending to represent the bank had contacted the customer.

"Thankfully, the customer suddenly started to question the initial contact and believe that when the bank contacted him, it was the actual bank," Roger Lester, account director at United Kingdom-based Featurespace, told PYMNTS in a recent interview.

Featurespace specializes in adaptive behavioral analytics powered by artificial intelligence (AI) to fight fraud. Once again, behavioral analytics — combined with human insight — had saved the day.

ESTABLISHING ‘THE NORM’ IN BEHAVIORAL PATTERNS

The above story is not a rarity, unfortunately: These kinds of scams take place every day. The key to fighting them with behavioral analytics is to set a baseline of normal customer behavior and then watch for deviations, Lester explained.

“What we found to be the most effective is to profile and monitor good behavior,” Lester said. “The reason we’ve taken that approach is that if you’re monitoring or building your model [based on] confirmed fraud, you’re reacting only when a problem has occurred or happened. Because we focus on good behavior, we can act when we see a change in that pattern.”

Featurespace’s team of data scientists has been refining models of consumer behavior, determining which behaviors signal that a consumer is feeling confused when looking at an unfamiliar user interface.

“An example would be, let’s say, an elderly or young person who’s not familiar with the type of transactions you are asking them to do,” Lester explained. “You may see a hesitancy with which they’re navigating around their account.”

Featurespace’s model can detect when a different person has logged in to the customer’s account and is attempting to navigate through their records suspiciously, or even when a criminal is directing the user to take certain actions — all by watching for deviations from standard behavioral patterns.

AVOIDING ‘ALERT FATIGUE’

Behavioral analytics has benefited banks, merchants and consumers, Lester said, but there has been one downside: alert fatigue, in which consumers anticipate getting potential fraud alerts frequently and stop taking them seriously. FIs are combatting this by putting a new emphasis on ensuring that every alert sent is an indicator that something has indeed gone awry.

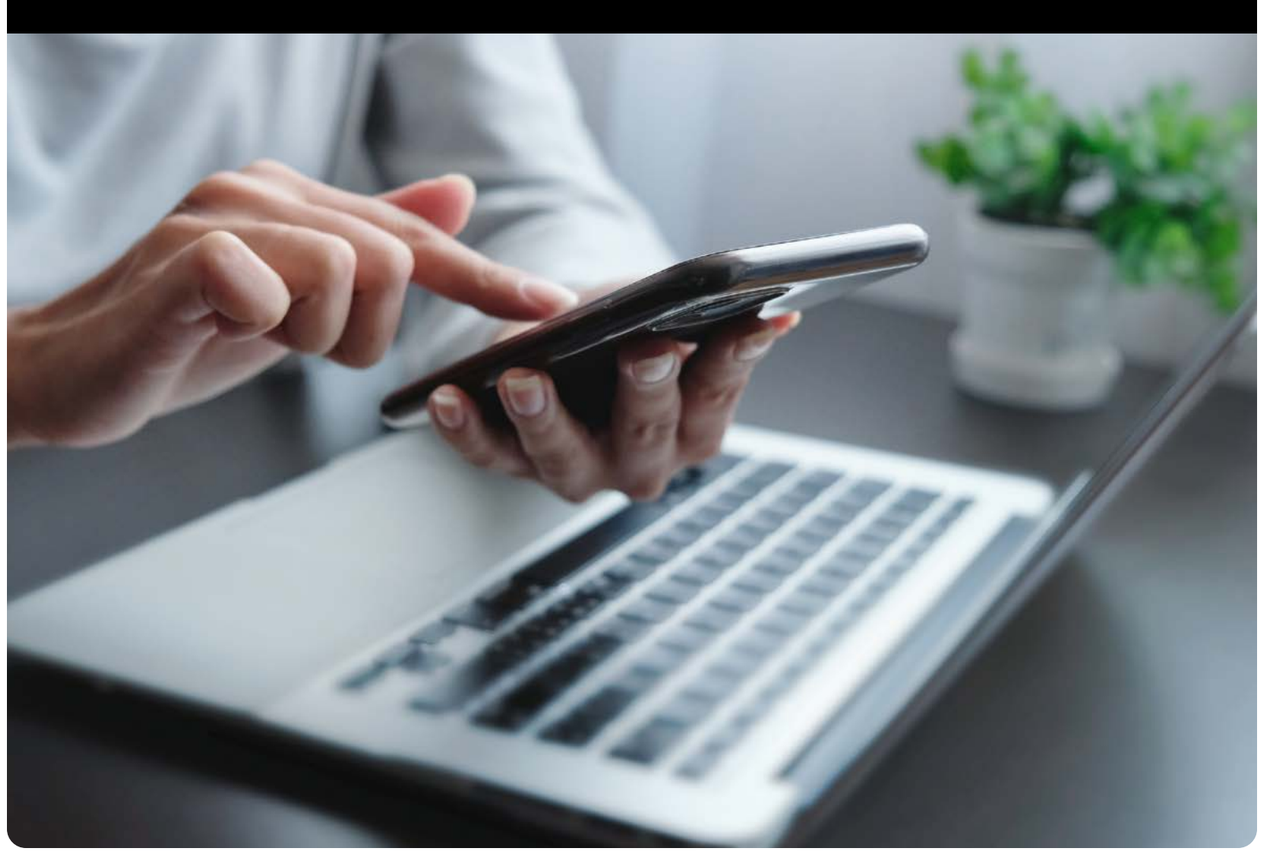
Additionally, he explained, some banks are watching for drops in activity or engagement, as that could be a sign, in the case of a business account, that the business is experiencing trouble or, in the case of a personal account, that the customer is less engaged and is considering switching banks. Either of these scenarios should prompt an outbound call to ensure that the FI is meeting the customer’s needs.

Overall, Lester noted, this technology has made operations smoother for everyone but fraudsters — including the one who impersonated the bank representative.

“I think AI behavioral analytics is definitely the way forward,” he said. “I have seen personally how much of a benefit that brings to everybody — the banks, their customers, the merchants, the whole industry in general. I see that only continuing in the future.”

PYMNTS Intelligence

Deploying Behavioral Analytics To **Smooth Friction Points In The Customer Journey**



PROTECTING AGAINST DIGITAL FRAUD IS A TOP PRIORITY FOR ORGANIZATIONS, CONSIDERING THE CYBERCRIME THREATS ARRAYED AGAINST THEM.

The average American has been harmed by at least seven data breaches since 2004, according to a recent study, and there have been more than 2.3 billion account compromises in the country during that same time. Any measure to reduce this massive tide of cybercrime is potentially a step in the right direction when it comes to protecting businesses and consumers.

Nevertheless, many of the existing measures designed to fight digital fraud ultimately end up doing more harm than good. Consumers are continually frustrated by obtrusive identity checks, verification interfaces and other measures aimed at ensuring they are who they say they are, with many would-be customers jumping ship for businesses with easier experiences. These simpler verification measures are often less effective at fighting fraud, however, resulting in increased cybercrime metrics.

Businesses must find a way to reduce these authentication obstacles without compromising security, and behavioral analytics offers a compelling double-edged solution. This month, PYMNTS Intelligence examines common friction points in the customer journey and how behavioral analytics can identify and adjust them while providing robust security.

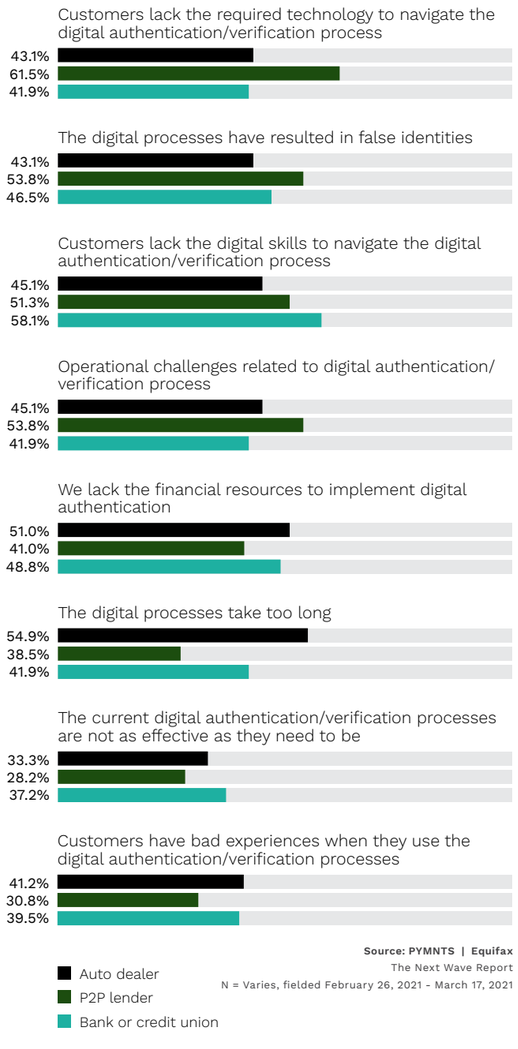
AUTHENTICATION COMPLICATIONS

Firms experience a range of challenges when authenticating their customers' identities. PYMNTS' research found that 55% of auto dealers, for example, said digital authentication processes take too long, and 54% of P2P lenders said their digital authentication processes often created false identities. Other complications included a lack of efficacy in digital authentication processes, operational challenges during authentication and a lack of customer knowledge when it came to verification. The most condemning finding, however, was that 41% of auto dealers, 31% of P2P lenders and 40% of banks and credit unions said their customers had bad experiences when using digital authentication processes.

FIGURE 1:

Digital authentication problems experienced by firms that plan to invest in digital authentication solutions

Share of digital authentication problems experienced by firms that plan to invest in digital authentication solutions



Source: PYMNTS | Equifax
The Next Wave Report
N = Varies, fielded February 26, 2021 - March 17, 2021

This last statistic is especially worrisome for merchants because of customers' propensity to abandon purchases — or businesses entirely — after subpar experiences. A recent study found that 83% of potential customers would leave a website that had a complex login process, with 49% saying such processes leave them frustrated and 21% saying they are too time-consuming. Cart abandonment is a particularly pressing issue among eCommerce merchants, with approximately 70% of transactions abandoned before the finish line. With a growing cornucopia of shopping options available to consumers, finding a new merchant is often much easier than navigating a complex authentication procedure.

Streamlining authentication processes is thus a key priority for businesses looking to reduce customer attrition. Behavioral analytics delivers on this need, not only due to its more seamless authentication procedure but also because of its ability to pinpoint customers' trouble spots and mark them for improvement.

LEVERAGING BEHAVIORAL ANALYTICS TO SOLVE AUTHENTICATION WOES

Behavioral analytics systems can offer a much more streamlined authentication approach than systems requiring active input from customers. The technology works by scrutinizing users' digital habits to separate genuine customers from fraudulent ones by deducing user intent based on behavior. It examines factors such as typing speed and mouse movement to determine if users are who they claim to be, detecting fraudsters with high accuracy.

In addition to making the authentication process easier, behavioral analytics systems can drill down on the exact friction points customers are grappling with and provide actionable data for company staff to improve them. The systems analyze how long it takes to fill out various forms, including which ones were left incomplete. The company can thus devote resources to streamlining these forms, such as by adding credit card autofill options or removing extra password entries. One company was able to reduce friction in a specific data field by 20%, for example, reducing cart abandonment, in turn, by 40%.

Providing a smooth user experience and protecting against fraud are often perceived as diametrically opposed goals, but this does not have to be the case. Behavioral analytics meets both objectives to score a win-win for businesses and customers.

NEWS & TRENDS

DIGITAL FRAUD TRENDS

AUTHENTICATION WEAKNESSES LED TO 80% OF ORGANIZATIONS EXPERIENCING A CYBERBREACH LAST YEAR

Data breaches have become commonplace in the business world. A recent report found that 85% of businesses experienced a cyberbreach in the past year, with the average organization seeing 3.4 during that time. The leading cause of these breaches was weak authentication systems, with 80% of financial service organizations experiencing a breach as a direct result of this deficiency. The average annual cost of these breaches was more than $2 million, and one-third of businesses affected said they lost customers to their competitors after the breach occurred.

Nevertheless, businesses do not see a problem with their existing authentication infrastructures. Ninety percent of victims thought their existing authentication approaches were sufficient, despite the data clearly demonstrating otherwise.

SHIFTING TO PRE-SUBMIT DATA COULD REDUCE FALSE POSITIVES AND CUSTOMER FRICTION

Most organizations rely solely on post-submit data such as passwords and biometrics to verify customers, but these can result in obtrusive interfaces or false positives and are largely ineffective against synthetic identity fraud. Many organizations are shifting to pre-submit data analysis instead, relying on how customers interact with these forms and determining if they are fraudsters by their swiping or typing patterns. This can potentially save billions in data breach losses.

A recent report found that more than 1,800 data breaches occurred last year, a 68% increase from 2020. Shifting to pre-submit data could result in a more convenient customer experience as well as greater protection from data breaches.

INCONVENIENT CUSTOMER EXPERIENCES

75% OF CUSTOMERS ARE LIKELY TO ABANDON A TRANSACTION DUE TO A SUBPAR DIGITAL EXPERIENCE

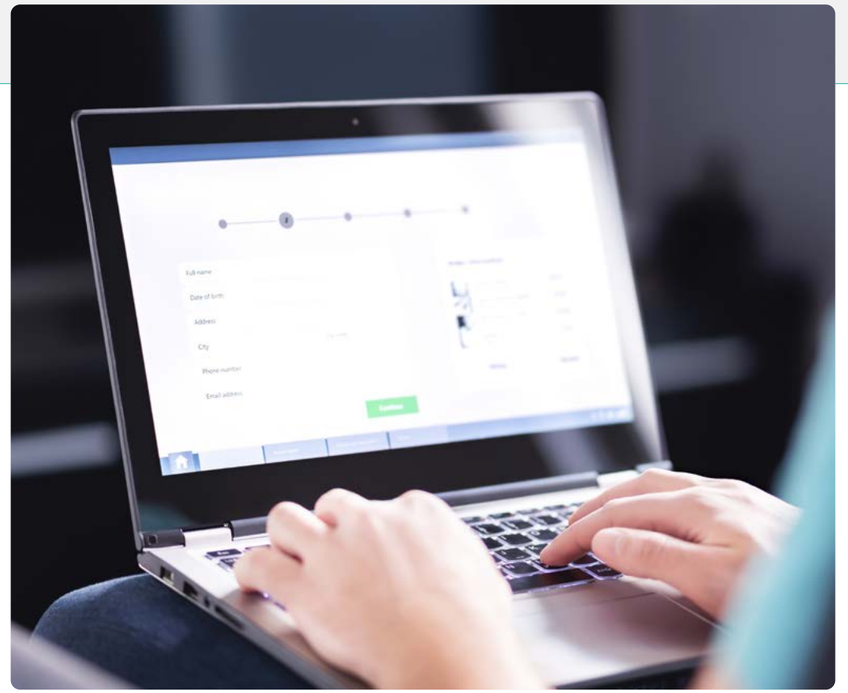
Convenience is king for customers, as digital interactions have become so routine that consumers have a wide variety of different businesses and storefronts from which to choose. A recent survey found that 75% of consumers are likely to abandon a transaction due to an issue with the digital experience, including authentication friction. Fifty-five percent of consumers said they are unlikely to return to a site or app after this bad digital experience, and 54% said they would trust a brand less.

Streamlined authentication is a key part of a smooth customer experience, but it is often at odds with secure verification. Many companies are leaning on behavioral analytics to provide both, thus preventing customer abandonment.

U.K. SEES PAYMENT DECLINES SPIKE BY 37% FOLLOWING SCA IMPLEMENTATION

Inconvenient authentication experiences come in many forms, but one of the most pervasive and irritating is payment declines. The United Kingdom saw a 37% increase in payment declines following the implementation of Strong Customer Authentication (SCA) rules in March, which mandated more stringent security protocols to prevent payments fraud, resulting in higher false positive and decline rates. More than one-third of businesses surveyed said their fraud rates had increased since the beginning of the pandemic, but 62% said they were dissatisfied with SCA's ability to prevent fraud.

Just 39% of businesses felt that SCA did its job effectively, while 29% said the regulations needed to go further to prevent fraud. Meanwhile, 33% of respondents said SCA resulted in a worse customer experience. Behavioral analytics could be a more effective means of transaction verification than current SCA requirements.



33% OF SUBSCRIBERS ARE LOST IN THE FIRST 24 HOURS, STUDY FINDS

Annoying customer verification can have disastrous effects on companies' long-term growth, and nowhere is this more apparent than in subscription commerce. A recent study found that nearly one-third of subscribers to any given business decide to unsubscribe within the first 24 hours after signing up, a phenomenon known as churn. This churn can occur for many reasons, but one of the most likely is an inconvenient customer experience. Another 40% of customers are known as sleepers, those who have not visited the website within the past 30 days and are also likely to churn. This group relies on new and engaging content to bring them back to the fold, but the 24-hour group will require a smoother customer experience. Enabling behavioral analytics for authentication could be a vital method for retaining this group past the first day.

BEHAVIORAL ANALYTICS

TRACKER®

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.

ABOUT

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