Planning for PSD2:
A Solution Buyer's Guide

A guide for
eCommerce merchants

Table of contents

What's in this guide?

As an eCommerce merchant, you have probably already done at least some preliminary investigation into how to best respond to the potential impact of PSD2's new security measures. This is not an easy task given the uncertainties surrounding the regulation. Although the delay in enforcement across most of Europe has meant more time to get ready, it has also further complicated the definition of sufficient preparedness.

The October 2019 EBA Opinion, indicating that the deadline for migration to Strong Customer Authentication (SCA) is 31 December 2020, should increase the likelihood of an aligned approach to SCA by banks across the region. But many online retailers are still working to develop comprehensive plans to protect their customers' experience and revenue from 2020 onwards.

To shed light on what's important to European consumers and to reveal how merchants plan to deal with PSD2, Riskified surveyed 2000 consumers and 200 online retailers across the UK, Germany, France, and Spain. The survey results reveal how online shoppers are likely to react to the increased security measures and potential friction, and that retailers' intended actions might not be sufficient.

In this guide, we share key findings from the survey - providing context to merchants who are assessing how to best prepare for PSD2's enforcement. We then describe the main approaches to protecting revenue under the regulation, followed by a list of considerations retailers should take into account (and questions to ask) when contemplating partnering with a third party to mitigate the risks associated with PSD2.

Planning for Enforcement: The Impact of SCA

SCA and friction

The anxiety among European retailers surrounding PSD2 is mostly related to the threat of increased cart abandonment resulting from mandated SCA.
Our survey reveals that over 40% of European retailers expect cart abandonment rates to grow by 21-60% in the first 12-24 months of PSD2's implementation.

Under the new regulation, customers will be required to provide two of the following in order to complete an online purchase:

- Something they know (e.g. password or PIN)
- Something they have (e.g. their mobile phone)
- Something they are (e.g. fingerprint or voice recognition)

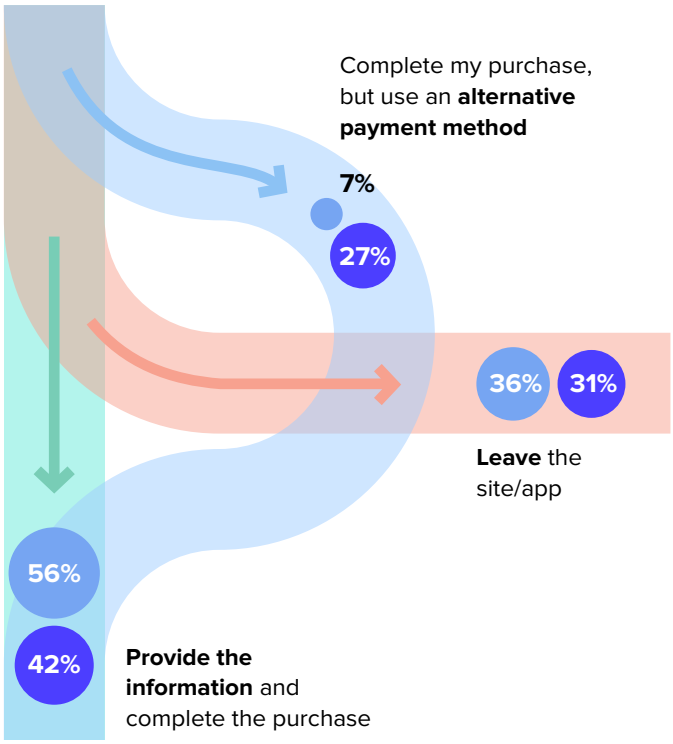
In this regard, retailers and consumers are aligned. Consumers were asked whether they would leave a site or app when requested to verify their identity (for example via passcode/ PIN, text message, on-screen knowledge-based challenge questions, or device evidenced through QR code).

Based on consumers' responses, retailers across the UK, France, Spain and Germany stand to lose about one third of orders due to these extra verification measures. Interestingly, 56% of French shoppers expressed willingness to provide additional information. This may be explained by the fact that consumers from France are also less likely to use alternative payment methods.

European Consumer Survey

IF YOU WERE ASKED TO VERIFY YOUR IDENTITY* WHEN SHOPPING ONLINE, WHAT ACTION WOULD YOU TAKE?

*e.g. via PIN number, SMS, knowledge-based questions, ID card or device evidenced through QR code



Using exemptions to mitigate friction

In acknowledgment of the friction expected to accompany SCA, European regulators devised nine exemptions (some of which are listed below) that can be used to prevent online orders from being subjected to this type of authentication.

Low risk	Low risk transactions **between the value of €30 and €500** can go through frictionless Transaction Risk Analysis (TRA) instead of SCA. The regulation requires that **acquirers meet certain fraud thresholds** (explained below) in order to obtain this exemption.
Low value	Orders **under €30** are exempt from SCA. However, SCA will be used on every 6th transaction on a card and/or if consecutive purchases surpass €100 and none have been challenged.
Whitelisted merchants	Cardholders can request that their issuer **whitelist specific merchants** so that future transactions with this card (at these merchants) will be SCA exempt.
Recurring payments	Except for the initial transaction, where recurring payments of the **same amount** are set-up by a customer with the **same merchant**, SCA won't be required.
Corporate payments	Issuers can initiate exemptions on corporate payments made by businesses. This doesn't apply to corporate credit programs.

Particularly beneficial, given its wide scope, is the low risk exemption. According to our survey, around half of European shoppers spend between €30 - €120 per online purchase. The low value exemption, on the contrary, has been met with wariness by some merchants. While some view the exemption favorably, others are concerned that fraudsters will exploit it by using stolen credentials to make low amount purchases.

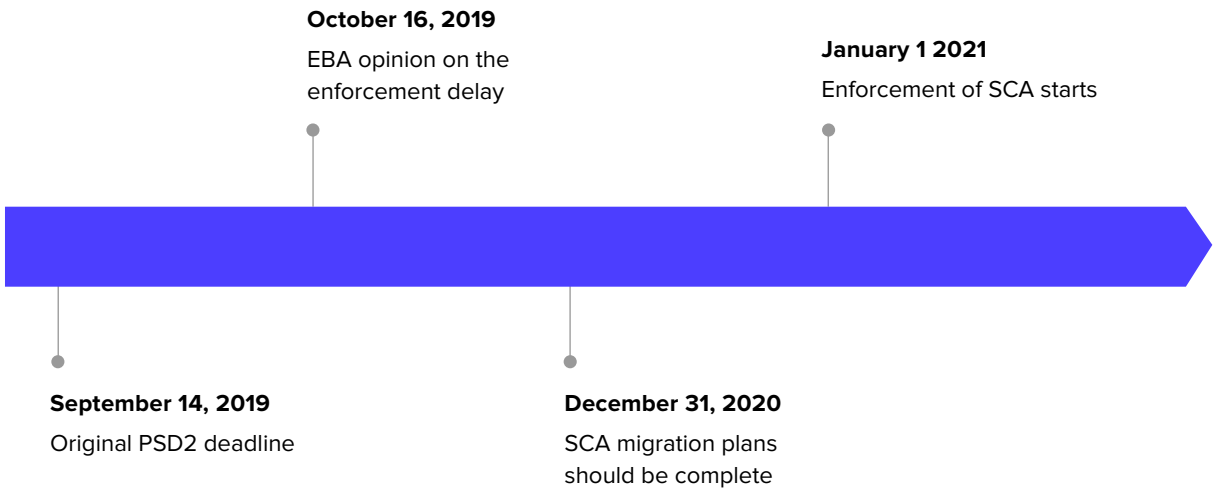
Will issuers grant exemptions?

Some retailers and payment providers have their doubts about whether issuers will be willing to grant exemptions. Let's consider the priorities and interests of issuing banks under PSD2. Once PSD2 is enforced, issuers will become liable for fraud on transactions that undergo SCA. At the same time, SCA adds friction to the shopping experience, that will cause many European consumers to abandon their cart and possibly select a different payment method.

By granting exemptions, issuers stand to benefit not only from the fact that fraud liability will shift away from them; reducing friction for cardholders will also help keep the issuer's payment method 'top of wallet'. It's worth noting that acquirers, who want to capture as many transactions as possible, also stand to gain from pushing for exemptions.

When will exemptions be applied?

There's a chance that exemptions will only start being applied consistently in late 2020 or even early 2021. So what should merchants operating in the European eCommerce market be doing between now and January 2021 to ensure customer friction is kept to a minimum?

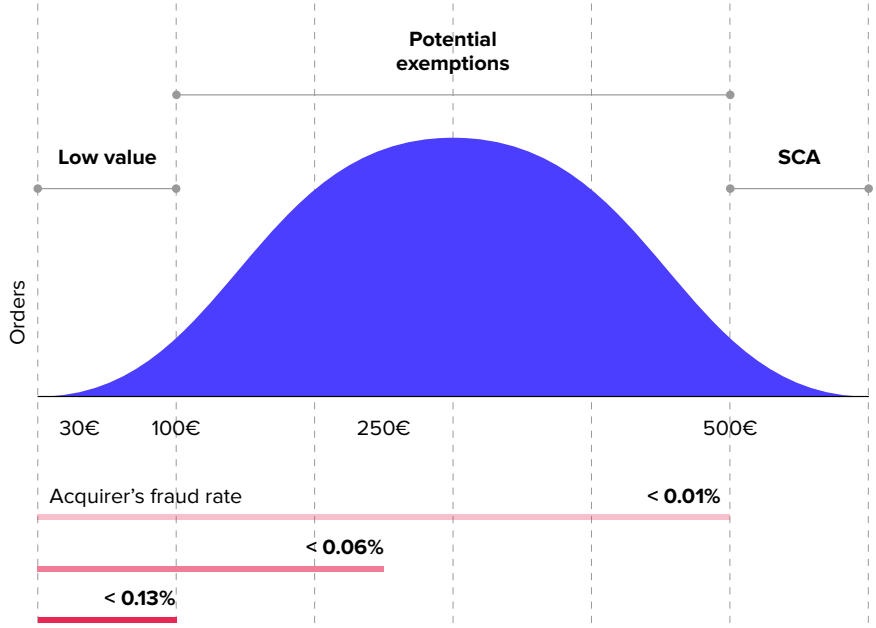


A PSD2 transition strategy

Keep fraud low

Acquirers will need to meet the fraud thresholds set by the regulator, in order for the issuer to consider granting a 'low risk' exemption.

ACQUIRER FRAUD THRESHOLDS



Acquirers will want to make use of the low risk exemption to keep friction to a minimum and capture more revenue. And because acquirer fraud rates are aggregated across all merchants, their preference will be to work with merchants who have low fraud rates. In order to benefit from their acquirers pushing for maximum exemptions once PSD2 is being enforced consistently, merchants will therefore want to keep their fraud rates as low as possible. This leads us to a big unknown - when will issuers start declining orders that haven't gone through 3DS?

Be prepared for SCA

It is anticipated that most European countries will follow the new timeline as per the October EBA Opinion (i.e. they will hold off enforcing PSD2 until January 2021). While there is no clear incentive to do so, there is a possibility some banks will start applying SCA ahead of this time.

Because of the added friction, it is best not to send orders to SCA if you don't have to. However, if you fail to submit 3DS data to an issuer that has started applying SCA, this will likely result in a higher rate of payment declines. Tracking payment authorization rates across issuing banks can help reveal when a specific issuer has started applying SCA, allowing you to react appropriately to avoid negatively impacting shoppers' customer experience (and your revenue).

Of course, you will need to make sure that you can immediately enable 3DS once issuers are applying SCA. Most European merchants have already integrated the original version of 3D Secure (3DS 1), which is currently supported by all banks. However, it does not allow for exemptions, doesn't offer a wide range of authentication methods, and in many markets is associated with high levels of customer drop-off.

Over 80% of European retailers who responded to our survey intend on integrating 3DS 2 by the end of 2020. This version of 3DS is optimized for mobile, allows for exemptions and offers a wider range of authentication methods. The newest version of 3DS is 2.2, which facilities SCA exemptions to the fullest capacity. While 3DS 2.2 also offers inherence, it's unclear when banks will start to broadly accept biometrics and behavioral data as a form of authentication.

3DS Versions

3DS 1

- Partially supports the use of SCA under PSD2
- Does not allow for exemptions (you can still ask for exemptions, but via the authorisation request)
- Does not offer all types of verification
- Often associated with high levels of customer drop-off

3DS 2

- Allows for exemptions
- Supports a variety of SCA methods
- More vigorous risk-based authentication
- Data sharing between banks/merchants
- Embedded within checkout
- Optimized for mobile, app-based authentication, digital wallets

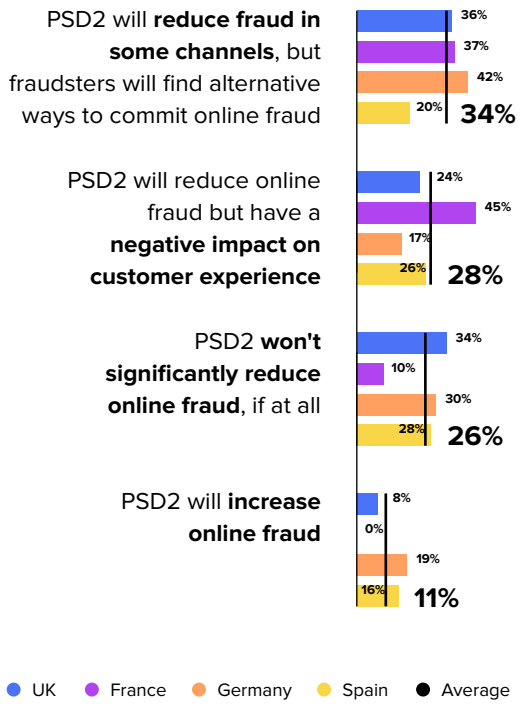
3DS 2.2

- Extended version of 3DS 2 that facilitates exemptions to their full capacity and the transmission of data that correlates with 'what you are'
- Currently not accepted by all banks, and doesn't actually offer biometrics yet

Fraud Management Under PSD2

European Retailer Survey

WHICH OF THE FOLLOWING STATEMENTS DO YOU AGREE WITH?



Once PSD2 is in force across the EU, it will likely prevent CNP fraud to some extent in intra-European transactions. But SCA is certainly not 'fraud proof' and fraudsters are already busy finding ways around the new safeguards.

Our survey revealed that almost 40% of European merchants are pessimistic about PSD2's ability to curb fraud. A quarter of these retailers even expect fraud rates to increase. The remaining 60% of merchants anticipate the new measures will reduce fraud, but are aware of its drawbacks.

Out of scope orders

Unless your business is based in the EU and you intend to sell only to domestic credit card holders, a portion of your eCommerce transactions will not be covered by PSD2.

You will still be liable for fraud in the case of 'one-legged' transactions, phone orders, merchant-initiated transactions, and all other purchases that don't fall within PSD2's scope.

Fraudsters trying to avoid SCA are likely to obtain details of cards issued outside Europe, as this will ensure the purchase is out of PSD2's scope. We expect to see fraudsters use non-EU payment methods to carry out account takeover (ATO) attacks as well.

While most merchants have been focused on basic compliance and the more technical aspects of preparing for PSD2, it's important to consider the processes required to effectively handle out of scope orders.

The rise of account takeover attacks

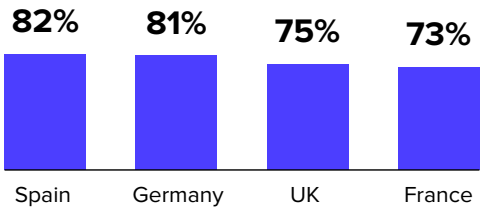
Fraudsters have proven themselves to be resourceful and adaptive. With PSD2 presumably making their lives harder, they will try to exploit whatever they perceive to be the weakest link. One such weak point is at the account login stage of the online shopping journey. When credentials are stolen by a bad actor, they can log in to a good customer's account and have a much higher chance of successfully committing fraud (because the merchant generally assumes they're a legitimate returning customer). This is an ATO attack.

So why do we predict ATO attacks will increase under PSD2?

Firstly, a lot of damage can be done before SCA even enters the flow at checkout – for instance, simply by gaining access to the account, and before making a purchase, fraudsters can steal the customer's PII (personally identifiable information). Customers' ability to whitelist merchants presents another opportunity for fraudsters. Card details will likely be sold on the dark web advertising "whitelisted for merchant X". Fraudsters will find it easier to successfully make purchases via the compromised account if there's a whitelisted card saved on it - the order will be exempt from authentication even if the fraudster changes the shipping address or email. This is probably one of the reasons that the whitelisting exemption is not popular with issuers.

It's also important to remember that one of PSD2's aims is to regulate innovation in payments. A large part of this is encouraging open banking, which means non-traditional methods of payment are set to become far more common, and many of these are vulnerable to ATO attacks. More players will have the freedom and flexibility to provide payments - including merchants. But even companies with experience offering account-based payments, who have a robust security infrastructure, experience ATOs. So if you intend on becoming a payment provider for your accounts or plan to offer your own in-store wallet, you need to keep this threat in mind.

European consumers who stated they were either very or fairly open to using forms of payment other than a credit/debit card (e.g. Google Pay, Apple Pay, etc.) for online purchases:



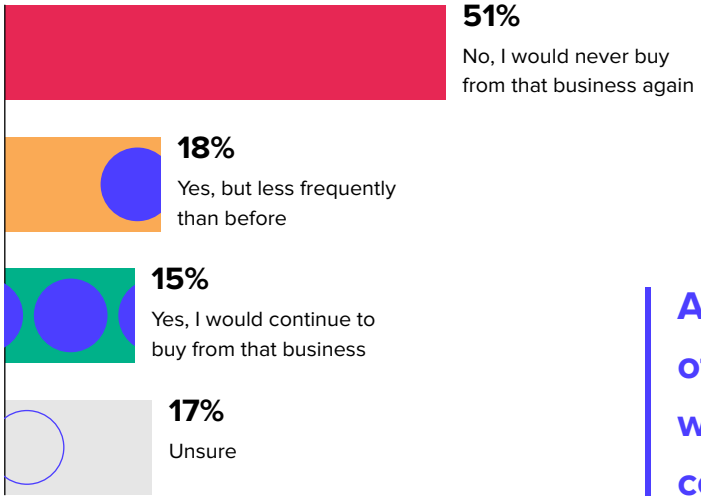
The ramifications of fraud

We all know that friction leads to cart-abandonment and that fraud can dramatically impact sales. In fact, over a quarter of consumers we surveyed chose security as their most important consideration when selecting where to make a purchase online.

Online businesses need to be concerned about fraud, not only because of surpassing fraud thresholds and incurring chargeback related losses - brand reputation is also at stake. **Over half of consumers surveyed said they would never return to shop at a business where their online account was compromised**. Spanish shoppers were the most adamant, at 62%. Only 15% of respondents said this type of security breach would not impact their shopping choices.

European Consumer Survey

WOULD YOU CONTINUE SHOPPING FROM A BUSINESS WHERE YOUR ONLINE ACCOUNT WAS COMPROMISED?



> **According to our survey, a third of shoppers will go elsewhere when experiencing issues completing an online purchase**

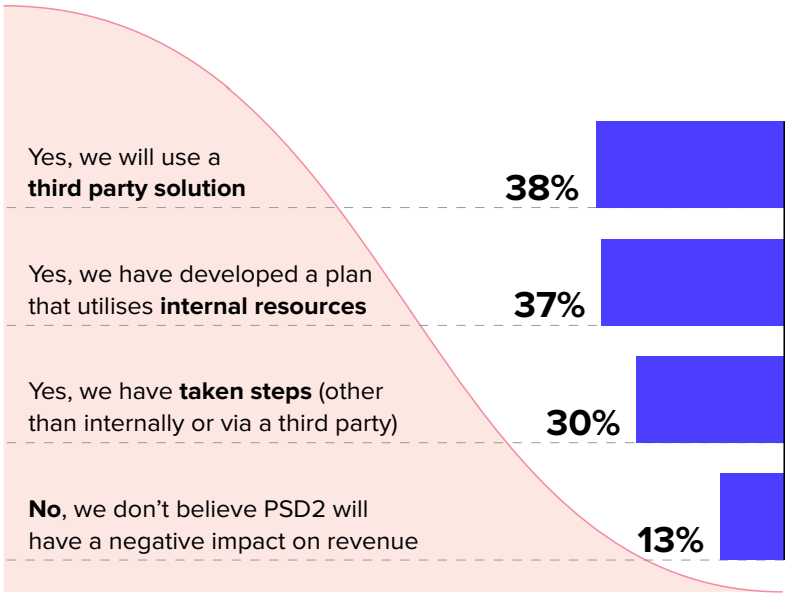
So what should you be doing to ensure you are both PSD2 compliant and sufficiently protecting your revenue and brand reputation?

Shopping for a PSD2 Solution

If you are like the majority of European retailers, you have already taken steps to minimise the negative impact that PSD2 might have on your revenue. But it's vital to make sure that your current plan is sufficient for the long-term.

European Retailers Survey

HAS YOUR COMPANY TAKEN STEPS TO MINIMISE THE NEGATIVE IMPACT THAT PSD2 MIGHT HAVE ON REVENUE?



The following section describes: some of the options available to merchants for protecting their eCommerce revenue in a PSD2 world; the key considerations when deciding which approach to adopt; and suggested questions you can ask vendors to ensure you are making the best choice for your organisation.

Common merchant approaches to PSD2

1. Basic compliance

At the very least, basic PSD2 compliance requires you to enable 3DS for CNP orders within the scope of the regulation. But relying solely on this protocol to deal with PSD2 has drawbacks:

- the potential for much more customer friction;
- limited insight into your online shoppers' experience;
- holes in your fraud review process; and
- no exemption optimization.

2. Developing an in-house solution

Some merchants are developing mechanisms to identify which orders are within PSD2's scope, which of those require SCA, and which transactions should be sent for exemption.

If you are thinking of building an in-house solution to manage your orders under PSD2, the principal factor to account for is the resources required to do this well. Reviewing CNP orders for fraud accurately requires significant expertise and technological know-how. Creating a system that runs in real-time, routing orders appropriately and reviewing them for fraud pre-authorization, is no easy feat. Amongst other things, an effective fraud prevention solution calls for:

- in-house fraud expertise;
- a team of data scientists and engineers;
- developing complex models;
- access to extensive historical data for model training; and
- ongoing investment in data enrichment services.

In short, developing an in-house solution can provide more insight into customer experience and control over the fraud review process, but you may want to consider engaging a third party solution to carry at least some of the load.

3. Engaging a third party solution

Gateways

Many payment gateways operating across Europe offer exemption routing services, often promoted in conjunction with fraud review products.

Pros

- You have an established relationship with your gateway, making this may seem like the least risky option in the short-term, while you're still unsure of the full implications of the regulation.
- Some gateways have close relationships with issuing banks, which may prove valuable for determining enforcement timing and staying on top of exemption thresholds.

Cons

- Fraud detection hasn't been a focus for payment gateways, so it's unclear how they will route the right orders for exemption.
- Gateways won't typically assume fraud liability for exempt transactions.
- Gateways will allow/block low-risk exemptions based on your fraud rate. This will inevitably lead to 'thrashing' - periods of 100% exemptions followed by periods of 0% exemptions, and so on.

Authentication-first solutions

A number of vendors offer 'frictionless' SCA as an alternative to 3DS via biometric and behavioural based authentication.

Pros

- Inherence-based authentication aims to decrease friction (compared to other forms of SCA). Some vendors are so confident of the approach, they claim exemptions could become redundant.
- There is no denying that verification via inherence is a step in the right direction for the long term (say, three years from now).

Cons

- Frictionless SCA relies on inherence data being transferred to the banks via 3DS 2.2, which isn't yet widely adopted by banks.
- Because it's still unclear which inherence-based solutions meet SCA standards, some orders will probably still go through older versions of 3DS or experience friction due to failed authentication attempts.
- This type of authentication must be FIDO certified (which is very difficult to achieve).

Exemption-first solutions

Several vendors, including established eCommerce fraud prevention companies, are offering solutions whose primary focus is to have as many orders as possible undergo frictionless TRA, rather than SCA.

Pros

- Fraud prevention companies are naturally experts at reviewing orders for fraud - and some have essentially spent years perfecting effective TRA.
- Some of these vendors offer a holistic solution that covers fraud outside of PSD2's scope. In general, these vendors will be best at dealing with ATO attacks, omnichannel orders, cross-border transactions, and order volume spikes.
- Vendors with a large database of transactions will be able to collect data on issuers and advise on enforcement timing.

Cons

- As the premise of these vendors' PSD2 products relies on exemptions, integrating with these solution before SCA is being applied, may seem premature.

Questions for potential vendors

Q: **Will you give me visibility into my orders?**

One of the challenges of PSD2 is that while it shifts fraud liability to the issuing banks, it also reduces your control over customer experience. Many merchants are concerned that under PSD2, they will lose control of how their eCommerce orders are handled. When considering your options, find out whether the vendor will provide you with insights on: which transactions were declined due to suspected fraud; exemption requests (which orders were routed for exemption and which exemptions were granted); what happened to out of scope orders; and what happened to the orders that underwent SCA (including those that failed).

Q: **What expertise do you have in my key markets of interest?**

Make sure the vendor has a successful track record working with merchants in the European eCommerce market. Ideally, seek evidence of their ability to improve revenue and performance for merchants in your industry. It's also important to find out about vendors' experience in global markets to ensure they can help you sustain high performance based on any international business expansion plans. This experience should also be considered given that orders outside of PSD2's scope include one-legged transactions.

Q: **As fraud evolves, how will you be able to protect me against new MOs?**

Given SCA's limitations in preventing CNP fraud, you stand to benefit from partnering with a vendor with a holistic solution to fraud prevention. Banks are only going to become more conservative when it comes to their risk management, so it's worth selecting a solution that mitigates the impact of fraud, including through pre-auth fraud review and ATO attack prevention.

Q: **How will you maximize SCA exemptions?**

Vendors that set broad rules for determining when to push for exemptions, or whose processes haven't been optimized, will negatively impact your revenue. Make sure the vendor is filtering out fraud prior to authorization to improve your standing with banks, reduce payment declines, and maximize SCA exemptions.

Q: **Do you provide a chargeback guarantee?**

Some vendors take full financial responsibility for chargebacks incurred on transactions exempt from SCA (where fraud liability shifts back from the issuing bank to you). A chargeback guarantee may also be applied to orders out of PSD2's scope.

Q: **What technology is at the base of your solution?**

There are so many buzzwords being thrown around - "machine learning", "artificial intelligence" - but what is the solution really offering you? It's important for a vendor to have an immense trove of transactional data in your key markets, models that have been trained on this data to deliver accurate decisions, and linking capabilities–so that new transactions can be cross-checked against all others in the vendor's database.

Q: **What kind of data do your models draw on to ensure accuracy?**

Many players claim they have superior ability to provide accurate decisions regarding fraud and SCA exemptions. You need to make sure the vendor has sufficient experience analyzing CNP orders, particularly across Europe. Find out how many orders the vendor has reviewed for fraud, and confirm that their models have been trained on vast amounts of order data. Does the vendor have access to the most relevant data sources per region? Which industry-specific data sources and model features does the vendor draw on? Do they have behavioral analysis, and anomaly detection capabilities?

Q: **What's your incentive to ensure my revenue remains protected under PSD2?**

For vendors providing a chargeback guarantee, the answer to this is fairly straightforward: their interests should be aligned with yours because their potential profit margin declines for every order that goes through SCA instead of TRA. Vendors who charge a flat fee per transaction, regardless of whether the order is captured, don't necessarily have this incentive.

Q: **How does your solution help deal with orders that fail mandatory SCA?**

Regardless of the solution you choose, some orders will ultimately go through SCA. As a result, some customers will drop-off due to the friction or fail authentication. Ask the vendor if they can help you reclaim these orders, particularly given that many of them could be over €500.

About Riskified

Riskified is a leading eCommerce solution provider with a proven track record driving eCommerce revenue and improving customer experience for some of the world's leading retailers. Since 2012, we have reviewed over a billion orders for thousands of eCommerce merchants, including Fortune 500 companies.

Our suite of products provides merchants with holistic coverage, from dealing with basic fraud to the most sophisticated ATO attacks. Riskified's AI platform recognizes fraud at any point in the online shopping journey, across channels, geographies, and industries, allowing merchants to safely approve more orders while providing a frictionless customer experience - all while guaranteeing the income.

PSD2 Optimization is our latest offering, designed to help merchants keep legitimate customers moving along the path to purchase. To hear more about how it can help you comply with PSD2 while still taking a proactive approach to protecting your online revenue and brand reputation, contact us at sales@riskified.com.

riskified