ACI Worldwide
Real-Time Payments

Thriving Post PSD2: ACI's Five-Step Guide to Conquering SCA Compliance

Start

Five Ways to Achieve Strong Customer Authentication Compliance While Protecting and Differentiating on the Customer Experience

THE SECOND PAYMENT SERVICES DIRECTIVE (PSD2) — WHICH CAME INTO FORCE IN JANUARY 2018 — REPRESENTS A SEISMIC SHIFT IN THE WORLD OF PAYMENTS.

A follow up to 2009's PSD1, the regulation gives customers and businesses the ability to integrate third-party providers into their financial management processes.

However, this third-party access is by no means the only significant change. As of December 31, 2020 banks will also need to enhance consumer protection with strong customer authentication (SCA) for online, instant payments or card-not-present (CNP) transactions. This new mandate should make payments more secure — but unless banks can find a way to implement it in the right way, the customer experience is also at risk of being damaged.

While PSD2 is positive for consumer security, the directive has already caused headaches for banks. They've had to work out how to provide third-party access securely and efficiently — while grappling with the fact they are now competing on a broader stage. Now, they also need to navigate providing an appropriate amount of friction to balance the demands of SCA with a positive customer experience. The matter is complicated further by the fact that more transactions are taking place across **more channels and payment types than ever before**.

To turn SCA compliance into a competitive differentiator, financial institutions will need a clear strategy. Here are five key points to help you conquer compliance and thrive in a post-PSD2 world.

What Is SCA?

Strong customer authentication (SCA) aims to improve security through the use of more stringent multi-factor authentication. This covers customer-initiated transactions, including card, CNP and alternative payments — although certain transactions, like low-value contactless payments, can be excluded.

1 Assess the Landscape

BEFORE YOU BEGIN IMPLEMENTING SCA, TAKE THE TIME TO ASSESS THE LANDSCAPE OF YOUR CURRENT PSD2 COMPLIANCE CAPABILITY.

Consider what stage of the journey you're at, and what challenges you're facing — whether that's a lack of internal resources to implement SCA, technical integration barriers or concerns around customer experience.

You should also account for the fact that SCA is a multi-factor authentication process, so you need to assess your organization's readiness to adhere to this, as well as your current processes.

Under SCA, online or CNP transactions will need to be judged on two or more of the following factors:

Knowledge: A PIN, a password or the answer to a secret question

Possession: A token or a known, trusted device

Inherence: A factor inherent to the individual, such as biometrics (typically fingerprints, facial recognition or voice recognition)

So, you may need to plan to onboard the relevant technologies.

3DS 2.2 and SCA

The latest version of EMVCo's 3-D Secure specification, 3DS 2.2, provides an effective way to complete SCA for a larger percentage of eCommerce card payments. When combined with an effective transaction risk analysis tool that can identify exemption-qualifying transactions in real time, the protocol also provides a frictionless payments experience which in turn brings enhanced customer experience.

2 Don't Just Meet Requirements — Exceed Expectations

WITH SO MUCH TO CONSIDER, STRIVING TO MEET A NEW COMPLIANCE MANDATE CAN FEEL OVERWHELMING.

As a result, it can be tempting to only aim for the minimum requirements. Unfortunately, this approach will have an immediate and undeniable impact on customer experience.

For example, to comply with SCA, many banks will verify online or CNP transactions with one-time passwords sent via SMS text message. While this meets SCA requirements, it can increase customer friction considerably (and thus damage the customer experience) if employed with a heavy-handed approach. Think of a business traveler sitting in a foreign airport lounge; while they'll have access to WiFi, they may not be receiving SMS messages, and thus won't be able to access their code.

Other examples include email, in-app authentication and hard tokens readers. Ultimately, all have potential flaws and will inevitably lead to frustration — especially if the transaction is one a customer regularly undertakes. This could have far-reaching implications to merchant acquiring operations, with higher rates of basket abandonment as a result.

While some element of friction is necessary in financial security procedures, banks need to find a smart "friction-right" solution if they're going to keep customers happy, as well as secure.

3 Explore Exemptions

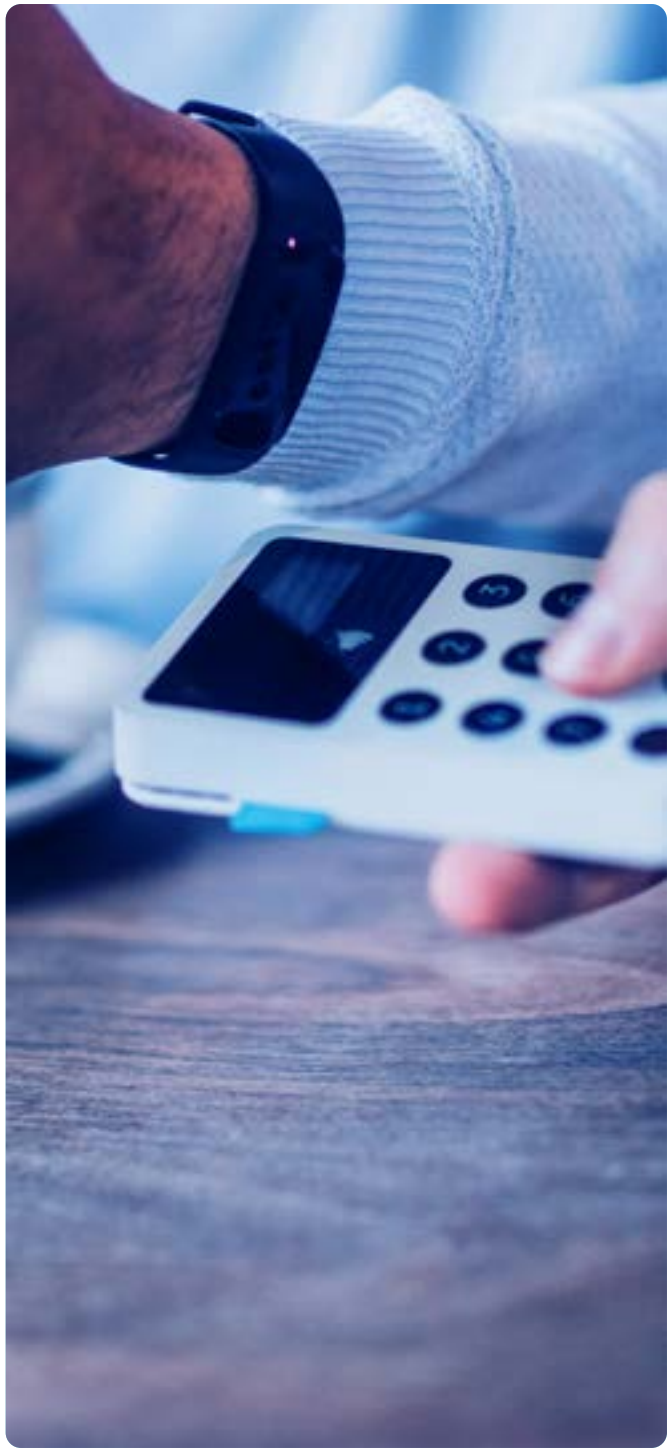
ONE WAY OF KEEPING CUSTOMERS HAPPY AS WELL AS SECURE IS BY EXPLORING THE POSSIBILITIES OF EXEMPTIONS.

Although banks all need to implement SCA as part of their PSD2 compliance, there are some circumstances in which exemptions can apply — and these can be utilized to reduce friction for consumers to an appropriate level.

Most of the time, it's possible to judge the validity of a transaction by exploring the contextual clues around it. If it's a low-value contactless payment at a coffee shop in an area the individual regularly frequents, the chances are it's legitimate, even if it is the tenth contactless transaction in a row. Likewise, a recurring payment for a weekly train ticket to the same location, from a previously used mobile device, is unlikely to be fraud.

Banks need not apply static rules if they can understand the context for that individual customer: there should not be limits on the number of genuine contactless transactions in a chain, or a requirement for a physical token-generating device for an instant payment to a known beneficiary. By applying these sorts of insights for exemptions, banks can significantly improve the customer experience even with the introduction of SCA.

Doing this successfully demands a capacity for real-time decision making. Banks need to be able to make a decision on whether or not a transaction should be exempt within milliseconds, or risk disrupting the customer experience even further.



4 Embrace Technology

MANY ARE UNDERSTANDABLY NERVOUS ABOUT ACHIEVING THE ABILITY TO APPLY EXEMPTIONS, AS IT REQUIRES A SOPHISTICATED SOLUTION THAT CAN ANALYZE ALL OF THE NECESSARY DATA POINTS IN THE BLINK OF AN EYE.

Fortunately, an appropriate technology — such as the **ACI® Fraud Management™ solution** — can integrate with access control servers to provide real-time decision making and thus help banks successfully navigate the challenges of SCA. ACI Fraud Management can also integrate with the payments gateway, which empowers merchants to implement exemptions, too.

By assessing a customer's movement patterns, transaction history and other essential data points from systems across the bank's own environment, ACI Fraud Management can accurately assess what a trusted merchant will look like for that individual, providing increased friction when a transaction flags as suspicious to keep customers secure. This transaction risk analysis will provide the right and appropriate amount of security, limiting unnecessary damage to the customer experience and promoting consumer spending. This sort of solution can also be deployed without an extensive implementation.

5 Consider Customer Communication

EMBRACING TOP-OF-THE-RANGE EXEMPTION TECHNOLOGY IS ONE THING, AND YOUR CUSTOMERS WILL CERTAINLY BE DELIGHTED IF YOU'RE ABLE TO PROVIDE A FRICTIONAPPROPRIATE EXPERIENCE WHILE KEEPING THEIR DATA AND ACCOUNTS SECURE.

Yet the reality is, their customer experience will change — and if they suddenly need to provide authentication on a previously frictionless transaction, they'll be confused and likely frustrated.

So, along with implementing the right technology, you also need to communicate effectively and ensure your customers are up to date with what's happening and what it means for their transactions. First off, banks must ensure that customer details — including mobile phone numbers and the best channel for contact — are up to date. Banks must also offer customers the opportunity to be involved in decision making, whether that's proactively identifying trusted beneficiaries or identifying their preferred method for SCA.

You should also lay out a clear position around the security benefits of SCA — and remember to avoid jargon, too. All too often, financial institutions speak in the language of their world, which often includes phrases or acronyms that aren't widely understood. Strive to speak to customers on their terms and you'll be able use the implementation of PSD2 as an opportunity to build trust and engender brand loyalty.

Achieve SCA Compliance with Confidence

MANDATES COMPLIANCE IS AN UNAVOIDABLE COST CENTER, BUT BY STRIVING TO GO ABOVE AND BEYOND, ORGANIZATIONS CAN CREATE VALUE IN REGULATORY SPEND.

Robust preparation for incoming directives will undoubtedly benefit you in the future, even as regulations change. Plus, you'll quickly reap the customer experience benefits of implementing SCA in a more intelligent way — and it doesn't have to be as complicated as you might think, because solutions already exist to serve this very purpose.

ACI Fraud Management is a best-in-class technology that provides end-to-end visibility across transactions, detecting issues as they occur and thus blocking fraud before it happens. Meanwhile, ACI has the experience and the expertise to deliver PSD2 solutions, helping you to ensure compliance, enhance security and provide great customer service with the appropriate level of friction. Combined, this can help you to achieve the mandates of SCA and PSD2 ahead of the deadline — improving security, enhancing customer service and preparing your organization for the future of compliance.

Interested in finding our more about thriving under PSD2?

Visit Our ACI Fraud Management Solution Page

ACI Worldwide
Real-Time Payments

ACI Worldwide is a global software company that provides mission-critical real-time payment solutions to corporations. Customers use our proven, scalable and secure solutions to process and manage digital payments, enable omni-commerce payments, present and process bill payments, and manage fraud and risk. We combine our global footprint with local presence to drive the real-time digital transformation of payments and commerce.

LEARN MORE

www.aciworldwide.com

@ACI_Worldwide

contact@aciworldwide.com

Americas +1 402 390 7600
Asia Pacific +65 6334 4843
Europe, Middle East, Africa +44 (0) 1923 816393

ABR1374 07-21