ALTERNATIVE PAYMENTS TRACKER®

MAY 2022

PYMNTS.com | Socure

Read the previous edition

APRIL 2022

Alternative Payments Tracker®

ALTERNATIVE PAYMENTS TRACKER®

PYMNTS.com | Socure

ACKNOWLEDGMENT

The Alternative Payments Tracker® was produced in collaboration with Socure, 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

eCommerce has made exponential gains throughout the past decade, receiving a considerable boost in the past two years from the pandemic's shutdown of brick-and-mortar retailers. Experts estimate that consumers in the United States alone spent more than $933 billion with eTailers in 2021. This number is likely to increase in the coming years as more and more businesses expand online.

A growing digital presence means a rise in digital fraud, however, as each customer shopping online represents a potential entry point for a bad actor looking to steal customer or corporate data or funds. Sometimes the bad actors are the customers themselves, exploiting charge-back or return policies to score merchandise without paying for it. A recent study found that more than 17% of all eCommerce transactions during the 2021 holiday shopping season were fraudulent, for example — a staggering loss.

eTailers are pulling out all the stops to keep this fraud to a minimum, employing digital identity protocols to verify that customers are who they say they are. One of the most effective methods eCommerce marketplaces can use to prevent identity fraud is multifactor authentication (MFA), which works by requiring more than one identifying detail when an individual is logging in or making a purchase. The most popular example of this is a text message sent to the user's phone, ensuring that the customer is legitimate and not a bad actor armed with a stolen password.

This method can be unpopular, however. Many consumers decline this extra step, given the option, and even switch eTailers if they face too much friction at checkout. Customers also have data privacy concerns about giving large companies their personal cell phone numbers. A recent study found that just 37% of companies require MFA for their customers, fearing that this extra friction could result in lost sales. With MFA preventing more than 99.9% of attacks that rely on stolen credentials, the savings could more than make up for any customer hesitancy. It will be up to each business and consumer to determine whether the sacrifice in convenience is worth it.

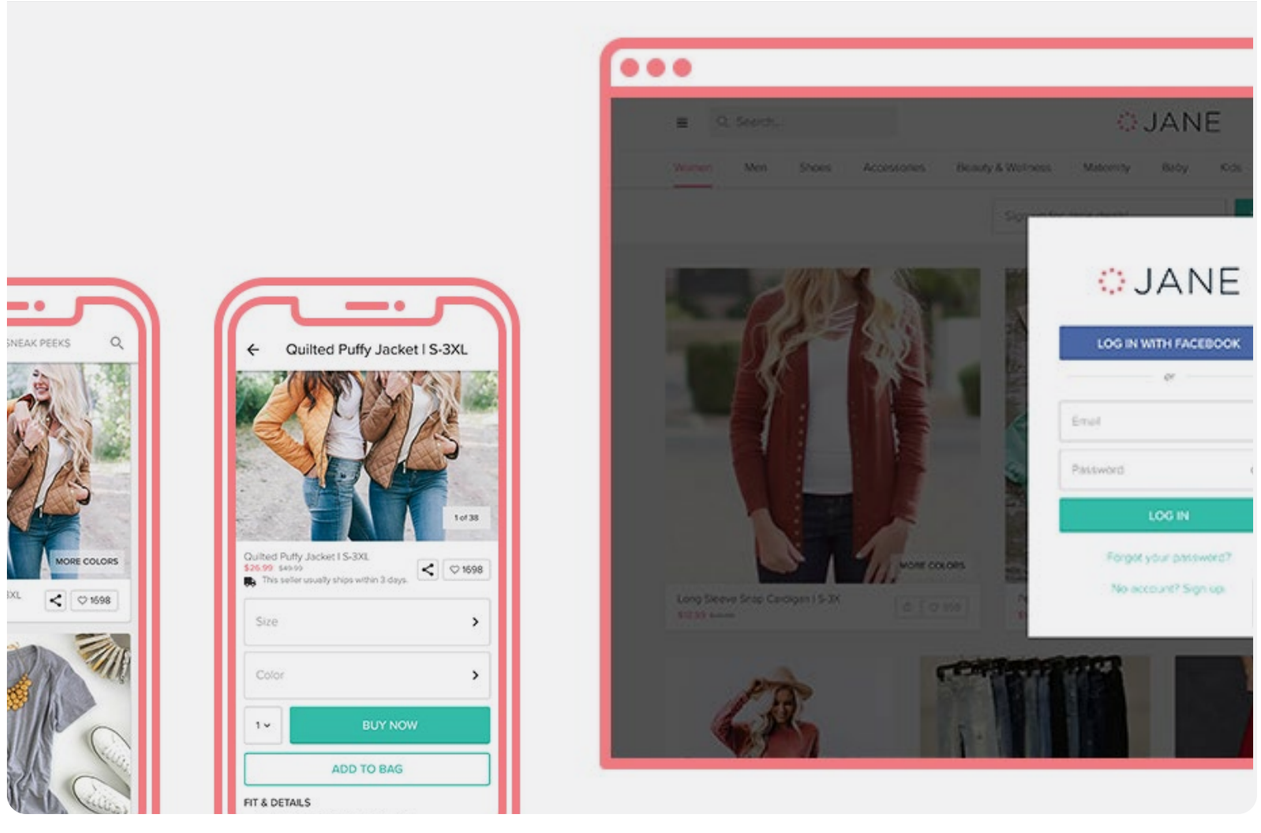
This edition of the Alternative Payments Tracker®, a PYMNTS and Socure collaboration, examines how fraudsters attempt to scam eCommerce marketplaces and their customers. It also explores how digital identity systems can help eTailers reduce fraud without introducing frictions into the customer experience.

Thought Leadership Team

PYMNTS.com

Feature Story

JANE On Protecting Retail Customer Data With **Digital Identity Verification**



eCOMMERCE MARKETPLACES ARE AT THE FOREFRONT OF FRAUD PREVENTION.

These marketplaces must be to protect the treasure trove of data they host, data that bad actors work tirelessly to get their hands on. Credit card information, usernames, passwords and the merchandise itself are all targets. Fraudsters are pulling out all the stops to exploit them for their own gains.

Robust digital identity tools are the lynch-pin to ensuring that this data is kept safe and secure. One company working to keep its customers' data safe is fast-fashion retailer Jane, which deploys an MFA-based approach in its cybersecurity stack.

"My biggest hope is that we can establish, as an eCommerce industry, a more seamless, secure and less invasive interaction with the consumer," said Mark Spencer, senior vice president of commercial operations for Jane. "[It's all about] informing [customers] and really ensuring that [their] online safety is top of mind in the very beginning."

Spencer provided PYMNTS an inside look at the most common threats eCommerce marketplaces face daily and how Jane leverages digital identity protocols for cybersecurity.

FRAUD THREATS

eCommerce storefronts face a massive array of fraud threats, but one of the most concerning is the use of botnets. Hackers deploy countless automated programs to flood checkout pages and onboarding forms in an effort to overwhelm automated defenses and score customer data or free merchandise.

“The bots try to stage [account takeovers] so they can change the delivery addresses,” said Spencer. “It’s primarily aimed at the luxury products that we carry, as well as the electronics.”

Fighting these automated systems can be extraordinarily difficult, though, as fraudsters are innovating and refining their techniques just as quickly as cybersecurity staff can develop defenses. Every new defense means a new workaround, resulting in cybercriminals and cybersecurity experts locked in an endless arms race.

“It’s a cat-and-mouse game: As quick as we find systems to stop fraudulent activity or make life easier for customers, there are bad actors that are out there looking to circumvent it,” said Spencer. “There’s a lot of time, money and effort [being] spent on keeping consumer data and consumer information private.”

Some of the most effective methods involve digital identity verification techniques. Jane deploys several different methods to keep customers safe.

PROTECTING AGAINST FRAUD VIA CUSTOMER VERIFICATION

The most effective digital identity tool against fraud, Spencer explained, is MFA, which requires customers to enter a code sent via text message along with their password. This method dramatically limits the damage a bad actor can do by purchasing credentials from a data breach, as they would have to find a way to intercept the text message as well. Jane also cross-references credit card verification values (CVV) to ensure the card is in possession of the customer and is not a stolen card number.

“We have [two-factor authentication], and when we feel that something is not right, we ask for the CVV to be reinforced again at checkout,” said Spencer. “There are also factors that alert one of our systems to ask for the consumer to enter in something additional. For example, as soon as we see a delivery address change, we will be asking them for a revalidation of their credit card details.”

There is a constant tension between customer security and streamlined experiences, however, with verification requirements adding to customer inconvenience. Spencer hopes that the next step in digital identity innovation could ease this conflict.

“[eCommerce is looking for] a more streamlined verification process that doesn’t detract from the actual process of checking out,” he said. “We’re all really wanting to find ways [to have] less clicks on the path to checkout. I think the more that organizations can come together on a central database of verified data for the payment processes, the closer to utopia we could be — where we could make one determination via a central [application programming interface], and that’s it.”

Closer cooperation between businesses will be necessary to make this dream a reality. Until then, organizations will have to use the best tools available to protect against fraud, and digital identity protocols are a key facet of this defense.

PYMNTS Intelligence

How eCommerce Marketplaces Can **Leverage Digital Identity Protocols** To Prevent Fraud

eCommerce fraud is a quickly growing problem, with bad actors attempting to steal customers' data, corporate funds and goods on a daily basis. A recent study found that more than 17% of all global eCommerce transactions during the 2021 holiday shopping season were fraudulent, a 25% increase from the rest of the year. This jump represented a microcosmic example of fraud trends around the world during the past several years, with more online shopping resulting in more entry points for fraud.

eTailers are scrambling to protect themselves and their customers from fraud, not just to avoid stolen data and funds but to preserve customer loyalty and prevent abandonment due to perceived cybersecurity weakness. Many eCommerce marketplaces leverage digital identity protocols such as MFA, which has an impressive fraud prevention record but comes with its own drawbacks. This month, PYMNTS Intelligence explores the nature of eCommerce fraud in recent years and how techniques such as MFA have their ups and downs when keeping businesses and customers safe.

HOW FRAUD AFFECTS eTAILERS

Bad actors ply a staggering variety of fraud tactics against eCommerce merchants, but the one that seems to worry fraud prevention professionals the most is identity theft. A recent survey found identity theft to be merchants' most common fraud concern, cited by 71% of respondents. Bad actors committing identity fraud exploit eCommerce websites, stealing customers' identities, and then leverage those stolen identities to make illicit purchases, often by implanting fake checkout pages that can harvest customers' email addresses and payment information. Businesses' difficulties in authenticating customers exacerbate this fraud. Half of all eCommerce companies in the U.S. report having trouble authenticating customers on browsers, and 58% struggle to verify mobile users, even when using advanced systems that incorporate artificial intelligence (AI) or machine learning (ML).

Digital fraud's impact is not limited to stealing funds and data, as it can also have long-term ramifications for customer loyalty. Customers are likely to abandon eTailers entirely after experiencing data theft or fraud, with 65% of consumers in a recent PYMNTS study saying they would be "slightly" or "not at all" likely to continue using merchants after having their data stolen. Baby boomers and seniors were the most likely to abandon merchants after a security incident at 80%. This willingness to switch merchants after security incidents is apt to increase, as 48% of eCommerce shoppers said they were more worried about data security now than before the pandemic began. Thirty-six percent of consumers already base their choice of payment method on the likelihood of theft, and this number shows no sign of declining.

TABLE 1:

HOW eCOMMERCE SHOPPERS WOULD REACT TO DATA THEFT AND FRAUD

Share who are "slightly" or "not at all" likely to continue using merchants after experiencing data theft or fraud, by generation

	SAMPLE	Generation Z	Millennials	Bridge millennials	Generation X	Baby boomers and seniors
• Any	64.9%	52.8%	53.2%	52.4%	64.3%	80.2%
• Only data theft	3.5%	10.6%	3.2%	3.3%	1.7%	2.4%
• Only fraud	7.6%	7.5%	8.3%	7.7%	8.3%	6.4%
• None	24.1%	29.2%	35.3%	36.6%	25.8%	11.0%

Source: PYMNTS.com

Robust digital identity protocols are some of the most effective ways for eCommerce merchants to stop fraud and maintain customer loyalty.

DEPLOYING DIGITAL IDENTITY TO PREVENT FRAUD

One of the most efficacious methods for preventing identity fraud is MFA, which works by requiring more than one identifying detail when logging in or making a purchase. The rule of thumb for effective MFA is to provide verification by "something you know, something you have and something you are," representing, for example, a password, an SMS code sent to customers and a biometric identifier, respectively. The typical MFA system requires two of these factors, and studies have found that MFA can prevent more than 99.9% of attacks that rely on stolen credentials.

There are some potential drawbacks of implementing MFA, however. Customers naturally desire the most seamless login method possible, and MFA requires an extra step that can add friction. Studies have found that many consumers decline this extra step if it is optional, even choosing a different eTailer if they face too much friction at checkout. Customers have also expressed data privacy concerns with giving large companies their personal cell phone numbers or tying their data to their smartphones, as the loss of a device then means the loss of the ability to verify one's identity entirely.

MFA's efficacy rate speaks for itself, however, and the savings in preventing data breaches, fraudulent purchases and lost customer loyalty could more than make up for any customer hesitancy. MFA's proliferation in other environments, such as workplaces, is bringing more and more customers into the fold every day, and eTailers could see this hesitancy slip away as MFA becomes more mainstream.

NEWS & TRENDS

REDUCING RISK WITH DIGITAL IDENTITY

TWO-FACTOR AUTHENTICATION IS EFFECTIVE, BUT ITS USE IS LIMITED AMONG BUSINESSES, STUDY FINDS

Two-factor authentication, which consists of users logging into online services with a password and a code sent via SMS, has proven to be an effective deterrent for fraud, but many companies opt out of its use. A recent study found that just 37% of companies require it for their customers' accounts, as well as 31% of charities. Its exact usage rate varies by field, with two-thirds of businesses in information and communications mandating it compared to just one in five food and hospitality businesses.

The latter field may think it is a less popular fraud target, but customers still have data on systems that fraudsters could steal. Bad actors are known to steal high volumes of passwords via phishing, for example, and the use of two-factor authentication could make this tactic far less effective as the fraudster would need to intercept the SMS as well.

BUSINESSES PLAN TO INVEST IN CYBERSECURITY TO PROTECT AGAINST REMOTE WORK EXPOSURE RISKS

Countless businesses shifted some or all of their workforce to be remote in the past two years to facilitate social distancing during the pandemic, and there have been many lessons learned about what remote work means for corporate cybersecurity. Companies found that employees who accessed office servers remotely offered fraudsters an entry to corporate systems, resulting in several security concerns. A recent survey of small to mid-sized businesses (SMBs) found that 56% of companies were concerned with the risk of data breaches, 57% were worried about hacking or intrusions, 54% were concerned with viruses and 50% said they were worried about identity theft.

Companies plan to invest in several areas to either continue their remote work or return employees to the office, with 31% saying they are developing technology to facilitate a split or hybrid work model. Half of the businesses surveyed said they have reassessed opportunities for improvement since the pandemic began, and cybersecurity should be a key focus if employees continue working from home.

SOCURE PARTNERS WITH DIBBS FOR KYC AND IDENTITY VERIFICATION

Businesses are pulling out all the stops to keep hackers at bay with advanced digital identity solutions. Blockchain marketplace Dibbs recently partnered with digital identity provider Socure in one such effort, with Dibbs adopting Socure's ID+ solution as its identity verification and fraud platform of choice. The system leverages a single application programming interface (API) and no-code customization dashboard to customize the integration, accelerating implementation. This will allow new customers to be verified more quickly, with Dibbs expecting a 20% boost in first-time deposits due to the added convenience.

ALTERNATIVE PAYMENT **DEVELOPMENTS**

CRYPTOCURRENCY FRAUD PREVENTION BEGINS AT ONBOARDING WITH FRICTIONLESS SOLUTIONS

An estimated 40 million U.S. consumers, or 16% of the adult population, have invested in, traded or used cryptocurrencies, indicating how digital currencies are becoming a widely accepted form of global value exchange, according to a recent PYMNTS 2022 Outlook eBook. There is growing recognition of the value of crypto as an alternative form of payment, despite its challenges of being used in illicit activities such as money laundering. Crypto exchanges are often targets of fraud due to the industry's lack of regulatory oversight and need for formal guidelines, something that the White House has been working on to establish crypto's credibility.

Crypto services must implement identity verification solutions at the account opening stage to help prevent fraud, but these may sometimes introduce frictions for consumers that can turn them away. Partnerships with digital identity providers can help these services offer frictionless experiences starting at customer onboarding to help drive growth. Digital identity provider Socure's platform, for example, delivers auto-approval rates of as much as 98% for mainstream populations, and up to 94% for hard-to-identify populations such as Gen Z, millennials, credit invisible, thin-file and new-to-country, according to the company's founder and CEO Johnny Ayers. The platform can also passively capture up to 90% of fraud in the riskiest 3% of users, he said.

CENTRAL BANK SURVEY FINDS CONTACTLESS P2P PAYMENTS TO DRIVE ADOPTION OF DIGITAL EURO

Research into implementing a digital Euro continues in Europe, with consumers making known their top priorities on the subject. Participants in a recent study from the European Central Bank said their ability to make contactless peer-to-peer payments is a top priority as the worldwide growth of digital payments continues.

Consumers surveyed showed a desire for the ability to confirm and give permission before payment but varied in the authentication methods they desired. Tech-savvy consumers were more likely to express the need for biometrics authentication using fingerprint, face or iris scanning, while others preferred a combination of biometrics and a code. Multilevel and QR code-based authentication were unpopular choices for an authentication method.

CRYPTO COMMUNITY RAISES LEGAL CONCERNS AS SHOPIFY INTEGRATES BITCOIN PAYMENTS

With cryptocurrency usage continuing to grow, more eCommerce merchants around the globe are looking to join in. eCommerce platform Shopify recently announced a partnership with payment app Strike, bringing Bitcoin payments into the fold, but those in the crypto community are expressing concerns over the move.

The new integration will allow U.S. merchants on the eCommerce platform to accept Bitcoin payments from consumers worldwide and enable users to pay with the digital currency without going through the know your customer (KYC) process, bringing legal and regulatory issues. Consumers spending Bitcoin without the KYC process can avoid paying taxes, a move causing regulators to react by creating reporting requirements for the eCommerce platform.

ALTERNATIVE PAYMENTS 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.

Socure

Socure is the leading platform for digital identity verification and trust. Its predictive analytics platform applies artificial intelligence and machine learning techniques with trusted online/offline data intelligence from email, phone, address, IP, device, velocity and the broader internet to verify identities in real time. The company has more than 750 customers across the financial services, gaming, healthcare, telecom and eCommerce industries, including four of the top five banks, seven of the top 10 card issuers, three of the top MSBs, the top payroll provider, the top credit bureau, the top online gaming operator, the top Buy Now, Pay Later (BNPL) providers and more than 100 of the largest FinTechs. Marquee customers include Chime, SoFi, Varo Money, Public, Stash and DraftKings. Socure customers have become investors in the company, including Citi Ventures, Wells Fargo Strategic Capital, Capital One Ventures, MVB Bank, Voyager and Synchrony. Additional investors include Accel, funds and accounts advised by T. Rowe Price Associates, Inc., Bain Capital Ventures, Tiger Global, Commerce Ventures, Flint Capital, Scale Venture Partners, Sorenson, Two Sigma Ventures and others.

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