Online payment authentication requirements further strengthened from 22 September 2020

Ms. Aylin Cebbar
Associate
aylin.cebbar@alitus.com

As part of the second European Payment Services Directive (i.e. Directive (EU) 2015/2366 of 25 November 2015 on payment services in the internal market) (PSD2), which entered into force in 2019 and replaced the Payment Services Directive (PSD), new rules have been developed to provide additional protection for customers when making electronic payments. One of the key new elements introduced by PSD2 is ‘strong customer authentication’, which should further increase consumer confidence in marketplaces and webshops.

‘Strong Customer Authentication’ (SCA): What’s that?

Payment service providers (including banks and other payment institutions) must from now on observe stricter security measures when they process payments or provide payment-related services.

To better protect consumers when they make electronic transactions or payments, both online and in physical shops, electronic payments must be performed with multi-factor authentication.

This means that to prove their identity, users have to provide at least two of the following three elements:

- something they know (e.g. a password or PIN code);
- something they own (e.g. a card or mobile phone); and
- something they are (biometrics, e.g. fingerprint or iris/face scan).

This ‘strong customer authentication’ (SCA) rule must also be applied when consumers access or use their online banking or payment account.

By introducing higher security standards, the European legislator wants to increase consumer

trust and confidence in online payments and thus foster the development of e-commerce.

Exemptions to SCA

There are, however, a number of exceptions to the application of these enhanced security requirements. Contactless payments in physical shops, online transactions for small amounts, payments in car parks and at tolls or transfers to “trusted” beneficiaries are among the transactions that do not need to be subject to such authentication.

Transitional period – Key dates to keep in mind

Strong customer authentication will be gradually introduced throughout the EU, to allow payment service providers sufficient time to adapt their security systems to the increased security requirements defined in the Directive.

In Belgium, progressive planning to allow such a transition, has been planned by the Belgian banks, in agreement with the National Bank of Belgium.

Currently (and since 25 August 2020), SCA applies to online transactions above 1,500 EUR.

Here is an overview of the key dates on which the threshold will be reduced:

- 22 September 2020: SCA will apply to online transactions above 250 EUR;
- 19 October 2020: SCA will apply to online transactions above 30 EUR;
- 17 November 2020: SCA will apply to all online transaction transactions (the threshold will be reduced to 0 EUR).

All online transactions above these thresholds will be refused if they do not comply with the new EU rules.

What will change for consumers?

In concrete terms, it will no longer be possible for consumers to make an online payment by simply encoding their credit card number and the number on the back of the card (i.e. the CVV number). The use of a single code received by SMS will also no longer be considered sufficient to secure a transaction (except for the exemptions above).

However, the impact of the Directive on Belgian consumers must be put into perspective. Indeed, many Belgian banks and online sales websites have been applying a strong authentication procedure on a voluntary basis for online payments for years to protect consumers and thus already comply with the new legislation.

With the Directive’s entry into force, this procedure is now also used for all European payments. The main changes should therefore be more visible when consumers make online purchases (i.e.

online shopping or booking flights, for example) on non-Belgian-based e-commerce websites.

… and what about the changes for payment service providers?

As set out above, non-Belgian e-commerce market players are in general less familiar with this principle. Not only will these payment service providers have to implement and try-out new securities measures, but they will also have to be able to prove that they have put such measures in place.

In this respect, it is important to note that if a payment service provider wishes to be exempted from strong customer authentication, it will first have to apply mechanisms for monitoring transactions to assess if the risk of fraud is low.

Furthermore, if during the transitional period (set out above) a payment service provider agrees to carry out a transaction without this “strong authentication” and the consumer concerned then disputes this transaction because he/she was the victim of online payment fraud, the provider will be liable for the loss and have to fully reimburse the consumer (unless it can prove that the consumer was grossly negligent). Hence the importance for payment service providers to ensure, without any further delay, prompt compliance with the new legislation.