Hello, is it me EU’re looking for? The new era of payment authorization in Europe

16 December 2019
By:

Return to Law à la Mode: Issue 29

Retailers in the EU who take online or card-based payments from customers will be affected by the EU’s Second Payment Services Directive (PSD2), which was issued in 2015 and the subsequent implementing rules in member states. In the UK those implementing rules are the Payment Services Regulations 2017 (PSRs).

PSD2 introduced some significant changes in the way that the payments industry, and those providing payment related services, are regulated. It also introduced new rules designed to accommodate and encourage emerging trends in the payments space – such as the advent of open banking and new and alternative ways that payments can be made and financial and payments information can be shared.

Included in those rules are requirements (and associated technical standards) relating to how the identity of individuals who wish to make a payment, or enable the exchange of financial information, is to be checked and confirmed.

Strong customer authentication

Strong Customer Authentication (SCA) is the key concept in the new rules relating to identification. It mandates the use of two-factor authentication to confirm the identity of an individual. That is achieved where the individual is identified using a combination of any two of the following three factors:

- something they know – such as a password;
- something they have – such as an electronic device (e.g. a mobile phone); and
- something they are – such as a thumb print.

The deadline for introduction and adoption of SCA was September 14, 2019. In introducing the SCA, firms are expected by regulators to have solutions to fit all customer groups – on the basis that, for example, older customers may not have mobile phones with thumbprint scanners.

Subject to some exemptions, the requirement for SCA to be used would apply when a payer:

- initiates an e-payment transaction;
- accesses a payment account online; or
- carries out any action remotely which may imply a risk of fraud.

Wait, wait, we’re not ready

Concerns about the scale of change required across multiple industries to be ready to comply with the new rules, and the level of awareness of businesses and customers, led to calls for the deadline to introduce SCA to be delayed.

In June 2019, the European Banking Authority (EBA), the agency tasked with overseeing the adoption of the new rules across Europe, published an opinion stating that there was a need to delay the implementation of the new rules beyond September 14, 2019. In August 2019, the UK Financial Conduct Authority (FCA) went further and announced a scheme for delaying the implementation of the new rules (regulators in other EU Member States such as Ireland made similar moves). More recently, in October 2019, the EBA published an opinion setting out its scheme for delaying introduction.

The FCA delay

For e-commerce transactions, the Financial Conduct Authority has agreed to give an 18-month adjustment period. As long as authorized firms (including retailers if they are authorized) are following an industry plan set by UK Finance (the UK payments body) to roll out SCA, the Financial Conduct Authority will not take enforcement against them. Once the deadline of March 14, 2021 has passed, the Financial Conduct Authority will start to enforce against non-compliance.

The EBA delay

The EBA has set a revised deadline for the adoption of SCA in e-commerce transactions to December 31, 2020. It will be interesting to see how that plays out given that most businesses aim to freeze any major IT changes towards the end of the calendar year to deal with holidays and a spike in seasonal trading. The rules have been praised as clearer, setting milestones, and calling for a harmonized adoption across the EU.

What can you do?

An important step if you have not already implemented SCA is to follow any agreed industry plan which has been put in place to ensure compliance as soon as possible and by the relevant extension date set by the applicable regulator. Meanwhile, aim to keep compliant and to avoid fraud.

It will also be important to keep customers updated on what you are doing. A concern of many retailers is how security measures add more time and more friction to the check-out process and ultimately more risk of abandoned baskets and lost sales. It will be important to make sure that you are telling your customers what is happening.

The good news is that payment providers are working on ways to ensure compliance by merchants. Adoption of the 3D-Secure standard, in particular 3DS 2.0, should also enable compliance.

Return to Law à la Mode: Issue 29