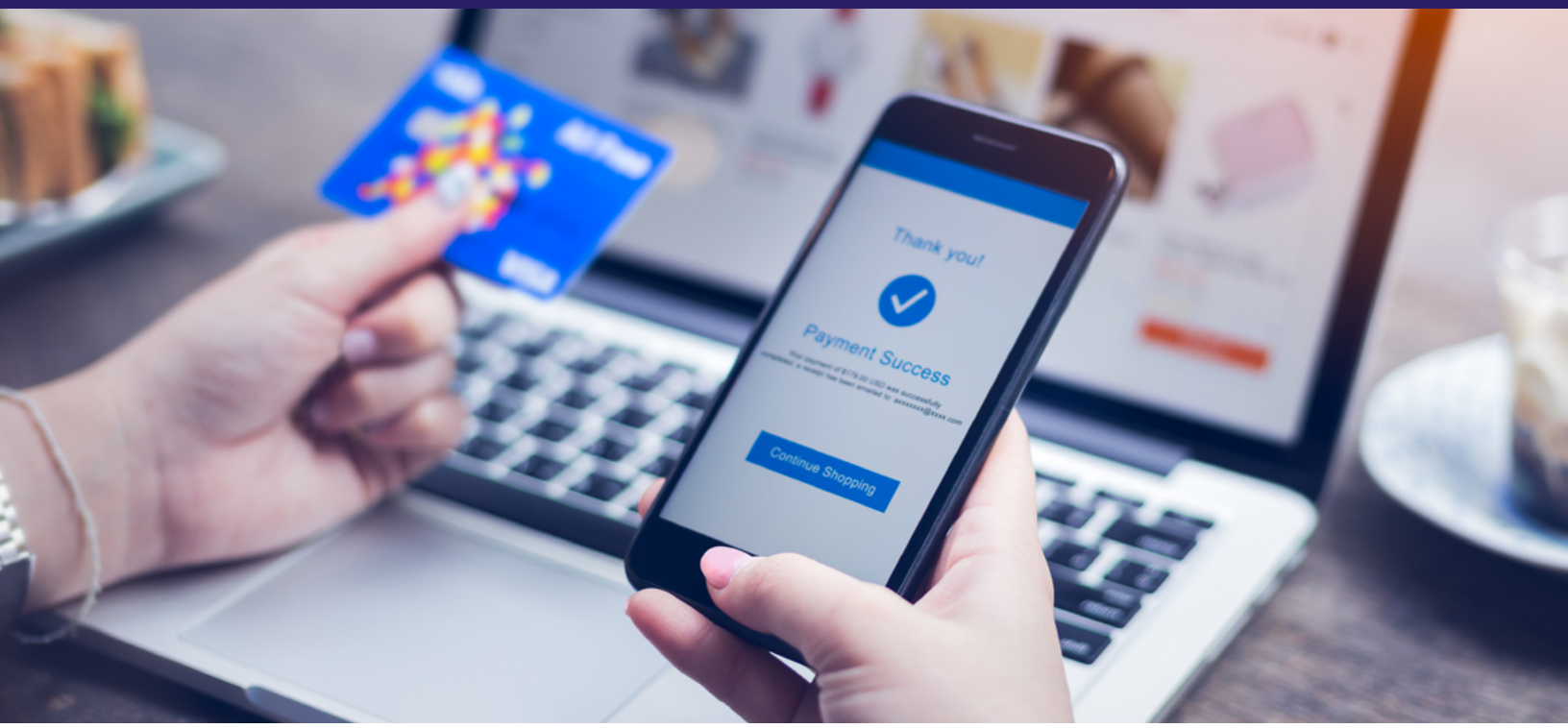
MARQETA



All about 3D Secure and Strong Customer Authentication

Organizations that issue cards face a tradeoff when it comes to fraud. How can they reduce fraudulent transactions and meet regulatory standards while still making sure their cardholders can purchase online with ease? Any increase in friction caused by additional authentication steps can lead to customer frustration and dropoff at the time of payment.

The good news is that cardholders are willing to participate in the process to reduce fraud. They aren't solely relying on their card issuer or the brands where they shop to isolate them from all risk. In a Marqeta survey of 4,000 U.S. and U.K. consumers, 87% of respondents said that they would be "happy for transactions to take longer to complete, if extra steps for authentication meant their information was better protected."

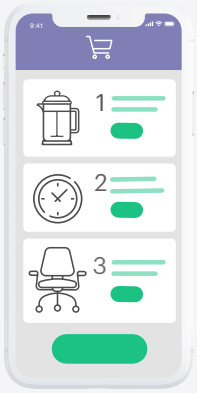
Having a strong 3D Secure authentication strategy can help card program providers combat fraud while still providing innovative payment experiences to their cardholders.

3D Secure: a quick primer

What is 3D Secure?

The Three-Domain Secure (3D Secure or 3DS) is a security protocol created by EMVCo (a body made up of the major card networks) that protects online payments by enabling cardholders to authenticate themselves with additional verification prior to authorization of the payment. To cardholders, it is commonly known as Visa Secure or Mastercard SecureCode for Visa and Mastercard cards, respectively. 3D Secure applies to transactions where the card is not present (CNP) such as online and mobile ecommerce.

The 3D name comes from the three domains involved in providing this added security:



The acquirer domain
(e.g., the merchant)

The interoperability domain
(e.g., the card network)

The issuer domain
(e.g., card issuer, card program provider, or Marqeta)

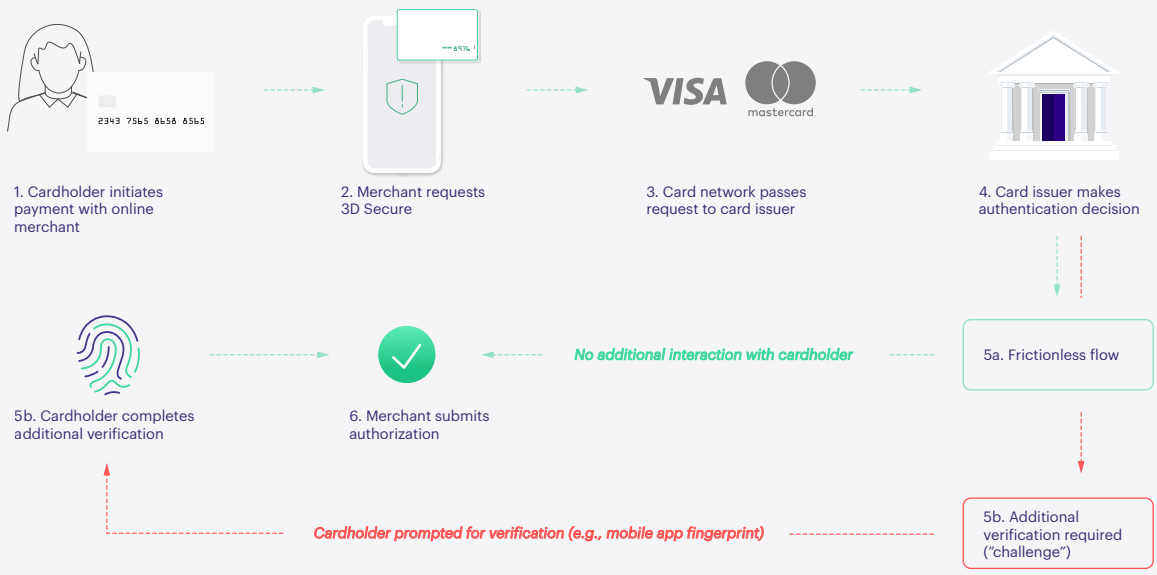
When does 3D Secure occur?

3D Secure authentication of the cardholder occurs prior to authorization of a transaction.

Let's walk through a real example:

A customer is shopping online and enters their credit card information at checkout. The online merchant (with its acquirer/payment service provider) can enable 3D Secure, and sends the request through the card network to the card issuer. If the card issuer wants additional security they can "challenge" the cardholder for additional verification (e.g., a one-time password or biometric authentication). Or, if the issuer feels that the transaction is low-risk, it can passively authenticate the transaction without requiring further interaction by the cardholder. This is known as "frictionless flow". In both cases, the issuer sends back the authentication result to the merchant so they can move forward with the payment authorization request.

3D Secure authentication flow



What is a liability shift and how will it impact my card program?

To encourage merchant adoption of 3D Secure, the card networks introduced a liability shift similar to how liability currently works with card-present transactions that utilize an EMV chip. If an online payment is successfully authenticated with 3D Secure (either with a challenge or when the issuer allows frictionless flow), the card network shifts liability for subsequent fraud-related chargebacks to the issuer. Below is a table that outlines various scenarios and the liability shift outcomes which could impact your business. Note that the dates for enforcement will vary by card network, region and version of 3D Secure.

Merchant	Card issuer	Authentication result	Liability shift to the card issuer
Requests 3D Secure	Challenges cardholder	Verified	Yes
Requests 3D Secure	Allows frictionless flow	Verified	Depends on card network/region
Requests 3D Secure	Challenges cardholder or allows frictionless flow	Failed or not verified (e.g., technical issue, cardholder doesn't complete authentication)	No
Requests 3D Secure	Card issuer does not support 3DS	N/A	Yes
No 3D Secure request	N/A	N/A	No

What improvements were made with EMV 3DS (3D Secure 2)?

When it was first introduced, 3D Secure 1 caused conversion issues for merchants and issuers. It required almost all transactions to be challenged and often used static passwords that were hard for cardholders to remember. 3D Secure 1 also didn't work properly on all devices causing an increase in customer frustration and a large drop in successfully completed checkouts. 3D Secure has since undergone many enhancements to its protocol.

The latest version, 3D Secure 2, also known as EMV 3DS or 3DS2, improves on 3D Secure 1 by:

- Using enriched data sharing (e.g., shipping address, transaction history) between the merchant and issuer to authenticate without having to challenge the cardholder for low-risk transactions (frictionless flow)
- Enabling authentication on any device (desktop, mobile, Internet of Things (IoT)) for better cardholder experiences
- Applying Strong Customer Authentication (SCA) exemptions, using specific indicators in the authentication messages

Given that merchant adoption of the 3DS protocol can vary by region, Marqeta supports multiple versions including 3D Secure 2 for Visa and Mastercard, and 3D secure 1 for Visa.

What authentication methods are available?

Organizations that issue cards have multiple options to authenticate their cardholders, but it's important to consider the steps your cardholders will have to complete in order to verify themselves. Some advanced methods that have improved the authentication experience include biometric and voice recognition.

Marqeta can provide default one-time password (OTP) authentication if cardholder information is on file, and can also enable advanced authentication methods such as using your own mobile banking app.

3D Secure and Strong Customer Authentication in Europe

What is PSD2 and SCA?

The Payments Service Directive 2 (PSD2) is a European law passed with the goal of creating an integrated payments market, making payments more secure and protecting consumers. Strong Customer Authentication (SCA) is a component of PSD2 and requires payment service providers in Europe to implement two-factor authentication (2FA) for certain online transactions. To help meet the requirements of SCA, issuers and merchants can enable 3D Secure to authenticate cardholders.

SCA requires authentication using two of the following factors:

Something the cardholder knows

e.g., a password or PIN

Something the cardholder has

e.g., a token or mobile phone

Something the cardholder is

e.g., a fingerprint or voice match

What are exemptions under PSD2 and SCA?

While 2FA can help reduce fraud, not all transactions require it. Adding additional steps to the checkout process, can sometimes lead to unintended drop-off. To allow merchants and issuers to bypass extra verification under SCA, they can utilize exemptions. An exemption allows a transaction to take place under SCA without requiring two-factor authentication.

These exemptions may be available in cases such as low-value transactions, low-risk transactions, recurring transactions, or those with trusted merchant beneficiaries. In these cases, the merchant (through its acquirer) is responsible for any fraud-related chargebacks.

However, it's ultimately up to the issuer to decide if an exemption is accepted. A merchant could request an exemption, but the issuer, if it deems the transaction too risky, can still require additional verification by the cardholder. In this case the liability would be shifted to the issuer.

Merchant	Card issuer	Authentication result	Liability shift to the card issuer
Requests SCA exemption	Allows exemption	Verified	No
Requests SCA exemption	Challenges the cardholder	Verified	Yes

In order to leverage certain exemptions with frictionless flow, issuers and merchants (through their acquirer) must meet certain thresholds for fraud rates and report their status to regulatory bodies.

What if a cardholder uses a card through a digital wallet or local payment method?

Many digital wallets such as Apple Pay, Google Pay, and European payment methods such as IDEAL support 3D Secure-like authentication experiences, because they already use a combination of authentication factors in their checkout experience, including biometrics or passwords. These payment methods may not require additional verification steps by the cardholder under SCA.

The full SCA requirements and exemption rules can be found here.

What's happening outside of Europe

How are businesses in non-European countries impacted?

Although regulatory bodies in countries like the U.S. don't currently mandate SCA, authentication can still be an important component of an issuer's overall fraud strategy, as it can provide an added layer of security.

Additionally, global issuers need to be prepared as more merchants begin to adopt the latest 3D Secure protocol outside of Europe. Liability shift is already activated for 3DS1 and it's expected that the card networks will begin to activate the liability shift for 3DS2 on a region by region basis. In the U.S. for example, Visa will be activating a liability shift for merchants who request 3DS2 starting August 2020. Therefore, if an issuer has not enabled 3DS and a merchant requests authentication, liability will shift automatically from the merchant to the issuer.

How to prepare for 3D Secure

What do I need to do as a card program provider?

Given evolving regulations and timelines, Marqeta suggests that organizations prepare for SCA in Europe and for card network liability shift mandates as soon as possible.

To support 3D Secure, issuers and card program providers must integrate with a certified Access Control Server (ACS). The ACS will receive 3DS Secure authentication requests from the merchant through the card network, and will enable challenges to the cardholder using the issuer's chosen authentication method. Once the cardholder is authenticated, the ACS will send a response back to the merchant with the authentication results.

Marqeta built and certified its Access Control Server in-house making it easy for businesses to enable 3DS via open APIs without having to integrate with a third-party.

What should I consider when choosing a 3D Secure provider?

While 3D Secure is an industry protocol, how an organization integrates 3D Secure into their processing strategy is not a one-size-fits-all approach.

When looking for a 3D Secure provider, card program providers should consider the following factors:

1. How much customization and control will I have over the authentication experience?
   The majority of transactions will be genuinely made by legitimate cardholders. Adding friction in these cases will be unnecessary. Make sure your provider gives you the control to decide when to apply a challenge, using your preferred methods of engagement with cardholders.

2. How integrated is 3D Secure with other processing services?
   Due to heavy network certification requirements, issuer processors often outsource or acquire 3D Secure technology. Separate agreements and complex integrations between the issuer processor and the 3D Secure provider's technology can slow down your time to market and put you at risk of sharing sensitive cardholder data between parties.

   Issuer processors that have built their own in-house ACS can help you create a 3D Secure strategy that is customized to your risk profile and keeps sensitive data protected. You may even benefit from having authentication data directly linked to your authorization messages to make more informed authorization decisions knowing the cardholder has been authenticated.

3. How quickly can the provider adapt to the changing protocol and regulations?
   3D Secure is a constantly evolving protocol and regulations in Europe are expanding to other markets. Look for a provider that can adapt quickly to these changing dynamics and has a good view on what is coming next to help you prepare for updates.

How can Marqeta help?

Marqeta offers a 3D Secure solution with multiple integration options that can help card program providers reduce fraud while customizing the authentication experience delivered to their users. We can delegate decisioning to you leveraging authentication methods you prefer for complete control, or you can build your decisioning policy using the Marqeta platform while providing all necessary data to satisfy reporting requirements.