



The latest standards for fast, frictionless payments



What EMV 3-D Secure 2.0 means for businesses



Martijn Van Os,
Senior Vice President

As digital payments evolve to meet changing consumer demands, so does digital fraud technology built to keep these payments secure. Since the introduction of ecommerce, security and standardization have become a large concern for Card-Not-Present (CNP) transactions. This new way to pay went hand-in-hand with the creation of 3-D Secure 1.0 (3DS 1.0) and our own Mastercard SecureCode – a global industry standard designed to give an extra layer of protection when authenticating payments.

However, that protection needs to evolve to meet changing consumer digital payment demands. As our payments advance, our digital fraud technology is growing as well to include richer data and greater security. To that end, we are discontinuing our support of 3DS 1.0 including Mastercard's SecureCode in October 2022.

In 2001, when 3DS 1.0 was introduced, we expected a gradual digital revolution. The Covid pandemic has accelerated this evolution with digital retail sales soaring over 25% between 2020 and 2021. It's difficult to predict where the future will take us, but wherever it does we'll need the next generation of tools.



Today's payment landscape needs a more robust protocol and stronger authentication, supporting a better digital experience while reducing fraud, friction, and false declines. EMV 3DS 2.0 addresses these needs.





The evolution of digital payment security

Typical Card-Present (CP) security measures like signatures and Chip & PIN aren't enough in a digital world. Smart phones, tablets, wearables, and other devices are increasingly used for banking and shopping. Predictably, as CNP activity increases, so does CNP fraud.

This isn't just a big business or banking issue. Small businesses who want to take payments via smart watch or accept instalments online also need to consider CNP fraud. Regionally we are also seeing direct regulations impact digital payment security and a greater need for security. European merchants are required to offer greater security through the Payment Services Directive 2 (PSD2) which came into force January 2018 and provides increased security layers.

This next step to EMV 3DS 2.0 enables the industry to meet PSD2 Secure Customer Authentication (SCA) requirements.



The future of authentication

SCA is perhaps better understood as two-factor authentication. That is, two pieces of separate information are required to confirm identity, from specific categories:



KNOWLEDGE

Something only the cardholder knows (e.g., PIN, password)



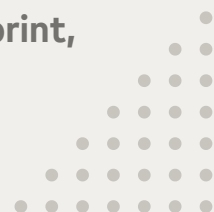
POSSESSION

Something the cardholder has (e.g., phone, hardware token)



INHERENCE

Something unique to who the cardholder is (e.g., fingerprint, face)





In contrast to 3DS 1.0, EMV 3DS 2.0 replaces static passwords with SCA and supports biometrics and one-time passwords, it can be used in-app and over the Internet of Things, and it allows 10-times more data to be exchanged. In short, EMV 3DS 2.0 is a big step-change in digital commerce security similar to the impact Chip & PIN had for CP. It meets today's payment demands and futureproofs online transactions, enhancing security and simplifying payments for the consumer.

Last year alone, this new technology enabled billions of transactions to be authenticated, with a 14% uplift in approvals.



Moving payments, authentication forward

As well as the benefits touched on above, EMV 3DS 2.0 provides enhanced authentication which makes online payments more secure and reduces fraudulent transactions for the benefit of merchants, issuers, and cardholders. It's mobile friendly, with a richer flow of data and much greater flexibility.

This improves the user journey and encourages increased sales with less friction, as well as providing an improved platform for whatever payment technology comes next.

Helping our partners transition

As your partner, we're here to guide you through the transition to EMV 3DS 2.0.

- > Merchants using Mastercard Payment Gateway Services must upgrade to WSAPI version 57 or higher and review the Online Integration guide for EMV 3DS 2.0.
- > Merchants using Mastercard Internet Gateway Services must consult their Virtual Payment Client reference guide.
- > Merchant Services Organizations (MSOs) and resellers, we recommend you enroll your merchants in the card scheme programs for EMV 3DS 2.0 (e.g., Mastercard Identity Check, Visa Secure and American Express Safe Key).

MSOs must also contact your payment processors to ensure they can process the new data fields in their Draft Capture File (DCF), found in the latest GEN4 DCF specification. We'd also advise reaching out to your merchants to make them aware of the changes and what they need to do.

We'll continue to support EMV 3DS 1.0 transactions until October 2022 or when each card scheme has confirmed their sunset date. If you have any questions or concerns about the transition, please get in touch with your account representative

