Your Guide to PSD2: Achieving Strong Customer Authentication

eBook
According to a recent McKinsey & Company study, the average share of customer interactions that were digital in nature rose from 36% to 58% between December 2019 and July 2020. This dramatic increase in digital transactions makes it more important than ever to ensure your customers’ identities, accounts, and interactions with your company are secure. A number of regulations are addressing this need, and if you do any of your business online, you likely have heard of the European Union PSD2 (Payment Services Directive 2) that rolled out early in 2021.

PSD2 is a new e-commerce regulatory policy that is now in place in the European Union and is reshaping the way that businesses and financial institutions process online transactions. With this new regulation in place, PSD2 compliance aims to increase security for online purchases and streamline customer authentication.

Adapting your business to new regulatory policies can seem overwhelming, but fortunately, implementing the right communication and security processes isn’t all that difficult. Businesses and financial institutions can meet these increased security measures with minimal friction and even improve the end-user experience.

This ebook will give you an overview of the high-level details of PSD2, its benefits to you and your customers, and some helpful information on building PSD2 requirements into your business.
First, let’s start with the basics

What is PSD2?

The short answer: PSD2 is a two-pronged regulatory policy in the European Union that compels banks to allow third-party access to customers’ account data and also requires that online transactions meet minimum security standards to protect customers from card-not-present fraud and ultimately increase the overall security of the payment landscape in the EU.
The long answer: PSD2 brings two major changes to the European digital payments landscape. First, it requires eCommerce vendors and financial institutions to implement stronger security and additional verification methods for online transactions. This is achieved through Strong Customer Authentication (SCA) which can defend against and mitigate account takeovers, unauthorized account access, and fraudulent transactions.

Second, PSD2 institutes ‘open banking’, which uses APIs to bridge the divide between the players involved in an online transaction. Open banking forces banks to give third-party access to consumer bank account data** and shortens the supply chain of information processing, making it easier for merchants to approve legitimate transactions. Payment Services Providers (think PayPal, Stripe, etc.) will have instantaneous access to customer account data and can more accurately authenticate user payments without having to wait for the merchant to talk to the Payment Services Provider, the Payment Services Provider to talk to the Account Information Services Provider, the Account Information Services Provider to talk to the bank, and so on.

**Don’t worry, these third-party services will only have access to user’s account information if account holders give their consent.

So, the big picture is that the EU wants to make the European payments market more efficient, level the playing field for payment service providers, make payments safer and more secure, and protect consumers from fraud. PSD2 does this by making customer account data more widely available so that it is easier for payment services to verify legitimate customer purchases and by requiring ecommerce platforms to enact stronger security measures at payment to verify that customers really are who they say they are.
Are you sure that PSD2 applies to me?

Well, if you are a business or a financial institution intending to do any online business within the European Union, it probably does. If you do not comply you will not be able to accept electronic payments within the EU.

Technically, the requirements only officially apply to transactions in which both the card issuer and the acquiring bank are in the European Economic Area, but given the benefits that the increased security standards provide, we expect that many European card issuers will apply the same rules across all transactions, regardless of the merchant’s location.

Besides, even if you don’t currently conduct e-commerce within the EU, you may want to think about becoming PSD2 compliant anyway—financial technology is constantly growing, and that growth has massive worldwide impact. China, Japan, Australia, Singapore, Mexico, and Latin America all support open banking practices and it’s also on the rise within the US.² Open banking means a streamlined payment approval process, but if you’re a merchant, you’ll want to back up that data flow with increased platform security.
PSD2 compliance could benefit you if you:

- Plan to conduct online business within the European Union
- Want to establish a reputation for your brand that emphasizes customer security
- Want to cut down on operational costs that occur when combating fraud (customer support, individual customer verification, payment refunds, etc.)
- Want to enjoy the benefits of open banking but still protect customer information
- Want to create a more personalized and secure experience for your customers
- Want to be ready for the next era of online commerce
- Would rather spend resources automating fraud prevention than spend them addressing fraudulent attacks after they occur
So what do I have to do if I want to become PSD2 compliant?

PSD2 makes it easier for merchants to know their customers and shortens the information supply chain that was previously involved when authorizing customer payments, but that customer data still needs to be protected. So, if you’re accepting online payments as a merchant, financial institution, or vendor, you should be sure that you have the proper multi-factor security measures and back-end data checks in place for verifying transactions inline with PSD2 regulations.
What would these security measures look like?

To comply with PSD2, you’ll need to build Strong Customer Authentication (SCA) into your eCommerce platform. Gone are the days of relying solely on usernames and passwords.

SCA requires multifactor authentication that uses at least two of the following three elements.

- **Something the customer knows**
  (e.g., password or PIN)

- **Something the customer has**
  (e.g., phone or hardware token)

- **Something the customer is**
  (e.g., fingerprint or face recognition)

These multifactor authentication elements must be independent in that if one element is breached, it does not compromise the reliability of the others. By ensuring that you have verified two out of the three above qualifiers, you achieve SCA and therefore become PSD2 compliant. When a customer logs onto an account using a username and password, you’ve already achieved the ‘something a customer knows’ qualification, and you just need one more to have SCA.

Covering the ‘possession’ component can be as easy as implementing SMS and Voice two-factor authentication into your platform. For instance, customers can combine a password (something they know – their password) with an SMS one time passcode (something they possess – their smartphone) to meet SCA requirements.

Additionally, the SCA requirements lay out that transaction verifications must be dynamically linked between payee and payor.
Dynamic linking is in place to prevent man-in-the-middle attacks, where a fraudster attempts to interrupt the connection between the payer and the payee and hijack the authentication code to authorize fraudulent transactions. Dynamic Linking requires financial institutions to dynamically link the authentication code to both the payee and the amount. Specifically, PSD2 requires verifications to meet the following qualifications:

- The payer is made aware of the amount of the payment transaction and the payee.
- The authentication code generated is specific to the amount of the payment transaction and the payee agreed to by the payer when initiating the transaction.
- The authentication code accepted by the payment service provider corresponds to the original specific amount of the payment transaction and the identity of the payee agreed to by the payer.
- Any change to the amount or the payee results in the invalidation of the authentication code generated.

When dynamic linking is deployed, man-in-the-middle attacks fail because the authentication code is automatically rejected if the authentication trail (i.e., transaction information, amount, or the payee) has been altered.
It seems like a good system, but will I really have to verify every customer transaction?

There are several exceptions for when SCA is not required for an online purchase. The current exceptions are:

• Transactions under 30 Euros (unless five or more of these payments have been made since the customer’s last identity verification)

• Transactions conducted over the phone

• Recurring transactions that have the same payee and payment amount (like subscription-type services)

• Transactions with any specific merchants that an individual customer has manually selected to whitelist

• High-value transactions IF the acquiring bank ensures low fraud rates through other risk analysis methods. The exemptions can apply to:
  – Transactions of up to 100 euros for fraud rates below 0.13%
  – 250 euros for fraud rates below 0.06% and
  – 500 euros for fraud rates below 0.01%.
Is there a date that I have to meet PSD2 regulations by?

The deadline for implementing the security measures was December 31st, 2020, so if you conduct online business in the EU and haven’t taken measures to become PSD2 compliant yet, you’ll want to do so as soon as possible to avoid any fines or penalties for failure to comply.
While no one loves new regulations, there is clearly a need to strengthen payment security and transparency. Digital identity fraud alone costs $56 billion each year and estimates say cybercrime costs topped $6 trillion in 2020. While not all of this cost is payment related, as we continue to spend ever increasing amounts of our daily lives online, the incentives for fraudsters only grow.

Data breaches and customer account compromises have high direct costs in and of themselves but losing trust with customers has hidden costs as well. In fact, 30% of customers who experience fraud or a data breach at a financial institution will close their account, even if the issue is resolved. It goes without saying that maintaining trust with your customers is critical.

SCA, which is a cornerstone of PSD2, is designed to double verify higher risk transactions to reduce card-not-present fraud and account takeover fraud, just to name a few. Adopting these kinds of security measures can help you prevent costly fraud, deliver transparency, and build trust with your customers. For added security, ensuring that communications used in online transactions have not been misdirected to unauthorized parties is a good idea. Combining your SMS verifications with SIM swap and number porting detection adds this additional security and improves your verification solutions.
Becoming PSD2 compliant doesn’t have to be a resource drain. When planning your current and future PSD2 compliance needs, it’s important to select a solution that can be easily deployed and can scale with you. TeleSign can help you implement PSD2-compliant security measures into your existing online platform while minimizing transaction friction for your customers.

TeleSign offers global SMS and Voice verification, complete with dynamic linking compliance, through 700+ direct to carrier routes for unparalleled global delivery rates. Together with phone number and identity intelligence including SIM swap detection, number porting history, contact match, and more, we help you detect and protect your verifications against communication redirects.

TeleSign can uniquely help you with your PSD2 compliance and risk mitigation strategies with end-to-end digital identity, verification and communications solutions. Want to learn more? Talk to us today.

Learn more about TeleSign Global Verification Solutions
telesign.com | @TeleSign