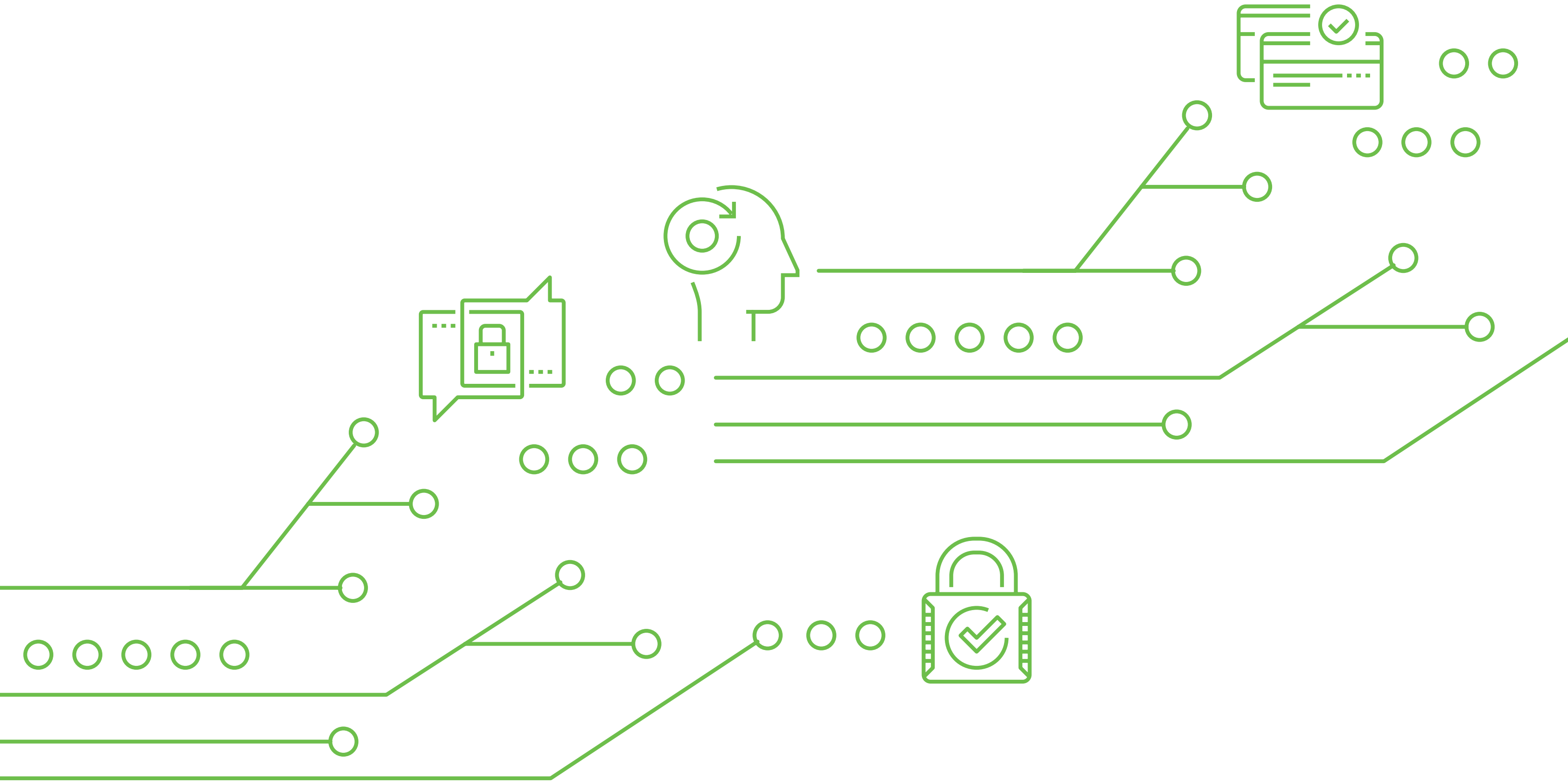
What’s New in 3D Secure 2.0?

PROVIDE A BETTER CUSTOMER EXPERIENCE WHILE REDUCING FRAUD

DATAVISOR

Table of Contents



Introduction

Online credit card payments are subject to authentication protocols. These protocols are continually evolving as new technology becomes available and more is discovered about how to protect consumers, card issuers, and merchants from potential fraud.

The latest protocol release is 3D Secure 2.0, which has been designed to improve upon 3D Secure 1 by addressing old shortcomings, improving e-commerce authentication, and providing a smoother, integrated user experience. Here's a brief overview of 3D Secure 2.0 and what to expect moving forward.

What is 3D Secure 2.0?

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 (e.g. all online transactions, over-the-phone payments, etc.).

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 introduction and implementation of 3D Secure 2.0 come on the coattails of the European Union's Revised Payment Service Directive (PSD2) and Strong Customer Authentication (SCA) requirements. These regulations have been developed with the aim of enhancing customer protection and security with digital payments. According to a Gartner report, 3D Secure 2.0 remains the most likely protocol that issuing banks and online merchants will use to achieve compliance with SCA and PSD2.

What's New in 3D Secure 2.0 (and Why It Matters)?

This protocol 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 e-commerce authentication.

Goodbye, Static Passwords

Typing in a password that never changes was the bane of the customer experience. Customers had to set up accounts with merchants with whom they wished to do business, then had to come up with passwords that met their requirements. Retrieving a forgotten password was a multi-step process, one that often resulted in shopping cart abandonment or slow checkout processes.

With 3D Secure 2.0, static passwords are being traded in favor of dynamic authentication methods such as token-based sessions and biometric data. Authentication is easier and more reliable without the challenges and hassles.

A Mobile-First Approach

3D Secure 1 was not built with mobile in mind because 17 years ago, it didn't have to be. Times have changed, however, with 24% of all transactions being conducted online or on mobile devices (an increase from just 17% in 2019).

The old protocol relied on browser re-directions and formatting that just didn't work for small screens. Now, with 3D Secure 2.0, challenge screens take a mobile-first approach and can be presented from within an app instead of opening a browser window. This creates more of a branded feel and saves some frustration for the end-user.

Greater Authentication Accuracy

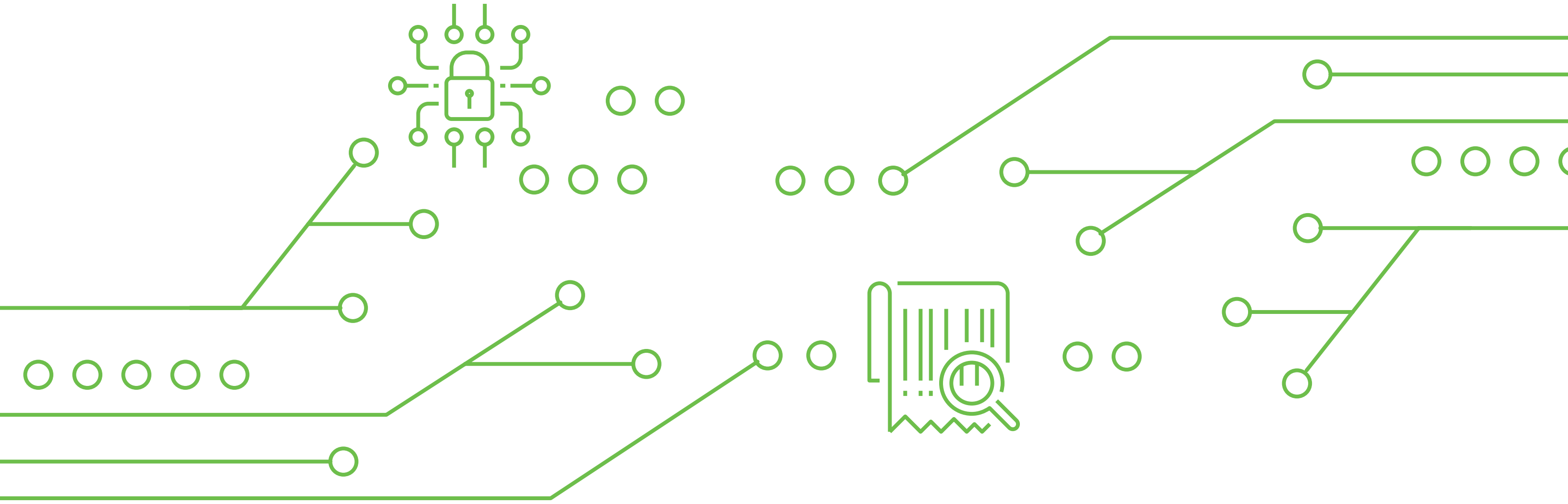
3D Secure 2.0 makes better use of data collection (up to 10x more, in fact) to more accurately determine a transaction's risk. It removes the standard sign-up process and the need for customers to input a static password every time, which can easily be compromised. Greater authentication accuracy helps weed out false positives and allows good transactions to proceed while also reducing fraud losses.

According to a Visa case study, 3D Secure 2.0 may approve as much as 95% of transactions immediately while cardholders will experience 40% less fraud.

Frictionless Customer Experiences

The mobile-first approach of 3D Secure 2.0 highlights the growing consumer preference to use mobile-based channels for transactions. The convenience and the speed that mobile inherently offers should be reflected in all activities, including the purchase of goods and services.

By eliminating stumbling blocks created by static passwords and blocked transactions due to false positives, customers can enjoy a faster checkout process with confidence. In turn, merchants may expect up to 66% less cart abandonment because digital checkouts can be completed without fail.



Explaining 3D Secure 2.0 Flow

Each transaction under the 3D Secure 2.0 protocol shares information between four entities: the cardholder, the 3DS 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. The Cardholder enters their payment details.
2. The Merchant's 3DS Server receives the data, then packages it to send to the Issuer for authentication.
3. The Issuer's 3DS Server assesses the data for fraud risk and may require the Cardholder to verify their identity (e.g. 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. The Merchant authorizes or declines the transaction, based on the decision from the Issuer.

Benefits of 3D Secure 2.0

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 e-commerce experience for all: issuers, merchants, and consumers.

For Issuers

Issuing banks are seeing an increased shift of liability when it comes to fraudulent chargebacks. This liability can be mitigated with the introduction of 3D Secure 2.0. E-commerce 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 interest from the consumer.

For Merchants

More than seven in 10 Americans say that security is their biggest worry when making mobile payments. As a result, merchants may 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.

For Consumers

Consumers can gain more confidence in conducting transactions via mobile device, 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.

The Bottom Line

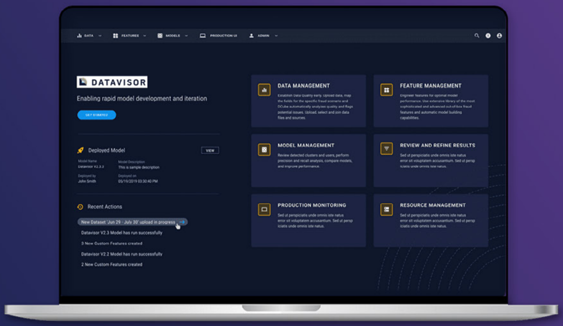
Contextual data is at the heart of 3D Secure 2.0. More data is used to make authentication decisions, which can better reveal a transaction’s potential fraud risk. Eliminating friction for good customers allows issuers, merchants, and consumers to thrive!

Discover how DataVisor’s AI-powered fraud and risk platform enables 3D Secure 2.0 for issuers and merchants to approve more good customers. Experience proactive AI-powered fraud prevention today.

Experience proactive AI-powered fraud prevention today.

GET A DEMO

DATAVISOR



Enabling rapid model development and iteration

Deployed Model

Model Name: Datavisor V2.3.3

Model Description: This is sample description

Deployed by: John Smith

Deployed on: 05/19/2019 03:30:40 PM

Recent Actions

New Dataset 'Jun 29 - July 30' upload in progress

Datavisor V2.3 Model has run successfully

3 New Custom Features created

Datavisor V2.2 Model has run successfully

2 New Custom Features created

DATA MANAGEMENT

Establish Data Quality early. Upload data, map the fields for the specific fraud scenario and DCube automatically analyzes quality and flags potential issues. Upload, select and join data files and sources.

FEATURE MANAGEMENT

Engineer features for optimal model performance. Use extensive library of the most sophisticated and advanced out-of-box fraud features and automatic model building capabilities.

MODEL MANAGEMENT

Review detected clusters and users, perform precision and recall analysis, compare models, and improve performance.

REVIEW AND REFINE RESULTS

Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium. Sed ut persp iciatis unde omnis iste natus.

PRODUCTION MONITORING

Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium. Sed ut persp iciatis unde omnis iste natus.

RESOURCE MANAGEMENT

Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium. Sed ut persp iciatis unde omnis iste natus.

About DataVisor

DataVisor is the world's leading AI-powered Fraud and Risk Platform that delivers the best overall detection coverage in industry. With an open SaaS platform that supports easy consolidation and enrichment of any data, DataVisor's solution scales infinitely, enabling organizations to act on fast-evolving fraud and money laundering activities as they happen in real time. Its patented unsupervised machine learning technology, combined with its advanced device intelligence, powerful decision engine and investigation tools, provides guaranteed performance lift from day one.

For more information on DataVisor:

✉ **info@datavisor.com**

🌐 **www.datavisor.com**

📍 967 N. Shoreline Blvd. | Mountain View | CA 94043

DATAVISOR