The European Union’s Second Payment Services Directive (PSD2) signaled a new era of change and innovation in the financial services industry. Designed to make financial transactions more transparent, efficient and secure, the directive’s requirements help institutions satisfy increased consumer demand for smarter and more flexible banking options — without compromising security.

But as these requirements have begun to be implemented and adapted to other geographies, confusion remains. Which institutions and transactions are subject to PSD2 requirements? What’s the best way to ensure compliance with those requirements? And how can institutions use the conceptual framework that underpins PSD2 to develop more compelling products and services?

In this guide, we’ll explain how PSD2 is shaping Open Banking standards around the world — and how its principles can help banks and financial services providers drive trust and enhance customer experience throughout the banking journey.

More specifically, it showcases:
- The decoding of names, terms and acronyms
- PSD2 and Open Banking in comparison
- PSD2 essential principles and requirements:
  - What it is
  - Why it’s important
  - How it’s playing around the world
- Specific requirements to consider
- What it means for banks and financial services providers
How PSD2 Has Shaped Open Banking Standards Around the World

PSD2 was released in 2015 in the European Union with the goal of increasing innovation and enhancing payment security. An ambitious piece of legislation, it entered into force in 2018, though the European Commission set and extended the deadline for PSD2 compliance a number of times.

PSD2 is now in full force for all institutions that do business with Europe. It also forms the basis of similar regulatory efforts in other areas of the world, and it remains the best reference for organizations who are trying to build payment systems that are flexible, secure and user-friendly.

As the world moves towards Open Banking standards that facilitate not just payments but broader financial data sharing, PSD2 principles can help institutions develop more robust, compelling products and services — and shift their focus from ensuring compliance to creating competitive advantage.

**DECODING NAMES AND ACRONYMS**

PSD2 aims to bring customers more personalization, choice and control. It also introduced a number of terms that are still routinely confused in the market.

**Application Programming Interface (API):** Codes and protocols that facilitate the fast, secure exchange of financial data between institutions and applications.

**Common Secure Communication (CSC):** A PSD2 requirement that seeks to secure and standardize communication between banks and financial services providers. Technical standards for CSC were defined by the Regulatory Technical Standards (RTS) that were released in 2018.

**Open Banking:** A concept that was defined before PSD2, Open Banking refers to the idea that financial data should be stored in a format that’s both secure and standardized through the use of open APIs that enable fintech providers to build better applications that can share more easily between authorized institutions and give customers a clearer and more comprehensive view of their finances.

**PSD2:** The European legislation that evolved from an earlier regulation, PSD1, and pioneered concepts related to increasing the security of financial transactions and promoting competition and innovation in the market. Many regions referred to it when creating their own payment directives as part of their Open Banking guidelines, but interpretations — and implementations — vary.

**Regulatory Technical Standards (RTS):** Detailed technical standards that underpin PSD2’s security requirements for authenticating financial transactions and communicating with other institutions. They also regulate the access that financial service providers have to customer account information.

**Strong Customer Authentication (SCA):** A PSD2 requirement that aims to increase security by calling for customers to use multi-factor authentication (MFA) whenever they access account information or make a payment. Technical standards for SCA were defined...
Third Party Providers (TPP): Organizations that rely on banks' data to propose new customer-centric solutions to the market. PSD2 distinguishes between two types of TPPs:

• **Account Information Service Providers (AISP):** Organizations that consumers can authorize to access and display information from their bank accounts — enabling them to aggregate information from multiple sources.

• **Payment Initiation Service Providers (PISP):** Organizations that consumers can authorize to initiate payment on their behalf without having to visit their bank's own portal — offering more flexibility and control.

UNDERSTANDING WHAT’S AT STAKE

PSD2 has and will continue to have a deep impact on the banking ecosystem. By ensuring that transactions are both secure and customer centric, it provides a crucial framework for accelerating trust and responding to growing demand for more customized, convenient financial services.

So it’s no surprise that PSD2 has been adopted as a guide by global regulators. Though different trends have influenced the development of secure payment and Open Banking initiatives around the world, the fundamentals are similar. Communication must be open. Innovation must be encouraged, but not at the expense of security. Customers must remain in control of their own financial data.

In the next section, we’ll unpack these concepts and principles — and explain how banks and financial services providers can leverage them to build more innovative, secure products and services.

PSD2 ≠ OPEN BANKING!

While some regions combine both PSD2 and Open Banking standards under their Open Banking umbrella, it is important to understand their respective purpose and realize that they are not one and the same. Both aim to put customers in control of their financial data — and enable them to authorize other organizations to access that data.

But PSD2 regulates security measures for the transfer of customer data for financial transactions or payments between specific institutions — AISP and PISP. Open Banking standards, by contrast, grant access to a broad range of third parties, and were designed not to streamline financial transactions but promote competition between banks and Fintech newcomers through common APIs.

Geographically, PSD2 is relevant to every organization that does business with Europe — not just those who are located in the region.
The Principles of Secure Payment Transactions

PSD2 requirements are designed to increase security, protect consumers and foster innovation and competition. In this section, we’ll review six essential principles introduced by PSD2 for securing financial transactions.

**USE STRONG CUSTOMER AUTHENTICATION (SCA)**

**What it is:** A requirement that consumers use multi-factor authentication (MFA) whenever they access account information or make a payment. SCA is one of PSD2’s core — and best-known — principles.

**Why it’s important:** Banks must be able to verify that people are who they claim to be. SCA protects account entry points, providing a first line of defense against fraudulent transactions without overburdening customers.

**What it means for banks and financial services providers:** The financial ecosystem is driven by trust. SCA helps banks and financial services providers extend this trust to new services, empowering people to adopt them.

**How it’s playing out around the world:** The Monetary Authority of Singapore (MAS) and Association of Banks in Singapore (ABS) have been especially proactive when it comes to payment security regulation, articulating standards and technical guidelines about authentication, identification and consent. India, Australia, Turkey, El Salvador and Mexico have also adopted — or are actively considering — SCA, and organizations in other regions should be prepared for the possibility that they, too, will be required to use SCA in the future. Even in the U.S., where industry initiatives, not regulatory directives, are driving developments, SCA is widely expected to be a question of “when, not if.”

---

### Specific Requirements

SCA comes into effect whenever customers access their account information online (whether by laptop or mobile device) or make a payment.

It requires people to use at least two of the following to confirm their identities:

- Knowledge based or something they know, like a PIN or a password
- Possession or something they have, like a card or a mobile app that generates a one-time password
- Inherence or something they are, like behavior biometrics or bio markers such as fingerprints or faces
MONITOR TRANSACTIONS FOR FRAUD AND MALWARE

What it is: PSD2 requires institutions to implement transaction monitoring mechanisms to analyze financial transactions in real time and detect unauthorized or fraudulent activity.

Why it’s important: As banking systems grow more open, it becomes easier for customers to share account information and initiate transactions. It also gives fraudsters more opportunities to interfere. Transaction monitoring tools help institutions detect fraud and malware while remaining invisible to customers.

What it means for banks and financial services providers: Transaction monitoring tools must be capable of spotting threats that range from stolen credentials to compromised devices. Fortunately, automated processes power more dynamic assessment, combining multiple solutions to combat the ever-changing threat landscape.

How it’s playing out around the world: For decades, the banking industry has relied on rules-based Anti-Money Laundering (AML) systems to spot potential fraud. Transaction monitoring enables institutions to be more proactive, identifying threats earlier in the banking journey and taking more effective action on both known and unknown threats. As bank fraud continues to rise, some governments are developing detailed technical regulations aimed at strengthening transaction monitoring. The Philippine Central Bank, for example, issued new rules in March 2022 that require banks to implement “automated and real-time fraud monitoring and detection systems.”

Specific Requirements

Transaction monitoring tools must be capable of spotting:

- Whether any authentication elements have been compromised or stolen
- Known fraud scenarios
- Signs of malware in the device that’s used for authentication
- Deviations from typical payment amounts
- Deviations from typical use of the device
EVALUATE TRANSACTIONAL RISKS

What it is: A requirement that institutions analyze the risk of all financial transactions — and use the information to streamline authentication and improve fraud detection.

Why it’s important: PSD2 balances security with ease of use by requiring that customers use SCA when executing all but the lowest risk transactions. Of course, you can’t manage what you don’t measure. That’s why PSD2 obliges institutions to incorporate transaction risk assessment (TRA) into their authentication systems.

What it means for banks and financial services providers: Institutions must leverage statistical data on fraud rates — and additional factors like spending and behavioral patterns — to flag high-risk transactions and set processes for taking action. Robust risk management solutions make this process easier, using statistical methods to spot patterns and enabling institutions to set a customizable threshold for transactions.

How it’s playing out around the world: Throughout much of Asia-Pacific and Latin America, TRA has been incorporated into Open Banking and SCA regulations. In India, by contrast, the need for SCA is linked to transaction amounts, not risk levels.

Specific Requirements

Transactional risks must be evaluated against:

- Abnormal spending or behavioral patterns
- Unusual account access patterns
- Signs of malware infection
- Known fraud scenarios
- Abnormal or high-risk geographical locations
LINK AUTHENTICATION CODES TO TRANSACTIONS

What it is: PSD2’s dynamic linking rule requires institutions to generate and send customers a unique authentication code when they initiate a financial transaction. This code links the transaction to its amount and intended recipient, and if it — or any payment details — are changed, the transaction should fail.

Why it’s important: Hackers often attempt to intercept authentication codes in order to authorize fraudulent transactions. If dynamic linking is applied, this type of attack won’t succeed, because the authentication code will automatically fail if any of the transaction details have been altered. By requiring transaction details to be displayed clearly at the time of authentication, dynamic linking also reduces the chances that the victims of compromised credentials will approve fraudulent transactions.

What it means for banks and financial services providers: The details of dynamic linking can seem arcane and overly technical. Yet the goal of increasing transparency is core to the Payment Services Directive 2 — and that’s exactly what dynamic linking facilitates on a transaction-by-transaction basis.

How it’s playing out around the world: Many banks outside the UK have already adopted this. For example, European banks are setting the example for ensuring payment transactions are built on integrity and trust by adopting SCA compliance. They are ensuring that dynamic linking becomes embedded inside the security framework which enhances two-step verification process. Essentially the payer must be made aware of the amount of payment transaction and of the payee. The key concept with dynamic linking is ‘what you see is what you sign’ in this regard are transactions should be transparent and tamper-proof.

Specific Requirements

Dynamic Linking operates according to the following principles:

- Customers must be aware of any online transactions they authenticate (this requirement is sometimes referred to as the What You See Is What You Sign, or WYSIWYS, principle)
- Each authentication code must be unique — and tied to the specific financial transaction that the customer initiated
- Each transaction’s authentication code and payment details must match the original transaction in order to be valid
SAFEGUARD SENSITIVE CUSTOMER DATA

What it is: PSD2 includes several requirements designed to ensure the confidentiality of customer credentials. Other global regulations have extended these principles to address broader concerns about data privacy.

Why it’s important: Customer credentials are very personal — especially biometric markers, which are unique to each individual. Exposing this information to malicious actors not only puts financial accounts at risk, but may even threaten people’s physical security. Across industries, consumers are holding organizations responsible for compromised credentials and indeed all personally identifiable information (PII).

What it means for banks and financial services providers: Data security is just as important as account security when it comes to transaction signing. PSD2 requires institutions to mitigate the risk that customer credentials will be compromised or exposed to unauthorized parties. This task requires careful thought about context and convenience; 15-character passwords may be more secure than a four-digit PIN, but they are also harder for people to remember, let alone enter into a mobile phone.

How it’s playing out around the world: In Europe, data privacy is covered by the groundbreaking 2016 General Data Protection Regulation (GDPR). GDPR extends the concept of “explicit consent” — also covered by PSD2 — and requires institutions to make sure consumers understand and agree to the way their personal data are used. GDPR has inspired similar laws in Canada, several U.S. states and countries from Brazil to South Korea. Australia, meanwhile, is incorporating its data privacy policies into the foundations of its Open Banking legislation to ensure the safe and secure transfer of consumer data.

Specific Requirements

The act of processing personal data is at the heart of financial services. But given how regulations are evolving around the world, institutions must hold themselves responsible for obtaining clear consent to use customer data — not just for financial transactions but for marketing and service improvements. What’s more, they can expect data privacy issues to have a transformative impact on service structure in the future, particularly when it comes to data sharing and portability.
PROTECT SYSTEMS AGAINST BREACHED CREDENTIALS

What it is: SCA — a core requirement of PSD2 — obliges customers to use multiple different factors to confirm their identities. However, institutions must ensure that the breach of any one of these factors does not compromise the others. This rule is also known as independence of the elements or factor independence.

Why it’s important: Data breaches have become commonplace, and organizations are starting to recognize that it’s no longer a question of whether sensitive information will be compromised, but when. Maintaining the independence of authentication elements mitigates risk and safeguards customer data.

What it means for banks and financial services providers: Ensuring factor independence requires authentication solutions that are technically more complex than the SMS verification codes on which banks and financial services providers still rely. Solution providers are exploring a range of technologies to meet these requirements — but institutions must commit to implementing them.

How it’s playing out around the world: PSD2 does not expressly forbid the use of SMS messages containing an authentication code, one-time-passwords (OTP) or payment details. It does, however, require institutions to “take all necessary security measures to ensure the confidentiality, authenticity and integrity” of any authentication codes transmitted via SMS. In countries like the U.S., banks and financial services providers continue to rely on SMS authentication in spite of its many vulnerabilities. Singapore’s monetary authority, by contrast, announced in January of 2022 that it will review the use of SMS authentication codes in an attempt to bolster the security of the digital banking ecosystem.

Specific Requirements

PSD2 requires providers to maintain factor independence by:

• Maintaining separate secure execution environments through the software they install on customer devices

• Incorporating mechanisms to ensure that the software or device has not been altered

• Incorporating mechanisms to mitigate the consequences of any alterations that are detected
FROM COMPLIANCE TO COMPETITIVE ADVANTAGE

PSD2 is an ambitious attempt to foster innovation and security, and few organizations can boast complete compliance with it — or with the many regulations that it’s inspired around the world.

Fortunately, there are also commercial imperatives for building more flexible, trustworthy financial services. The organizations that succeed in this new landscape find ways to incorporate security into a compelling consumer experience. That way, customers don’t try to circumvent the protections or, worse yet, abandon their transactions.

Take Transaction Security to the Next Level:

- Visit our fraud prevention information hub
- Visit our Open Banking information hub
- Book time with one of our payment security specialists to discuss your business needs.