cardinal
A Visa Solution

10 Myths about EMV® 3-D Secure and PSD2's Strong Customer Authentication Requirement

There is a lot of confusion and misinformation circulating in the payments and fraud landscapes today. It's hard to know who you should listen to.

Here are 10 statements we've heard, followed by the real story you need to know.

Myth: Merchants should avoid 3-D Secure at all costs, even when they need to comply with PSD2 SCA

Fact: Merchants can't avoid using some form of authentication in countries where PSD2 SCA is required.

Some transactions may qualify for exemptions, but **it is the issuers' choice whether to accept them or not**. Merchants have little control over which transactions can bypass 3-D Secure with exemptions, so they need to be prepared with a solution that can provide a smooth consumer experience.

In fact, we recommend that merchants **send as many of their transactions** through 3-D Secure as they can, to not only give their shoppers a consistent, safe experience, but to take advantage of all of 3DS' benefits.

Myth: 3-D Secure is a conversion killer and will negatively impact authorization rates

Fact: In the EU market, 3DS has already been widely adopted by acquirers, issuers and merchants since the rollout of EMV chip cards for point-of-sale. With strong participation, 3DS is a conversion optimizer, which **can yield up to a 95% approval rate**, vs non-authenticated approvals at 90% average[1].

Issuers have adopted risk-based authentication methods which will help them apply issuer Transaction Risk Analysis (TRA) if their fraud rates are within the allotted threshold, based on transaction amount. When the TRA exemption is applied successfully, authentication happens in the background, with no consumer checkout friction.

Because SCA is being mandated, there will be a level playing field where all merchants and issuers need to participate. And even when challenges happen, the challenge methods are smoother and less invasive than they were in the past, with biometrics.

Myth: A fraud tool is all you need to satisfy the SCA requirement

Fact: SCA requires two out of these three factors: **something you know**, **something you have**, or **something you are**. A fraud tool cannot satisfy these requirements, unless it also performs authentication. EMV® 3-D Secure can satisfy these requirements. EMV 3DS is a mainstream, pragmatic solution that meets the SCA requirement. It is widely available in Europe and is not difficult to implement. A fraud tool is a great idea to layer, along with 3DS, but you really need a solution that provides two-factor authentication. Most importantly, all card networks stand behind 3DS and it satisfies the SCA requirement.

Myth: Merchants should try to use exemptions whenever possible

Fact: Maybe. But remember that whoever requests the exemption also takes on liability for any fraud. **Not all transactions will qualify for exemptions and not all merchants may be able to use exemptions**.

In the case of the low value exemption, it only applies if it is not the fifth transaction below 30 euros and the cumulative total of the low value transactions doesn't exceed 100 euros (since the last time SCA was delivered to the consumer by their issuer), so there is no guarantee that there won't be SCA on every low value transaction.

And especially as exemptions roll out, there will be a lot of effort required to take advantage of them, by issuers, acquirers and merchants. Some of the card networks' exemption programs have criteria that merchants need to meet, and we would recommend a conversation with your acquirer to see if you -- and they -- qualify.

Myth: A 3DS challenge is a bad thing

Fact: This really is a myth. In fact, challenges can save transactions that otherwise would be declined. And when a transaction is subject to PSD2 SCA, sometimes a challenge is unavoidable. 3DS challenges today are much less invasive than they were in the past. **You can also think of a challenge as a life raft**. The issuer has a choice with a risky transaction: they can challenge it or they can decline it. By sending a challenge, the issuer is trying to save the transaction, and lets the consumer prove that they are who they say they are. If the transaction doesn't authenticate successfully, there's a good chance that the transaction was, in fact, fraudulent.

Issuers also have adapted to using Risk-Based Authentication, which applies 3DS data elements and other important data points to model and analyze the risk of the transaction, along with risk scoring and rule criteria. They have the same goal that merchants do, and that's to approve valid orders, with the shopper experience in mind – and keeping their card top of the wallet.

Myth: Delegated authentication is a good solution for SCA for all merchants

Fact: It allows for a merchant who has sophisticated means to **authenticate a consumer through their own website**, app or similar offering, so a lot of merchants will not be able to take advantage of delegated authentication. Merchants can authenticate in several different ways.

An example of a merchant supporting authentication is when a consumer views or changes sensitive account information after logging in to the merchant's website. A consumer may be asked to use their fingerprint if biometrics are enabled on their device. Not all merchants may have this level of sophistication or have an SCA compliant solution.

This could qualify a merchant for delegated authentication. This would identify the merchant as the authenticator and if the consumer was presented with authentication within the guidelines of the Regulatory Technical Standards (RTS), then the issuer can accept the DA, and not have to provide additional SCA to the consumer on the transaction.

Myth: If all your transactions are below 30 euros, you don't need to do authentication for SCA

Fact: Even if all your transactions are under 30 euros, you aren't going to be exempt from doing authentication for SCA. **There are two use cases for the low value transaction exemption** that you need to comply with, by authenticating transactions.

The first one is that every fifth transaction (per PAN, across all merchants) below 30 euros needs to be authenticated for SCA. The issuer keeps track of the PAN's activity, so the merchant will not know which transaction will need to be authenticated, but they need to be prepared, or risk the transaction being declined. As an example, if a consumer uses the PAN for a coffee, a ride-share, another coffee, a small grocery order (under 30 euros), and a lunch order, the lunch order would trigger authentication, as the fifth transaction under 30 euros.

The second use case is that for those five transactions below 30 euros (since authentication was last performed), the cumulative total may not exceed 100 euros without performing SCA. Again, the issuer keeps track of the transaction amounts and triggers authentication when a low-value transaction makes the cumulative total hit 100 euros. Like the example above, from the last time the PAN was authenticated, if a consumer uses the PAN for an online coffee order under 30 euros, two online lunch orders at just under 30 euros each, and then an online grocery order for just under 30 euros, which makes a total of more than 100 euros, authentication would be triggered.

Myth: Merchants need to implement EMV 3DS version 2.2 to satisfy the SCA requirement

Fact: EMV 3DS version 2.2 is your best option, though technically, all versions of 3DS can fulfill the SCA requirement (though all of them may not be consumer or merchant friendly). **Version 2.2 supports enhanced functionality to manage SCA exemptions**, and in particular, the trusted beneficiary exemption that allows consumers to add their preferred merchants to the trusted beneficiary list their card issuer maintains.

Version 2.2 also enables authentication for travel agent transactions (which can include airlines, hotels, car rentals, and other charges), split shipment authentication, out of band authentication, and 3RI cryptogram/decoupled authentication applications. EMV 3DS version 2.1 provides enhanced SCA functionality, sharing more data with issuers to enable better risk decisions; this version (as well as version 2.2) works on all devices. Mastercard has also supports 2.1 + extensions which support exemptions (TRA, Recurring, MIT, Secure Corp Payment and Whitelisting). Please refer to each network's program rules to review what's available now on their network, as this varies.

Myth: Issuers don't need to be on the latest version of 3DS

Fact: Issuers do have deadlines to implement EMV 3DS versions 2.1 and 2.2, so **they can be ready for when the SCA requirement is enforced**. The card networks (Visa and Mastercard) have announced dates for when issuers will need to support EMV 3DS version 2.1 and version 2.2, as follows:

- Mastercard has required issuers, acquirers and merchants in the EU to support EMV 3DS and their Identity Check program globally since December 1, 2019.
- As of March 14, 2020, Visa required all EU issuers to deploy and support EMV 3DS version 2.1.
- On September 14, 2020, Visa will require that all issuers in Europe support EMV 3DS version 2.2.
- On October 16, 2020, Visa will require that all acquirers support EMV 3DS 2.2.

Myth: Merchants need to send transactions using specific versions of 3-D Secure, based on what the issuer is using

Fact: **A qualified 3DS provider will support all versions of 3DS and EMV 3DS and will be able to route transactions on the appropriate 3DS rails**, depending on the issuer BIN. (The provider will know which version the issuer is using, based on the BIN, in order to route transactions for the most benefit). Merchants don't need to figure out what version of 3DS each issuer uses or try to guess. When merchants implement 3DS, their service provider should be able to manage that. Merchants will only need to integrate once and going forward, their provider should be able to manage all protocols. Talk to your 3DS provider about this, or make sure to ask potential providers before you hire them.

There are a lot of mixed messages and confusion in the marketplace today. Make sure you do your research and talk to the card networks and trusted providers.

Choose experience, choose Cardinal.

Let's talk.

cardinal
A Visa Solution

[1] Source: Visa Merchant Bulletin, 3rd edition, 10 March 2020
[2] Authentication Guide for EU, MC v1.3 – March 2020