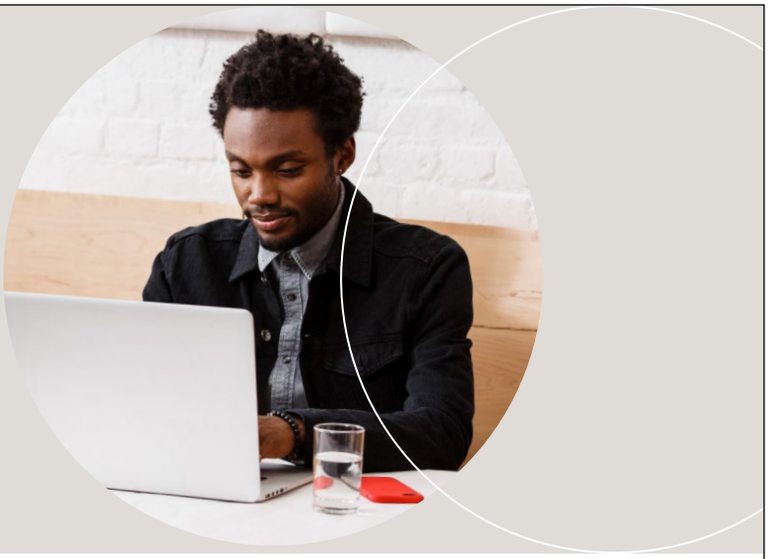
mastercard

EMV® 3-D Secure provides the path to fast, frictionless authentication

MASTERCARD IDENTITY CHECK™



Current landscape

As countries around the globe make the move to EMV chip, organized crime will look for a new path to exploit card fraud, with digital commerce as their preferred channel. Today, card-not-present (CNP) transactions make up 22% of transaction volume, but account for as much as 59% of all fraud, with more transactions migrating to CNP channels every day.* This migration represents a key challenge for merchants and issuers trying to prevent fraud without disrupting their customers' purchasing experience.

For many in the industry, false decline rates—sometimes referred to as "customer insult rates"—are more troubling than fraud losses. False declines occur when a good customer's transaction is mistakenly declined by the issuer's or merchant's fraud models. In the U.S. market alone, false declines for payment card transactions totaled US$303 billion in 2017.* CNP channels are disproportionately impacted by false declines, with average decline rates being up to 6 times higher than card-present transactions.

In 1999 when the industry introduced 3-D Secure (3DS), the objective was to reduce fraud and improve customer authentication during CNP transactions. And while the protocol helped recreate the security of a physical payment and shifted liability for fraud losses away from businesses, it clearly had some gaps, including failing to address the issue of false declines as evidenced above. Other challenges:

- It increased customer friction
- It provided a poor customer experience with an inconsistent user interface
- It was limited to browser-based transactions

But this year with the global launch of the new version of 3DS it is expected to solve all the gaps that the previous protocol had while improving the security of digital commerce.

What is EMV 3-D Secure and what are its benefits?

EMV 3DS is the new industry standard and protocol for merchants to send data to issuers during a CNP transaction to help address false declines and lower CNP fraud while providing a better customer experience. EMV 3DS is relevant for all CNP purchases, including recurring and card-on-file payments. These new EMV 3DS standards improve on many of the shortcomings inherent in the original version. Some of these improvements include:

- Being able to exchange 10x more data than 3DS 1.0 to allow for more informed authentication and authorization decisions
- Performing risk-based authentication or frictionless authentication to allow cardholders to be passively authenticated
- Improving end-to-end transaction processing time by limiting the authentication cycle to one
- Enabling state-of-the-art authentication methods, such as biometrics, for stronger two-factor authentication
- Supporting new payment needs on any device, such as in-app and mobile payments
- Supporting additional use cases, for example, card on file, wallets, and tokenization
- Eliminating the need for consumer registration while shopping

What is Mastercard doing?

Launch of the Mastercard Identity Check

With the rollout of EMV 3-D Secure, Mastercard has created a new solution called Mastercard Identity Check, which replaces Mastercard SecureCode that governed the old protocol. This new solution will enable issuers and merchants to take advantage of the new standards and capabilities to help drive simple and secure payments. Mastercard Identity Check will govern the usage and participation of EMV 3DS to ensure that issuers and merchants are operating within the key performance indicators set in the program for optimal results.

Launch of the Early Adopter Program

In preparation for the launch of EMV 3DS in Q4 2018, Mastercard organized a group of early adopters (issuers and merchants) to be the first to test the protocol. Over the past several months, the group has been testing thousands of live successful and authenticated transactions.

"The use of new security standards, such as EMV 3DS, enable an industry approach for consumer authentication and helps strike the right balance of security and convenience for the end consumer. The data-rich EMV 3DS protocol is poised to be a game-changer for the payments industry. . . . Earlier this year Mastercard launched an early adopter program with key merchants, issuers and technology partners – enabling close industry collaboration during the initial rollout of EMV 3DS. The initial results of this industry collaboration are very strong and will lay the foundation for the long-term success of these programs."

– Dennis Gamiello, Senior Vice President, Global Identity Solutions, Mastercard

In the next few paragraphs we will describe the findings of this test, as well as key takeaways for issuers, merchants, and service providers that are looking to participate in EMV 3DS.

What was tested?

Frictionless flows took priority

The test focused first on frictionless flows – or flows in which the issuer cannot challenge the cardholder and the authentication happens in the background. This flow was a priority because it is estimated that over 90% of authentication requests on the new EMV 3DS standard will be frictionless. Frictionless authentication is based on the issuer's third-party access control server authenticating consumers through a model called risk-based authentication.

Mastercard also used the early adopter test to review the Identity Check Program registration, enrollments, system connectivity, and testing environments and processes.

Preparation for testing

Key to the success of EMV 3DS is the ability for the merchant to send all of the new data variables required in the EMV specification. The new standard passes 10 times as many data elements than the old protocol—over 40 required data elements and 150 total possible data elements. During the testing period the group discovered that most participating merchants needed to make enhancements to their browser JavaScript integrations to pass all the new data required in the EMV specification, including browser device information and/or full address.

Key learnings from testing

Protocol

- Mastercard completed the first live EMV 3DS transactions in late September 2018
- The end-to-end processing of the transaction was 2 to 3 times faster than the average time of the 3DS 1.0 protocol
- Mastercard predicts EMV 3DS frictionless transactions to always be much faster than 3DS 1.0. The reason for this is that the frictionless transactions will only require one authentication cycle, as opposed to the former 3DS 1.0 standard that required two authentication cycles every time authentication was requested.

Issuer and Merchant Service Providers

- Start connectivity testing and server certificate configurations early. Allow time for troubleshooting errors. Endpoint access issues were the number one issue (72%) during early adopter testing.
- Check firewall settings to ensure they are not causing processing and timeout errors
- Validate the secure payment application implementation with Mastercard prior to moving to production

Merchants

- Ensure there is access to data elements like device, payment account number, and address that are necessary for successful processing
- Monitor the data that is being collected for EMV 3DS to ensure that it is following the correct format and is present when the data element is conditional per the EMV specification available on the EMV website:
    - If, for example, country is being included, it must be submitted as country code ISO 3166, e.g., USA, not as United States of America - please correct as necessary.
    - If, for example, shipping information is being sent, then country must be sent, as it is a conditional data element
- Ensure that authentication data used in payment authorization (accountholder authentication value and security level indicator) are being included in the payment authorization message. Partner with your payment gateway(s) or acquirers(s) to ensure that this data is being passed during payment processing.

Next steps to participate in the Mastercard Identity Check Program

All parties

- Once the access control server or 3DS service provider has completed the EMV compliance testing and received their letter of approval, they will then need to register in the Mastercard Service Provider program as required by Mastercard rules
- Review all the onboarding and program guides to ensure all prerequisites and processing requirements are understood

Acquirers

- Ensure the acquirer authorization system is updated to support new Identity Check data elements (transaction ID and protocol ID)
- Register through the Mastercard Identity Check test platform
- Request the Mastercard Identity Solutions Services Management (ISSM) platform to enroll merchants for Mastercard Identity Check

Merchants

- Select and integrate with a 3DS service provider
- Explore Mastercard's 3DS enablement solutions
- Register for Mastercard Identity Check via acquirer
- Review Mastercard Identity Check branding, onboarding, and program requirements

Issuers

- Open a project with your access control server provider and select a Mastercard Identity Check compliant solution
- Register for the Identity Check program on the Mastercard Identity Check test platform
- Enroll access control server and card ranges on the Mastercard Directory Server via the ISSM platform tool available on Mastercard Connect
- Learn about the new Mastercard ISSM platform, which will be used for issuer enrollment in Identity Check
- Work with your access control service provider to take advantage of Mastercard's new Secure Payment Application 2 (SPA 2) algorithm for AAV generation
- Take advantage of Mastercard's Stand-In Risk-Based Authentication services to ensure readiness to support EMV 3DS in Q4 2018
- Check and make sure that your payment processor is able to support Mastercard's real-time digital transaction insights service (Mastercard Announcement 2122)

mastercard

Mastercard resources

Mastercard Identity Check readiness resources

The following readiness resources for Mastercard Identity Check can be found at mastercardconnect.com > Support > Authentication Network > Information Center. You must be a registered user to view the resources.

- *Mastercard Identity Check Onboarding Guide for 3-D Secure Acquirers, Merchants, and Service Providers*
- *Mastercard Identity Check Onboarding Guide for 3-D Secure Service Providers, Operators, Issuers, and Processors*
- *Mastercard Identity Check Program Guide*
- *Mastercard Test Platform User Guide*
- *Mastercard Identity Solutions Services Management User Guide*

EMV 3DS readiness resouces

Mastercard and RSA webinar on preparing for 3DS 2.0 for issuers
https://community.rsa.com/videos/32056

Mastercard and NuData EMV 3DS webinar for merchants
https://register.gotowebinar.com/register/152371813206353153

Mastercard authentication webinar series: "All You Need to Know About PSD2"
https://cc.readytalk.com/cc/playback/Playback.do?id=6e315p

Mastercard authentication webinar series: "How to Participate in EMV 3-D Secure and Increase Your CNP Approvals"
https://cc.readytalk.com/cc/playback/Playback.do?id=3o37j4

EMV specifications
https://www.emvco.com/emv-technologies/3d-secure/

Merchants, to learn more, please visit

https://www.mastercard.us/en-us/merchants/safety-security/identity-check.html

Issuers, to learn more, please visit

https://www.mastercard.us/en-us/issuers/safety-security/identity-check.html

---

Sources

* Federal Reserve. Payments Study: Annual Supplement, 2017.

mastercard