PREPARING FOR **PSD2** AND ITS IMPACT ON FRAUD

FORTER

WHAT IS PSD2?

The retail market continues to expand rapidly, with e-commerce sales in the EU-5 expected to pass $325 billion this year, and exceed $400 billion by 2020. The continuous expansion and development of this space is exciting for consumers and merchants alike. But it comes with the growing need for increased security management and regulatory requirements. In an effort to create a level playing field in the payments space, the European Union designed the **Revised Payments Services Directive (PSD2)** to standardize, integrate and improve payment efficiency.

PSD2 essentially breaks the banks' monopoly on their users' data, giving online retailers the ability to retrieve customer account data directly from a customer's bank, with the customer's permission. The idea would be to cut out the middleman completely, allowing the retailer to make payments on behalf of their customers, without ever having to redirect the user to another service provider.

PSD2 was initially introduced in 2015 (and has applied since January 2016), but members of the EU have had until January 2018 to implement the directive. By September 14, 2019, merchants were supposed to ensure that they comply with the broader scope of the PSD2 rollout which includes a more stringent authentication process called **Strong Customer Authentication (SCA)**.

At this time, enforcement is uncertain and going to be determined on a market-by-market basis. So far, the UK's Financial Conduct Authority (FCA) has confirmed an **18-month delay to the introduction of Secure Customer Authentication (SCA) rules for firms in the UK** in a bid to give relevant parties more time to prepare. The FCA was not alone in this request, as the Central Bank of Ireland and regulators in Malta have asked for similar delays.

It is important to note that at this time, **only the UK has been granted such a delay**. The agreement reached between the FCA and payment card issuers, payment providers, and online retailers, **provides scope for e-commerce retailers to work towards the required SCA-compliance over a period that could last up until 14 March 2021**, without fear of punishment from regulators over non-compliance issues.

PSD2 and the expectation of SCA compliance will eventually be enforced, though some markets may experience delays. Nevertheless, all merchants should ensure their businesses are prepared for forthcoming requirements and enforcement timelines.

THE DRIVING FORCE BEHIND PSD2

Both PSD2 and its predecessor PSD1 were created with the intention of equalizing the payments landscape, with the end goal of increasing competitiveness and strengthening security and authentication processes for online customers. The idea is to ultimately provide consumers with better value, ushering in a new era of "open banking." This new era would provide customers with unprecedented freedom in how they access financial services, and how they choose to transact online.

With that idea in mind, the PSD2 regulations introduce two new types of authorized payment institutions, or what are deemed **third party payment services providers (TPPs)**, giving customers expanded options in how they manage their finances:

1. **ACCOUNT INFORMATION SERVICE PROVIDER (AISP)**
   AISPs provide aggregated account or available balance information on one or more payment accounts held by the payment service user.
2. **PAYMENT INITIATION SERVICE PROVIDER (PISP)**
   PISPs initiate payment orders at the request of the payment service user with respect to a payment account held at another payment service provider.

Under the tenets of PSD2, fintech companies, merchants, banks, and insurance companies are all eligible to become TPPs. Companies that desire to become TPPs (and thereby gain access to customer transactional data and account information) will need to obtain either AISP or PISP licenses.

> This expansion of access also means private consumer data will now be available to more players than ever before.

However, this expansion of access also means private consumer data will now be available to more players than ever before. As such, the introduction of PSD2 regulations means stricter rules to which all new providers will need to abide.

THE DIRECTIVE SETS OUT RULES CONCERNING:

- **Strict security requirements** for electronic payments and the protection of consumers' financial data, guaranteeing safe authentication and reducing the risk of fraud
- The **transparency** of conditions and information requirements for payment services
- The **rights and obligations** of users and providers of payment services

STRICTER SECURITY REQUIREMENTS THROUGH SCA

In an effort to improve cybersecurity in the payments space and better protect consumer data, the European Economic Area (EEA) created requirements for authenticating online payments known as **Strong Customer Authentication (SCA)**. SCA requirements fall under the broader scope of the PSD2 rollout, and are set to pose the greatest impact on all players in the market. These SCA requirements intend to better protect online customer data while reducing online transaction fraud.

SCA requirements will apply to customer-initiated online purchases that occur specifically within the EEA, under the condition that both the cardholder's issuing bank and the merchant's payment provider (acquirer) are in the EEA. The additional SCA security requirements will mean that customers will need to authenticate their identities using **two** of the following three options:

> These increased authentication requirements injected into the payment process are likely to increase friction in consumers' shopping experiences.

KNOWLEDGE

Something the customer knows (e.g. password)

POSSESSION

Something the customer has/owns (e.g. phone)

INHERENCE

Something the customer is (e.g. fingerprints, facial recognition)

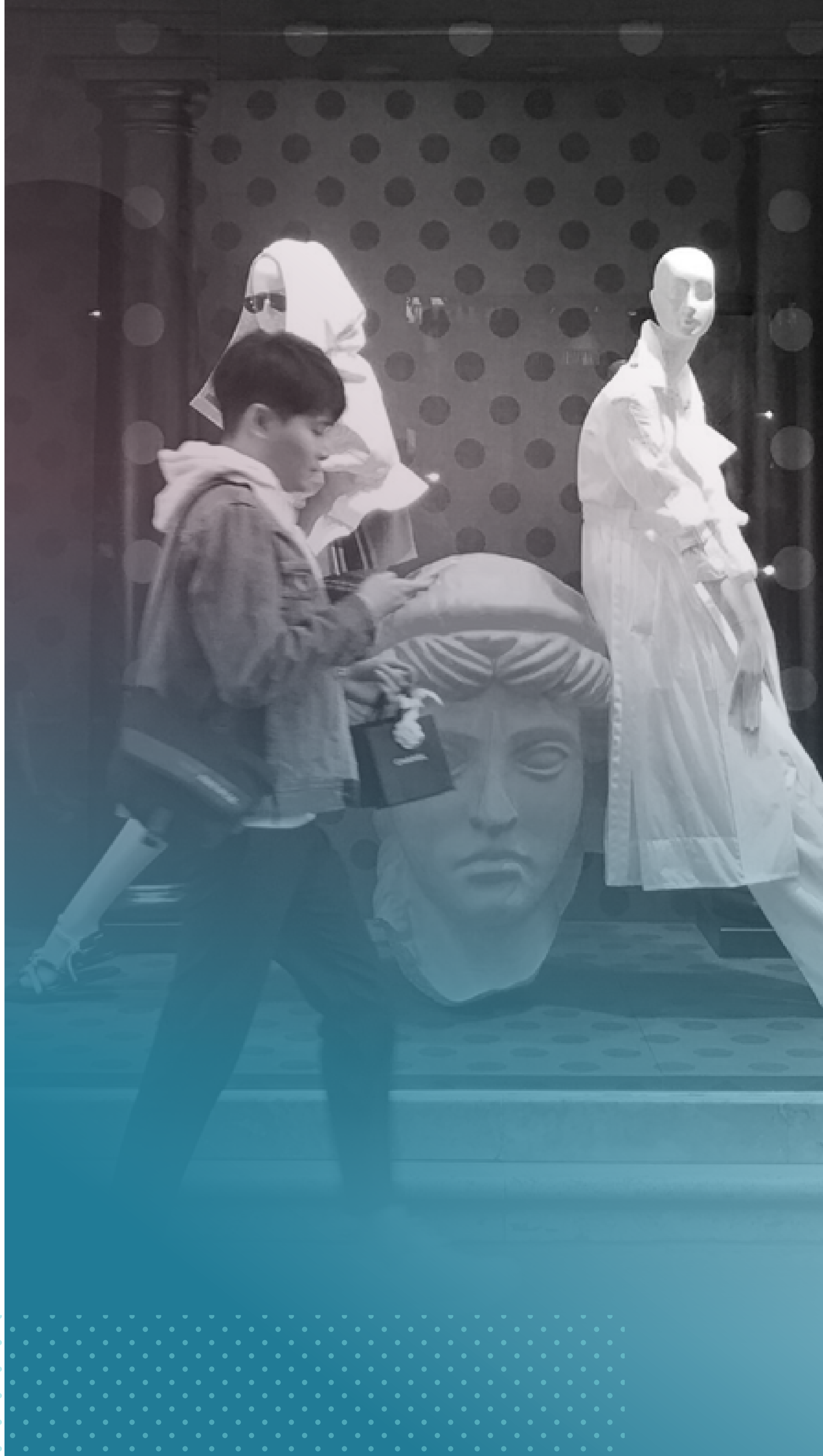
These supplemental and stringent regulations intend to minimize and mitigate online fraud by mandating a more uniform approach to customer authentication. However, these increased authentication requirements injected into the payment process are likely to increase friction in consumers' shopping experiences, and businesses will have to find a way to simultaneously add security measures while ensuring a streamlined customer journey.

SCA EXEMPTIONS

Not all transactions will be required to adhere to SCA. There are exemptions, but they are poised to be very limited and ultimately controlled by the issuers.

The key exemptions to SCA include:

✓ LOW RISK TRANSACTIONS	Transactions assessed as low risk through Transaction Risk Analysis (TRA) and where the PSP is below set fraud thresholds
✓ LOW VALUE TRANSACTIONS	• Transaction under €30 may be exempt from SCA • However, SCA is still required if exemption is applied more than 5 times OR if sum of payment is > €100 since last exemption on the card
✓ RECURRING TRANSACTIONS	Recurring transactions of the same amount to the same business; SCA is still required on the 1st transaction
✓ TRUSTED BENEFICIARY	Customer adds business to a whitelist with their issuer
✓ CORPORATE PAYMENTS	B2B payments made using a dedicated payment instrument



Additionally, there are exclusions that fall outside of the scope of PSD2, including: merchant initiated transactions, mail and phone orders, anonymous prepaid card transactions, direct debit payments, and one-leg-out transactions, when either the payer or payee is based outside of the EU.

Again, **PSD2's SCA requirements go into effect on 14 September 2019**. Although there is the potential for delays to enforcement of these laws, merchants should plan to ensure their businesses are compliant as soon as possible.

At this time, **only the UK has been granted an 18-month delay** to this upcoming deadline, requiring instead that all businesses have **SCA compliance by 14 March 2021**. Until this date, merchants may operate without the fear of punishment from the regulator for non-compliance with the new standards.

COMPLYING WITH PSD2 THROUGH 3DS

In order to comply with PSD2 and SCA requirements, the standard protocol for merchants is to rely on **3-D Secure (3DS)** for affected transactions. 3DS is a protocol developed by EMVCo., and is an authentication scheme which requires a cardholder to enter an additional password when making an online purchase. **When 3DS authentication is enabled and successful, liability shifts from the merchant to the issuing bank**. 3DS has been leveraged as an additional layer of security and is typically applied to higher-value transactions.

However, 3DS (the predecessor to the newly updated 3-D Secure 2.0 (3DS2) protocol), was notorious for creating additional friction in the customer journey, and had a negative impact on conversion rates. Under the original 3DS protocol, nearly one quarter of global payments were lost when authenticated, and authentication took an average of 37 seconds. according to data from Ravelin. 3DS2, as the latest iteration of the protocol, has been designed to be less intrusive for customers than its predecessor. But there is no doubt that it will introduce significant friction into the shopping journey, and will be required for every transaction, not just the riskiest.

Additions to the 3DS2 protocol include an expansion to the number of data points captured for issuer evaluation (150 instead of 15 as occurred in 3DS), an increase to the number of authentication models (RBA, biometrics, one-time passwords, out-of-band), as well as improvements to the UX (enhanced browser support, optimized for mobile & native apps, supports exemptions).

SCA AND THE IMPACT ON CHECKOUT

Some merchants are hopeful that SCA may be able to increase authorization rates overall, but consumer data reveals an ominous trade-off. SCA will notably increase friction for consumers since it requires customers to engage in additional authentication steps.

The increase in friction is a concern for merchants with an eye on their bottom line, since friction is known to correlate with cart abandonment. According to a Forter survey, 56% of consumers said that the more effort it took to complete a purchase, the less likely they would be to buy their items. Inherently, extra verification mechanisms take more time and more effort from the consumer, allowing for customers to second guess their purchase and buy less impulsively. In fact, even forward-thinking banks that have already implemented one-time password and app-based verification still lost 19% of transactions through 3DS.

Until now most merchants have avoided 3DS where possible. Under PSD2, that will be more difficult. Merchants will have to devise a process which meets SCA when required but aims to avoid friction otherwise. Merchants should explore relationships with partners like Forter who are able to achieve SCA but are also strongly focused on optimizing customer experience.

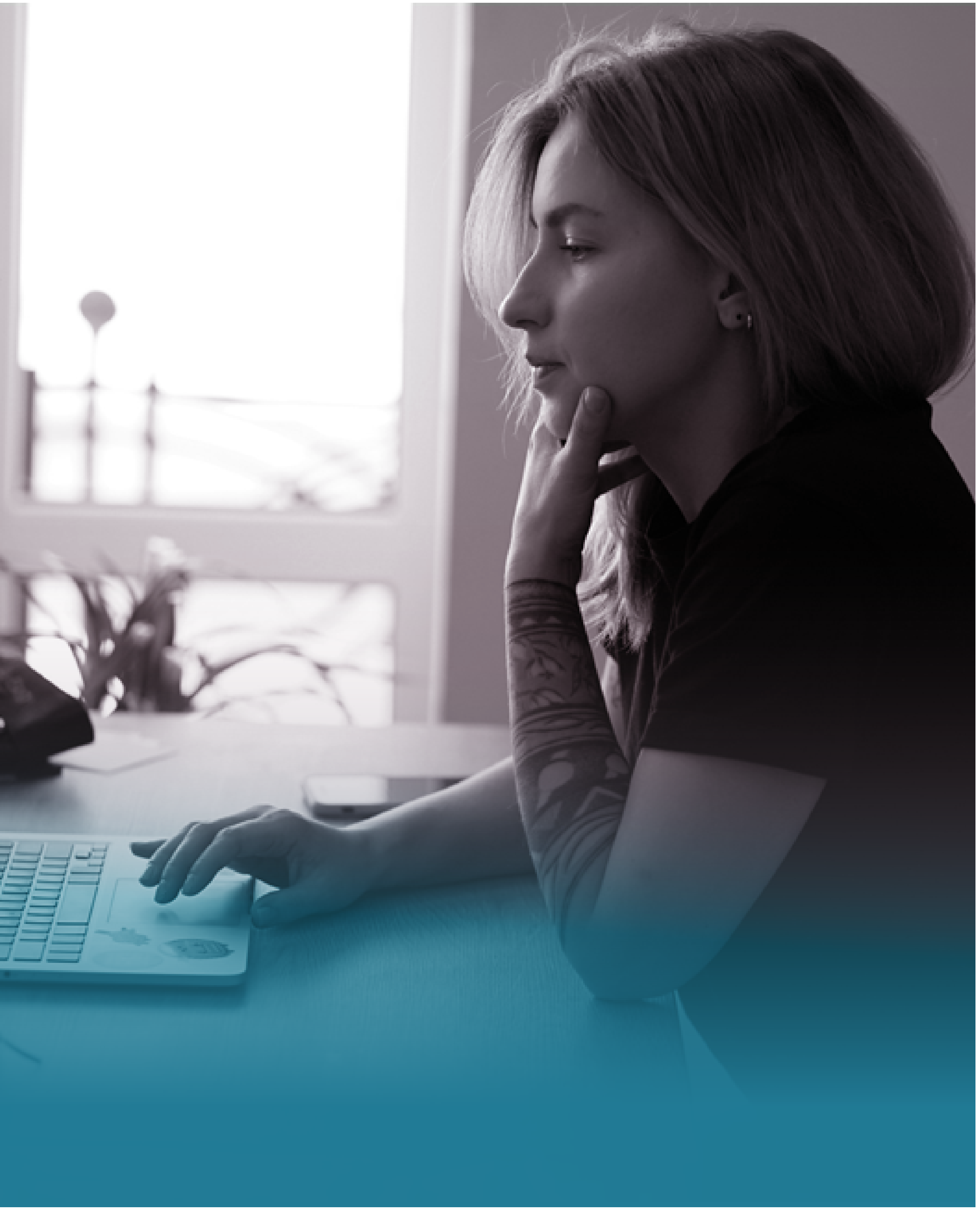
The consequences of a poor customer experience can be long-lasting. Forter's survey found that 76% would not shop with a merchant again if they had a negative online shopping experience. Merchants should start considering the customer experience aspect as part of all of their relationships with providers in the payments space. With PSD2 changing the playing field, it's important to make sure partnerships are geared towards enabling revenue generation and positive purchase experience as well as ensuring compliance and lowering risk.

CHANGING RELATIONSHIPS WITH ACQUIRING BANKS

The initial drive behind PSD2 was to open up opportunities for new companies and technologies in a space which had traditionally belonged exclusively to banks. The idea was to smooth the path to innovation, something that would ultimately benefit everyone involved, including merchants and consumers. It was therefore expected that PSD2 would change things for banks.

The way PSD2 was formulated means banks will feel its impact from the very beginning. Banks will be measured on the collective fraud rate of their entire merchant portfolio, instead of the fraud rate of each individual merchant. This means that acquiring banks will need to closely manage their overall fraud rates in order to remain eligible for receiving low risk transaction exemptions.

This has a ripple effect on merchants as well. Banks may become more conservative about approving transactions if there is any uncertainty about them, since their focus will be on maintaining a low fraud rate and protecting their own liability. As 3DS shifts liability away from the merchant, banks may fear increasing their own liability in the case of chargebacks. Banks aren't incentivised to approve transactions, and merchants may see a higher number of transactions being declined as a result. This can heavily impact a merchant's bottom line, but also their customer relationships if legitimate transactions get regularly declined. Merchants should engage in an open discussion about these issues to ensure they are working with banks and payment partners who are sensitive to these possibilities.



> With PSD2, fraud prevention for merchants becomes an integral part of maintaining healthy relationships with acquiring banks.

The specter of fraud also becomes a greater problem for merchants, for a new reason. Since every merchant in a bank's portfolio contributes to the bank's overall fraud rate, it will become even more important for merchants to keep their fraud rates low. A high fraud rate could harm a merchant's relationship with their acquirer, as this will contribute to the bank's overall portfolio fraud rate, or even cause them to get dropped. With PSD2, fraud prevention for merchants becomes an integral part of maintaining healthy relationships with acquiring banks.

THE FUTURE OF FRAUD

Fraud is constantly changing, and merchants need to be prepared for that. PSD2 will impact multiple aspects of the payments landscape, and fraud is no exception. As was seen in the shift to EMV cards, when fraud decreased in-store but drastically increased online, fraudsters keep up to date with changes in the payments world that may impact their theft and change their attacks accordingly. Businesses who try to fight fraud based on last year's data rather than looking ahead to the post-PSD2 shift will be at risk.

One advantage of PSD2 from the fraud perspective is that it may become easier to separate real fraud from "friendly fraud." Some customers abuse the system by claiming fraud when they are not satisfied with the merchandise or have a similar service complaint, in order to increase their chances of a refund. These individuals will find this trick harder to play with new authentication requirements adding extra protection. As a result, these "liar buyers" will have to submit service chargebacks instead of fraud chargebacks to dispute product issues, and merchants may want to prepare their customer service departments accordingly to plan for increasing operational costs in that area.

> Businesses that try to fight fraud based on last year's data, rather than looking ahead to the post-PSD2 shift, will be at risk.

It is also likely that merchants who accept phone orders may see an increase in fraud attempts against that channel. Phone and mail orders are excluded from SCA by PSD2, so fraudsters might shift to other channels in order to get around restrictions, similar to the effects on CNP fraud with the introduction of EMV cards.

There is a geographical component to the forecasted changes as well. PSD2 is specific to the EU; it will affect all EU to EU transactions. Transactions with only one EU leg, and transactions with no EU component at all, are unaffected. As a result, fraud will shift geographically, to regions outside of the EU such as the US and APAC, and fraudsters will begin using non-EU cards to get around SCA. Since many EU companies take non-EU cards, and many EU-based companies operate global businesses, this international perspective is something which will be vital to bear in mind.

Fraud teams and systems need to prepare for the changes coming to the geographical component of transactions and analysis. Fraud prevention partners who already work on a global basis will be able to offer advice about how best to guard against the shift and the types of attacks fraudsters are likely to attempt as a result.

FRAUD AT THE ACCOUNT LEVEL

Fraud prevention is primarily focused on protection of transactions; companies want to ensure that fraudsters don't place orders on their site. This is still important, but as customers interact with more and more touch points and merchants invest more in the overall customer experience — not just checkout — fraudsters are shifting to account attacks as well. PSD2 will only exacerbate this trend.

As SCA makes fraud at the transaction level more difficult, fraudsters will seek easier paths. For a fraudster, it's all about ROI: they want to be able to invest the least amount of time and effort possible for the greatest possible payoff. If transaction fraud is harder to pull off, they'll target customers' accounts instead.

The most obvious form of account attack is account takeover (ATO), when a criminal hacks into a victim's account and uses the information to their benefit. Sometimes they will use the stored payment information to make a purchase, which may still be possible even with PSD2, as the transaction may well appear to be low risk since it emanates from the victim's account and leverages their data.

> As PSD2 makes account attacks more appealing to fraudsters, companies will need to be able to identify and block these attempts.

Loyalty programs are also a weak point on the account level. The use or transfer of points is typically not guarded to the same extent as the point of transaction, even though a purchase is effectively being made. Customers need protection, as they rarely check their points with the same regularity that they do their bank accounts.

More complex types of fraud such as collusion in online marketplaces and identity theft used for private label card applications are also possible avenues of interest for fraudsters looking for vulnerabilities, and companies who offer such services should prepare.

Merchants need to shift their perspective to protect the entire customer journey, not merely the point of transaction. As PSD2 makes account attacks more appealing to fraudsters, companies will need to be able to identify and block these attempts which will otherwise damage their revenue, their understanding of their own ecosystem and precious customer trust.

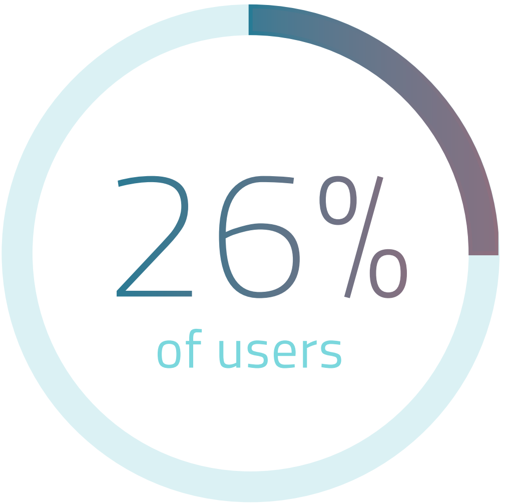
HOW CAN MERCHANTS PREPARE FOR PSD2?

There is an increased focus on the importance of consumer privacy and data protection, and the introduction of the PSD2 regulations are a reflection of this phenomenon. The true intention is to drive innovation in the market, creating a more competitive landscape for merchants and consumers alike.

So what can merchants do to prepare for these new regulations?

Merchants will need to strike a balance between risk and friction, to ensure they retain their customer base and don't turn away potential customers. Increased friction injected into the customer shopping and buyer's journey will ultimately lead to higher rates of customer drop off. A 2018 Baymard Institute study found 26% of users abandon shopping carts if the checkout process is too long. As such, 3DS2 will not be a silver bullet solution to PSD2 and SCA. Merchants should look to partner with fraud prevention experts like Forter who can offer a compliant solution to PSD2 and SCA, while ensuring the path of least possible friction so merchant customers will receive an optimal user experience.

> Increased friction injected into the customer shopping and buyer's journey will ultimately lead to higher rates of customer drop off.



abandon shopping carts if the checkout process is too long.*

*Baymard Institute study

Merchants should also start conversations with acquirers to understand their approach to Low Risk Transactions (TRA) exemptions, their portfolio fraud rates, and to better understand the TRA exemptions. It is important to note that applying for an exemption is optional. The merchant or acquirer can ask for exemptions, but ultimately the issuer will have final say over whether one is granted. In this instance, liability is then shifted to the party requesting the exemption. As part of the 3DS protocol, if an exemption is indeed applied, the fraud liability will fall back on the party that requested the exemption instead of the card issuer, which will own the fraud liability on all transactions to which SCA is applied. As such, the payment provider (or merchant) will want to have a solution in place that is able to guarantee fraud chargeback coverage in order to avoid the liability shift and costs associated with these claims.

PSD2 and SCA may be focused on strengthening authentication surrounding payment and transactional fraud, but merchants should be investing in broader fraud prevention now, and preparing for shifts in vulnerable areas beyond the point of transaction. Merchants should look to providers with global experience, who can meet the new regulations while simultaneously protecting the broader customer shopping experience. In light of PSD2 and SCA, fraud attempts are likely to shift to other areas of the customer journey, and merchants will need to have a fraud prevention solution in place in order to combat all forms of fraud. **Moreover, fraudsters aren't lying in wait as SCA enforcement goes into place. They will continue to launch attacks against merchants and will do so in the time leading up to global SCA enforcement.**

From fraud at the account level, ranging from ATO attacks to loyalty program abuse, merchants will need to take a more holistic view of the customer journey, understanding that fraud will occur and continue to grow within other more vulnerable touch points. As such, merchants need to protect the entirety of their platform and customer ecosystem.

THE WAY FORWARD

There are many uncertainties surrounding PSD2, and interpretations of the directives are constantly changing. **PSD2's SCA requirements go into effect on 14 September 2019**, enforcement has yet to be determined, but at this juncture, **only the UK has officially announced an 18-month delay to SCA implementation (requiring compliance by 14 March 2021)**.

Regardless of timeline for enforcement or any delays to implementation notwithstanding, it is in all merchants' best interests not to wait on their PSD2-preparedness. It is essential for merchants to be ready and compliant for every market so that their business will not experience any delays once enforcement does indeed go into effect. Requirements and enforcement schedules may vary and will be difficult to predict, some markets will require earlier compliance and activation, while others may take longer to ramp up. Banks and other financial institutions may even require SCA prior to legal enforcement. As such, it will be important for merchants to remain informed and knowledgeable of shifting PSD2 timelines and requirements in order to ensure they don't fall behind or have transactions unnecessarily declined as a result of ill-preparedness.

Similarly, as merchants prepare their businesses for this quickly approaching deadline, they should remain nimble and ensure that they have a trusted partner who can help them navigate the shifting global landscape. As online commerce continues to expand and more stakeholders join the fold, it is important that businesses ensure continued compliance efforts by leveraging the most up-to-date procedures and systems. The payments field is growing rapidly and new regulations globally are likely to become increasingly common in order to ensure a more uniform approach to data security in the market.

NEXT STEPS

Not sure whether you're on the right path? Here are some key action items for your business to ensure your way forward to a PSD2-compliant solution is clear.

□ DETERMINE IF YOUR BUSINESS IS (OR WILL BE) IMPACTED BY PSD2

Figure out if your business falls under the scope of PSD2 and its requirements. If your business uses a European acquiring bank and sells to European customers, then your business is likely affected.

□ DEVELOP A PLAN FOR HOW YOUR BUSINESS WILL MEET PSD2'S SCA REQUIREMENTS

Ensure that your business has a plan to meet and comply with PSD2's SCA requirements by the September 14 2019 deadline. You will want to find a tool or strategy to maximize the usage of exclusions and exemptions to provide the most optimal customer experience to every customer.

□ ALIGN WITH YOUR PSPS AND ACQUIRERS

Work with your PSPs and Acquirers to understand their plans for PSD2 – how they're going to manage Transaction Risk Analysis (TRA) exemptions, what their current portfolio's fraud rate is, and more.

□ MAKE SURE YOUR FRAUD PREVENTION SOLUTION IS PRE-AUTHORIZATION

Pre-bank authorization fraud screening enables your business to decline fraud upfront and avoid unnecessary authentication and authorization costs, minimize friction under PSD2 to maximize conversions, and more.

□ INVEST IN A HOLISTIC FRAUD PREVENTION SOLUTION

Leverage a holistic fraud prevention solution that can proactively identify and stop payments fraud – stopping unnecessary authentication or authorization costs, while also stopping other types of fraud across the entire customer journey.

□ ALIGN YOUR SCA PROVIDER WITH YOUR FRAUD PREVENTION SOLUTION (IF NECESSARY)

Both authentication and fraud prevention solutions leverage data about your business to protect it from fraud, and they also both impact your customer experience. Make sure that they're in sync for optimal accuracy and performance.

About FORTER

Forter's fraud prevention solution protects online merchants from fraud attacks and abuse at both the account level and the point of transaction, while maintaining a seamless customer experience. By leveraging an expansive global network spanning more than 2.1B devices and over $130B in processed transactions, Forter determines the legitimacy of each individual that comes into contact with a retailer's site. We are powered by a unique blend of artificial intelligence and predictive fraud research, resulting in exceptionally accurate fraud protection, more sales, and happier customers.

For more info visit **www.forter.com**