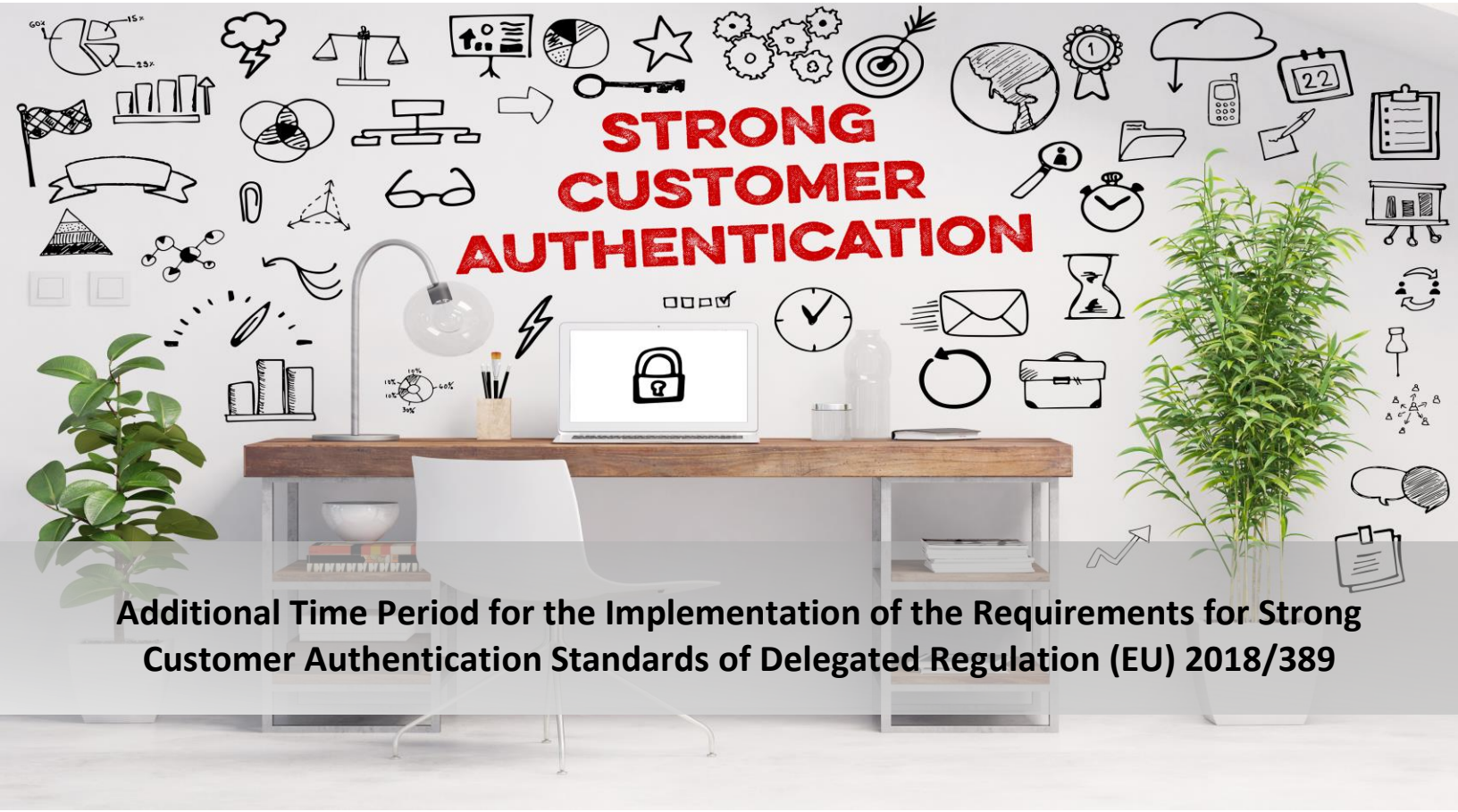

Additional Time Period for the Implementation of the Requirements for Strong Customer Authentication Standards of Delegated Regulation (EU) 2018/389

By its Announcement of 26.08.2019 the Bank of Greece has accepted to provide an additional time period for the implementation of Regulatory Technical Standards [1] adopted by the EU Commission that set out the specific requirements of compliance with the new obligations in PSD2, such as the requirements for Strong Customer Authentication Standards. Such extension has been provided following the EBA's Opinion as of 21.06.2019.

Background

On 25 November 2015, Directive 2015/2366 on Payment Services II (PSD II) with entry into force as of 13 January 2018. The Greek parliament transposed the Directive by adopting Law 4537/2018. PSD2 aimed to improve the framework for achieving a single market for electronic retail payments, which will enable consumers, retailers and other market players to enjoy the full benefits of the EU internal market and the digital single market particularly in terms of e-commerce. Therefore, the main target of PSD II were:

(a) to enhance competition by introducing new market players, such as third parties providing payments-related services (TPPs), such as Payment Initiation Services Providers (PISPs) and Aggregators and Account

[1] Delegated Regulation (EU) 2018/389 supplementing Directive (EU) 2015/2366 (PSD II) of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.

Information service providers (AISPs) or FinTech companies and other banks.
(b) to enhance consumer protection via strong customer authentication and secure open standards of communication.

Due to the complexity of compliance, a different date of application had been foreseen for the enhanced security measures, namely strong customer authentication (SCA) and standards for secure communication - introduced in the PSD2. This date has been set to be September 14th 2019, namely the date of the entry into force of Regulatory Technical Standards.

Strong Customer Authorization

In this context, the proposed Regulatory Technical Standards on strong customer authentication and secure communication are key to achieving the objective of the PSD2 of enhancing consumer protection, promoting innovation and improving the security of payment services across the European Union. In particular, in order to reduce the risk of fraud and to protect the confidentiality of the user's financial data and personal data, Payment service providers will be obliged to apply so-called strong customer authentication (SCA) when a payer initiates an electronic payment transaction.

Strong customer authentication is an authentication process that validates the identity of the user of a payment service or of the payment transaction (more specifically, whether the use of a payment instrument is authorised). Strong customer authentication is based on the use of two or more elements to validate the user or the transaction, i.e.
(a) knowledge (something only the user knows, e.g. a password or a PIN),
(b) possession (something only the user possesses, e.g. the card or an authentication code generating device) and

(c) inherence (something the user is, e.g. the use of a fingerprint or voice recognition).

These elements are independent in the sense that the breach of one element does not compromise the reliability of the others and are designed in such a way as to protect the confidentiality of the authentication data. For remote transactions, such as online payments, the security requirements go even further, requiring a dynamic link to the amount of the transaction and the account of the payee, to further protect the user by minimising the risks in case of mistakes or fraudulent attacks.

Exemptions

Exemptions have been defined by the European Banking Authority (EBA) and adopted by the EU Commission, taking account of the risk involved, the value of transactions and the channels used for the payment as per Implementing Regulation 389/2018 and include the following:

(a) low value payments at the point of sale (to facilitate the use of mobile and contactless payments). In particular,
(i) the individual amount of the contactless electronic payment transaction does not exceed EUR 50 and

(ii) the cumulative amount of previous contactless electronic payment transactions from the date of the last application of strong customer authentication does not exceed EUR 150 or

(iii) the number of consecutive contactless electronic payment transactions since the last application of strong customer authentication does not exceed five.

(b) low value remote (online) transactions. In particular,

(i) the amount does not exceed EUR 30 and

(ii) the cumulative amount of previous remote electronic payment transactions since the last application of SCA does not exceed EUR 100 or

(iii) the number of previous remote electronic payment transactions since the last application of strong customer authentication does not exceed five consecutive individual remote electronic payment transactions

(c) recurring transactions

(d) trusted beneficiaries

(e) unattended terminals for transport fares and parking fees

(f) credit transfers between accounts held by the same natural or legal persons

The EBA's Opinion on the elements of strong customer authentication (SCA)

In response to continued queries from market actors as to which authentication approaches the EBA considers to be compliant with SCA and in order to facilitate proper and timely implementation, on 21 June 2019, the European Banking Authority (EBA) published an Opinion on the elements of strong customer authentication (SCA) under the revised Payment Services Directive (PSD2) available at https://eba.europa.eu/documents/10180/2622242/EBA+Opinion+on+SCA+elements+under+PSD2+.pdf.

Indicatively, with regards to the *inherence element*, the Opinion provides that *"communication protocols such as EMV® 3-D Secure provide a means for merchants to support the use of SCA. The EBA notes that versions 2.0 and newer support a variety of SCA methods, while trying to ensure customer convenience, limiting fraud through data sharing and transaction risk analysis, and enable the use of exemptions set out in the RTS. For those reasons, the EBA encourages the use of such communication protocols and expedient onboarding. Older protocols such as EMV® 3-D Secure version 1.0, although supporting the use of SCA, are not fully adapted to PSD2. For instance, they do not include the possibility of using exemptions or use all forms of SCA approaches."*

With regard to the *possession element*, and following queries from stakeholders if card details and card security code that are printed on the card can constitute a could constitute a possession element the EBA is of the view that such details cannot do so. However, dynamic card security codes (where the code is not printed on the card and changes regularly)

may provide evidence of possession in line with Article 7 of the RTS.

With regard to the *Knowledge element*, the EBA is of the view that the following elements could constitute a knowledge element: a password, a PIN, knowledge-based responses to challenges or questions, a passphrase and a memorised swiping path (as opposed to keystroke dynamics, namely the manner in which the PSU types or swipes, which may be considered an inherence element).

CONTACT

For any further comment or query, do not hesitate to contact us:

Anastasia Dritsa
Partner

a.dritsa@kglawfirm.gr

Violeta Panagiotopoulou
Senior Associate

v.panagiotopoulou@kglawfirm.gr

Fenia Mylonaki
Junior Associate

f.mylonaki@kglawfirm.gr

Sofia Athanasaki
Junior Associate

s.athanasaki@kglawfirm.gr

Main (Athens) Offices
28, Dimitriou Soutsou str., 115 21, Athens, Greece, Tel: +30 210 8171500, Fax: +30 210 68 56 657/8
Thessaloniki Branch
17, Ethnikis Antistaseos str., 551 34, Thessaloniki, Greece, Tel: +302 2310 441552

www.kglawfirm.gr

Follow Us