DIGITAL FRAUD TRACKER®

MARCH 2022

PYMNTS.com | DATAVISOR

DIGITAL FRAUD TRACKER®

Read the previous edition

FEBRUARY 2022

Digital Fraud Tracker®

PYMNTS.com | DATAVISOR

ACKNOWLEDGMENT

The Digital Fraud Tracker Tracker® was produced in collaboration with DataVisor, 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

Credit card fraud is a problem that affects banks, merchants, credit card providers and consumers alike, with fraudsters deploying a wide variety of tactics to drain customer accounts of funds and data. This type of fraud can be divided into two categories: card-present (CP) fraud, in which the bad actor has physical possession of the stolen card and is using it to make a purchase at the point of sale (POS), and card-not-present (CNP) fraud, in which the bad actor has credit card information but not the card itself and is using it for a digital purchase.

Card providers have developed several defenses against card fraud, including multifactor authentication (MFA), biometrics and behavioral analytics, but many of these methods have proven ineffective or will quickly become so when fraudsters find loopholes or workarounds. One promising step was the development of 3D Secure, an extra authentication layer to ensure that card users were who they said they were. This protocol faced criticism, however, due to its requirement for additional customer authentication that caused friction and cart abandonment.

Fixing these flaws is the primary goal of 3D Secure 2.0, which leverages authentication data, artificial intelligence (AI) and machine learning (ML) to review transactions made by payment cards. This additional layer is largely seamless to customers, but it can reduce credit card fraud by up to 40% while approving as much as 95% of transactions instantly without any needed inputs from the consumer.

Merchants feel the benefits as well in the form of reduced cart abandonment. Almost 70% of purchases are abandoned before the finish line, largely due to frictions in the checkout process. Reducing these frictions through more seamless fraud detection programs such as 3D Secure 2.0 could go a long way toward reducing cart abandonment rates. The protocol also enables a collaborative data exchange among card issuers, merchants and banks, reducing overall dollars lost to fraud by up to 40%.

This edition of the Digital Fraud Tracker®, a PYMNTS and DataVisor collaboration, delves into the ways fraudsters stage credit card fraud both in person and online and the steps institutions have taken to try to curb this threat. It also examines how the implementation of 3D Secure 2.0 has improved fraud prevention protocols for banks, merchants, credit card providers and individual consumers while offering a more seamless experience for credit card users.

THOUGHT LEADERSHIP TEAM

PYMNTS.com

Feature Story

American Express On How 3D Secure 2.0 Threads The Needle Between **Fraud Protection And Customer Convenience**

CREDIT CARD FRAUD IS ENDEMIC IN THE U.S. AND ABROAD, AND BANKS AND PROVIDERS HAVE WORKED TIRELESSLY FOR DECADES TO MINIMIZE ITS IMPACTS.

The rise of eCommerce has made this task only trickier as bad actors can now spoof thousands of credit cards at once and use them almost instantaneously.

The credit card industry thought it had a good handle on the problem with the introduction of 3D Secure in 1999. The protocol was leveraged by many card providers under various names: Visa Secure, Mastercard SecureCode and American Express SafeKey, among others. This system was effective at preventing fraud, but it inadvertently created issues with customer seamlessness, according to JJ Kieley, vice president of payment products at American Express.

“The key thing that they were focusing on was an interoperable system, so that merchants and card issuers could use a standard protocol of sorts,” Kieley said in a recent interview with PYMNTS. “What it focused on was authenticating a customer at checkout. Merchants would send information to the issuer through 3D Secure, and through that authentication, they can see whether or not there is a fraudster trying to use a compromised card or if it’s actually the card member.”

This authentication process was extremely time-consuming, leading to the development of 3D Secure 2.0 in 2016. Kieley offered PYMNTS an inside look into the drawbacks of the first iteration, what led issuers to reconsider their approaches and how 3D Secure 2.0 improves on the original version.

THE DRAWBACKS OF 3D SECURE

The original 3D Secure had a number of deficiencies, especially when it came to customer and merchant satisfaction. The authentication system was obtrusive and slow to process, and it also required additional active input from the customer to make transactions go through.

“You click a button saying ‘checkout,’ and then the merchant sends the transaction information to the issuer of that card,” Kieley explained. “Then the issuer will decide whether or not we need to send some type of notification to the card user using the information we have with the

card number, and then the customer will get a pop-up that'll say, 'American Express is trying to authenticate your transaction. Please enter the code that we just sent to your phone or email.'"

Customers on eCommerce websites frequently were annoyed with the obtrusiveness of this extra step, often abandoning transactions entirely rather than checking their email inboxes or phones for the extra codes. This, in turn, irritated merchants because they were losing otherwise surefire sales.

"Merchants knew it was an effective tool in preventing fraud, but they had to make the decision of whether to protect [themselves] against fraud or create friction that could lead to abandonment of transactions," he said. "It really wasn't a great experience."

Card issuers took these complaints to heart when developing the new iteration of their authentication system, 3D Secure 2.0, which aims to improve customer experiences without compromising fraud detection.

HOW 3D SECURE 2.0 IMPROVES UPON THE OLD

Making customers' and merchants' experiences more streamlined and convenient was a top priority when developing 3D Secure 2.0, Kieley explained. Instead of requiring an extra authentication step on the user's side, the new system leverages more data points to make a fraud determination behind the scenes.

"The reception on the consumer side has been very positive," Kieley said. "They thought that because of regulation, they [were] going to have to go through an authentication process like they experienced with 3D Secure 1.0, but now they're getting a much better experience on it."

The new system's other major improvement is its flexibility. 3D Secure's first iteration worked only on web browsers, meaning that smartphone shoppers needed to navigate a small, unoptimized authentication screen on their phones' internet apps. Now, the system can be implemented natively on eCommerce apps.

"The other benefit is that the experience that the customer goes through got a big step up," Kieley said. "3D Secure 1.0 only supported browser-based payments and browser-based pop-ups, so [it] really wasn't a great experience. [3D Secure] 2.0 supports both browser and native apps, which means lower friction and a better experience."

Fraud will continue to be a concern for card-based payments, especially as eCommerce usage grows during the pandemic. But with 3D Secure 2.0, card issuers, merchants and consumers can all access a more secure shopping experience with minimal amount of friction.

Q&A

YINGLIAN XIE
CEO and co-founder
DATAVISOR

What are 3D Secure and 3D Secure 2.0? What were some concerns about 3D Secure, and how does 3D Secure 2.0 address those concerns?

3D Secure 2.0 is a credit card security protocol designed to prevent the fraudulent use of credit card numbers. The '3D' stands for '3 Domain,' which consists of the card issuer's domain, the acquirer's domain and the interoperability domain. Collecting data from these three domains supports the authentication of cardholders during card-not-present transactions, [such as] all online transactions, over-the-phone payments [and so on].

The 3D Secure protocol is developed and managed by EMVCo, which is jointly owned by the major credit card brands Visa, Mastercard, American Express, Discover, UnionPay and JCB.

The first version of this protocol, 3D Secure, was first deployed 17 years ago — before the introduction of digital wallets, mobile payments and app-based shopping. The introduction of 2.0 is a new specification of the original protocol that will take into account new payment channels, advancements in digital security and a better user experience that will improve the speed and reliability of eCommerce authentication.

3D Secure 2.0 implementation is expected to help issuing banks and merchants achieve compliance with Europe's revised Payment Services Directive and strong customer authentication requirements. What are some of the benefits of 3D Secure 2.0 to merchants, issuers and consumers?

3D Secure 2.0 offers a faster, simpler and smarter way to process and authenticate transactions. This, combined with mobile-first alignment, creates a better eCommerce experience for issuers, merchants and consumers.

eCommerce authentication can be made with greater confidence when entities are allowed to share more contextual data surrounding each transaction. The more honest transactions approved, the more the issuer stands to gain through transaction fees from the merchant and potential interests from the consumer.

Merchants experience higher cart abandonment when shoppers cannot seamlessly complete the checkout process. The other concern for merchants is too many hurdles for customers to jump through as merchants try to protect themselves from fraud. Both of these challenges are diluted with 3D Secure 2.0. A frictionless checkout experience is estimated to reduce checkout times by 85% and shopping cart abandonment by 70%, all while ensuring fraud risks are at a minimum.

Consumers can gain more confidence in conducting transactions via mobile devices, thanks to a more streamlined experience and stronger security controls. Rather than keeping up with multiple passwords and the hassle of resetting forgotten passwords, users can be authenticated in other ways, such as temporary passwords. This eliminates the risk that a password might become compromised, which can lead to stolen consumer data.

Q&A

How does the 3D Secure 2.0 protocol insert itself into existing card payment processes? What parties are affected and how does information flow between them?

Each transaction under the 3D Secure 2.0 protocol shares information between four entities: the cardholder, the 3D Secure server, the directory server and the issuing bank. More data can be collected, shared and compared during each transaction. This data includes information about the cardholder's browser or mobile device, their account history with a specific merchant and other details that are passed on to the issuing bank. Responses from the issuing bank are returned along the same route. The exceptions are challenge messages, which are sent directly to the cardholder from the issuing bank in the event a challenge is necessary.

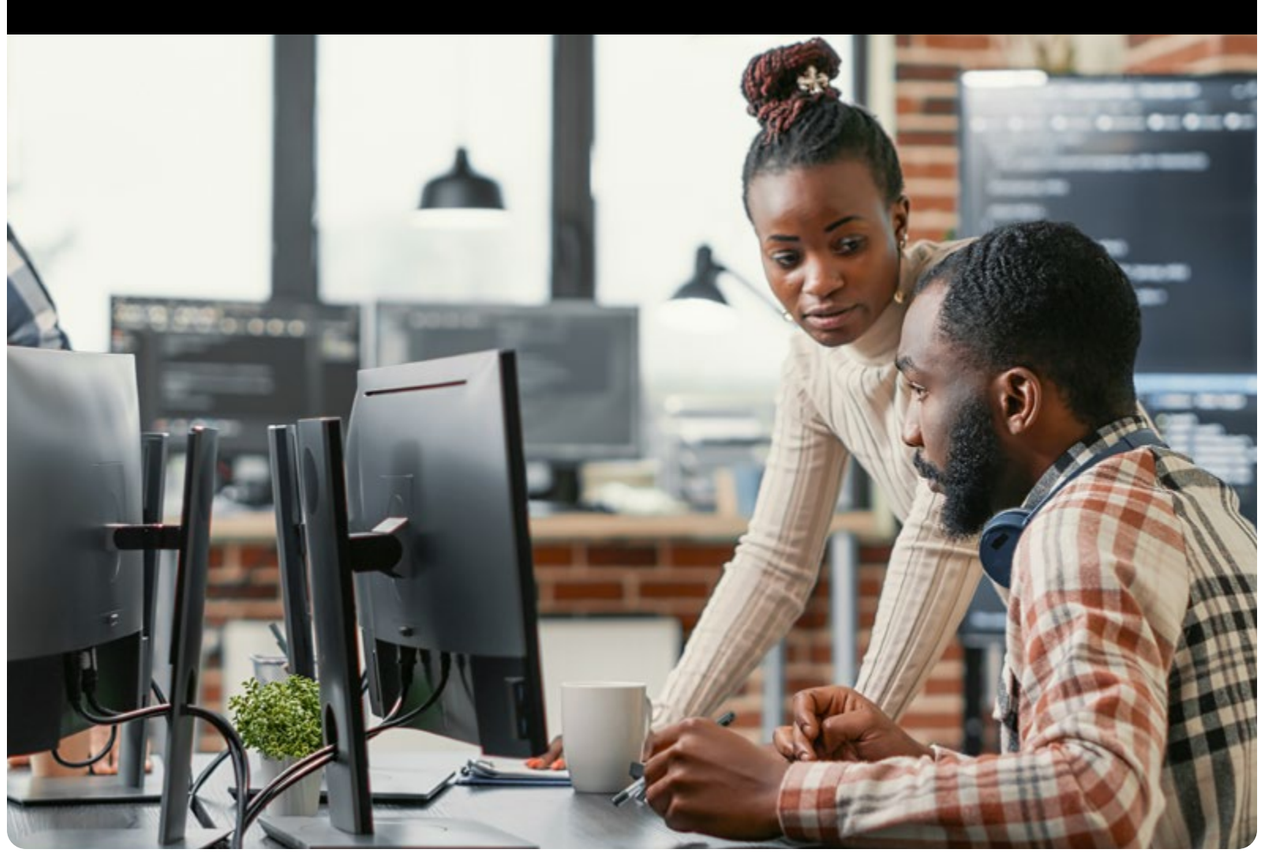
Here's how a transaction flows with 3D Secure 2.0:

1. First, the cardholder enters their payment details.
2. Then, the merchant's 3D Secure server receives the data and packages for sending to the issuer for authentication.
3. The issuer's 3D Secure server assesses the data for fraud risk and may require the cardholder to verify their identity [with] a one-time password — typically only 5% of transactions.
4. Once a cardholder has been authenticated, the issuer sends the decision to the merchant.
5. Finally, the merchant authorizes or declines the transaction based on the decision from the issuer.

As this process highlights, contextual data is at the heart of 3D Secure 2.0. More information is used to make authentication decisions, which can reveal a transaction's potential fraud risk. Eliminating friction for good customers allows issuers, merchants and consumers to thrive.

PYMNTS Intelligence

How 3D Secure 2.0 Can Help Merchants, Banks And Issuers **Put A Stop To Card Fraud**



Credit card fraud is a pressing issue for consumers, merchants, banks and card providers, costing a total of $32 billion in 2021 alone. This number is expected to swell to $38.5 billion by 2027, primarily fueled by an increased reliance on online shopping. Fraudsters perpetrating schemes online can conduct payment card fraud digitally en masse without the difficult task of having to steal and use credit cards in person.

While merchants, banks and card providers have leveraged sundry techniques in an attempt to curb credit card fraud — including MFA, biometrics and behavioral analytics — many of these methods have proven subpar or vulnerable to loopholes or workarounds, especially when used individually. Many card issuers deployed 3D Secure to prevent this fraud but ran into issues regarding customer convenience and seamlessness.

3D Secure has seen massive improvements since, however, with the introduction of the 3D Secure 2.0 protocol in 2016. In this month's PYMNTS Intelligence, PYMNTS explores how 3D Secure 2.0 works, what makes it superior to its first iteration and how implementing this security protocol can benefit banks and merchants.

> "3D Secure 2.0 can reduce credit card fraud by up to **40%** while approving up to **95% of transactions instantly."**

AN OVERVIEW OF 3D SECURE 2.0

3D Secure 2.0 adds a layer of protection for online purchases, leveraging authentication data, AI and ML to review transactions made by payment cards and then either allow them to proceed or flag them as suspicious. It does not rely on passwords or other knowledge-based authentication, thus preventing fraudsters from compromising customers' credentials. It also eliminates the need for an additional customer-facing security layer, meaning consumers are not forced to encounter authentication-related friction that could result in transaction abandonment. One study found that 3D Secure 2.0 can reduce credit card fraud by up to 40% while approving up to 95% of transactions instantly — all without added consumer input.

The new system offers several advantages over its predecessor, with the most obvious being more seamless integration with mobile devices. The system relies on a behind-the-scenes security layer rather than additional browser redirects and formatting, which may have worked well on full-size monitors but were challenging to navigate on small smartphone touchscreens. 3D Secure 2.0 also works within apps rather than only browsers, offering a more seamless shopping experience for consumers using these apps.

3D Secure 2.0's other major advantage is its speed, with Visa finding that the time to checkout has been improved by as much as 85% when the protocol is in play. This can be attributed to the system's more accurate fraud identification capabilities, as it flags just 5% of transactions as potentially fraudulent and in need of further authentication.

The consumer-facing benefits of this new protocol are apparent when compared to its predecessor, but it also has many advantages for banks and merchants.

HOW 3D SECURE 2.0 BENEFITS BANKS AND MERCHANTS

The biggest single benefit banks and merchants will experience as 3D Secure 2.0 becomes more widespread is a dramatically streamlined customer experience that removes many of the obstacles that customers have faced when transacting. This, in turn, is expected to reduce eCommerce cart abandonment dramatically. Consumers abandon nearly 70% of purchases before reaching checkout and clicking "pay," largely due to frictions during the purchasing process. Reducing these frictions via more seamless fraud detection measures such as 3D Secure 2.0 could go a long way toward solving this issue.

Another major benefit of 3D Secure 2.0's implementation is that it enables a collaborative data exchange between card issuers, merchants and banks. One case study of a bank in the Middle East, which saw 24% of its total transaction volume occurring via CNP transactions, found that the exchange of risk assessment data from 3D Secure 2.0-enabled transactions at eCommerce merchants reduced its overall fraud losses by 40%. The bank observed several other benefits, with customer service calls being reduced by 95%, customer complaints going down 25% and customer checkout times being reduced by 80%.

Merchants have also benefited because 3D Secure 2.0 shifts the liability for fraud away from retailers and onto banks, which typically have much more capacity to deal with such incidents. Merchants also report that they have experienced significant time savings, as they are no longer on the hook for fraudulent chargebacks and staff no longer have to field fraud complaints.

3D Secure 2.0 is a nascent development compared to many other technologies and measures dealing with fraud prevention, but it has already afforded numerous benefits to banks, merchants, card issuers and individual consumers in the past six years. As the technology matures, additional benefits are likely to emerge as more merchants and banks capitalize on its functionality in the fraud-prevention space.

NEWS & TRENDS

DIGITAL FRAUD TRENDS

TWO-THIRDS OF COMPANIES HAVE FALLEN VICTIM TO EXTERNAL FRAUD IN THE PAST 12 MONTHS

Untold billions of dollars have been spent on fraud prevention, but cybercrime continues to wreak havoc on businesses of all sizes. A recent survey found that 67% of companies have been victimized by external fraud within the past 12 months, with 42% of these victims reporting they experienced up to a 1% revenue loss due to these cyberattacks. Research predicts that fraud losses between 2021 and 2025 will total $206 billion, with bad actors deploying tactics such as phishing, social engineering and fake apps designed to scam company employees.

Thirty-eight percent of companies surveyed said they expected the risk of fraud to increase within the next year, but companies are leveraging new technologies to try to counteract this. ML, data science and shared global intelligence are just some of the techniques being deployed.

ENGLAND AND WALES SAW 5.1 MILLION FRAUD INCIDENTS IN THE YEAR ENDING SEPTEMBER 2021

Fraudsters operate all around the world, with various countries seeing different impacts depending on local circumstances. England and Wales reported 5.1 million fraud instances in the year ending September 2021, according to a recent study, with fraudsters leveraging a wide array of schemes. Advance fee fraud, consumer fraud and retail fraud were the top cybercrime categories, according to the report, with many bad actors exploiting the ongoing pandemic as an opportunity for new scams. Only 26% of these fraud incidents resulted in loss of money with no reimbursement, the study found.

This marks a 27% increase in fraud attempts compared to the same period in 2020. Different types of fraud saw different rates of increase, however, with a 42% growth in financial investment fraud and an 18% increase in advance fee payments fraud.

CITY OF LONDON POLICE REPORTS ACCOUNT TAKEOVERS THE MOST COMMON TYPE OF FRAUD IN 2021

Digital fraud consists of a legion of different tactics, but account takeover was the most common method in 2021, according to a Freedom of Information (FOI) request submitted to the City of London Police (CoLP) in January of this year. Identity fraud, bank card fraud and click fraud domain name scams were the runners-up, but CoLP said the common outcome was that justice and restitution are highly unlikely after the attack has already occurred. Instead, businesses and individuals should shore up their cybersecurity before the attacks take place if they wish to avoid losing funds or data to cybercriminals.

Another report noted that there were 481,096 reports of cybercrime in London between December 2020 and December 2021. This comprises 62% of all fraud complaints CoLP received within that time frame.

PREVENTING DIGITAL FRAUD

UK INSTITUTES NEW FRAUD PREVENTION RULES THAT MAY REQUIRE ADDITIONAL CUSTOMER AUTHENTICATION

In light of troubling fraud trends, the U.K. announced it would be strengthening its know your customer rules several years ago, and new rules officially go into effect this month. These may require more stringent authentication on the part of individual consumers, however, as online retailers and payment service providers will be required to verify customer identities before processing transactions. The rules will apply when a customer makes an electronic payment, accesses a payment account online or does anything that runs the risk of payment fraud.

3D Secure 2.0 is expected to take center stage in this regulation rollout, potentially offering more seamless authentication experiences for card providers that already have implemented these protocols.

NEW YORK STATE UNVEILS NEW CENTRALIZED CYBERSECURITY COORDINATION CENTER

Authorities across the pond are also unveiling new efforts to curb cybercrime. New York governor Kathy Hochul recently announced the creation of the Joint Security Operations Center, which is responsible for handling cybercrime issues across the entire state. The center will be headquartered in Brooklyn and will include experts from municipal and state law enforcement agencies, local and county government officials and NYC3, a body created in 2017 that coordinates cybersecurity for New York City.

Cities across New York state have faced several digital fraud threats in recent years, including a ransomware attack on the state capital of Albany. New York City mayor Eric Adams augmented the creation of the Joint Security Operations Center with a new executive order that mandates the designation of a cybersecurity liaison for each city agency.

DIGITAL FRAUD

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.

DATAVISOR

DataVisor’s mission is to build and restore trust online. It partners with the largest financial and internet properties in the world to protect them from a wide array of attacks, including fraud, abuse and money laundering. The company’s unsupervised ML-based detection solution detects attackers without needing training data, and often before they can do damage.

DataVisor is made up of a team of world-class experts in Big Data infrastructure and ML. It builds advanced algorithms to fight the world’s most sophisticated online attackers.

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