RegCORE Client Alert

EBA clarifies the application of strong customer authentication requirements to digital wallets and ESAs publish draft Guidelines on the system for the exchange of information relevant to fit and proper assessments

March 2023

ESAs: Customer Authentication Requirements and the Exchange of Relevant Information

EBA clarifies the application of strong customer authentication requirements to digital wallets and ESAs publish draft Guidelines on the system for the exchange of information relevant to fit and proper assessments

Dr. Michael Huertas
Tel.: +49 160 973 757-60
michael.huertas
@pwc.com

Contact RegCORE Team
de_regcore@pwc.com

QuickTake

On 31 January 2023 the three European Supervisory Authorities (EBA, EIOPA and ESMA – **ESAs**) took an important step towards establishing a common ground on rules by (i) clarifying the safeguarding standards applicable to digital wallets and the requirement to apply a strong customer authentication (**SCA**) process and (ii) promoting the exchange of relevant information in the context of fit and proper assessments.

The European Banking Authority (**EBA**) published three Q&As which, together with three other Q&As previously published by the EBA, comprehensively clarify the application of SCA to digital wallets in the context of the revision of the Payment Services Directive (**PSD2**). By doing so, the EBA aims to create a common understanding of the applicable requirements among all market stakeholders to thereby improve the

safety of digital wallets.[1] This clarification, while welcome in terms of certainty, may however mean that a number of traditional financial services firms, FinTech and in particular cryptoasset services providers will need to amend their processes to comply with these supervisory expectations.

On the same day, the three ESAs have published a consultation paper on draft common rules on the information exchange system when assessing the fitness and propriety requirements (the **Guidelines**). These Guidelines aims to increase the efficiency of information exchange between sectoral supervisors by harmonising practices and clarifying how competent authorities should use the information system developed by the three ESAs. The consultation on the Guidelines is open until 2 May 2023.

EBA: Implications by the Q&As

The six Q&As clarify the application of the SCA to the registration of a payment card in a digital wallet and to the initiation of payment transactions with digitised versions of a payment card. Additionally, they clarify the requirements for outsourcing the application of the SCA to digital wallet providers.

Key takeaways from the Q&As are that (our clarifications in square brackets):

1. **the PSP issuing the payment card (the issuer) is required to apply SCA when adding a payment card to a digital wallet and is responsible for providing the respective SCA elements to the PSU. Also, the issuer is required to ensure that adequate security measures are in place to protect the confidentiality and integrity of PSU's personalised security credentials.[2]**

Overall, within the Q&As the EBA clarifies that: "[…] issuers may outsource the provision and verification of the elements of SCA to a third party (e.g. by concluding contractual arrangements with the third party), such as a digital wallet provider, in compliance with the general requirements on outsourcing, including the requirements of the EBA's guidelines on outsourcing arrangements, [as may be supplemented as a matter of national law and supervisory expectations of national competent authorities]. However, the responsibility for compliance with the SCA requirements cannot be outsourced and [therefore] issuers remain fully responsible for the compliance with the requirements in PSD2 and the Regulatory Technical Standards (**RTS**) on SCA & CSC [i.e., common and secure open standards of communication - **CSC**]."

2. **in terms of the initiation of electronic payment transactions, the initiation with the digitised version of the payment card also requires the application of SCA under Article 97(1)(b)[3] of PSD2, unless one of the specific exemptions from the application of SCA set out in the RTS on SCA & CSC applies.[4]**

Therefore, when enrolling a payment card to a digital wallet, "[…] this process leads to the creation of a token/digitised version of the payment card and requires the application of [SCA] under Article 97(1)(c) of PSD2, because it is an action that may imply the risk of fraud or other abuses. By applying SCA, the payment service provider (PSP) verifies remotely that the payment service user (PSU) is the rightful user of the payment card and associates the PSU and the digitised version of the payment card with the respective device."[5]

3. **the unlocking of a mobile device with biometrics (e.g. a fingerprint) or with a PIN/password cannot be considered a valid SCA element for the purpose of adding a payment card to a digital wallet, if the screen locking mechanism of the mobile device is not a process under the control of the issuer. Furthermore, the issuance of a new token, replacing a previously existing one, and binding it to a device/user also requires the application of SCA.[6]**

This clarification may mean that certain user interaction and thus user experiences in various app-based customer journeys may need to be adopted to reflect this change.

[1] The press release can be found here.
[2] Q&A 6141 to be found here.
[3] Article 97(1) of PSD2 states that "a payment service provider applies strong customer authentication where the payer: (a) accesses its payment account online; (b) initiates an electronic payment transaction; (c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses".
[4] Q&A 5622 to be found here.
[5] The press release can be found here.
[6] Q&A 61145 to be found here.

ESAs: The proposed common Guidelines on information exchange

As a result of the ESA's publication of proposed common Guidelines[7] on the system for the exchange of information relevant to fit and proper assessments the ESA's are moving towards a much more efficient and joined up means to conduct fit and proper assessments. National competent authorities are expected to apply these and thus drive forward supervisory convergence in the EU.

The Guidelines have been developed in accordance with principles binding upon the ESAs to jointly establish a system for the exchange of information relevant to the assessment of the fitness and propriety of holders of qualifying holdings, directors and key function holders of financial institutions by competent authorities in accordance with the legislative acts.

The ESA's have developed a system which consists of a cross-sectorial database (**ESAs Information System**). Together with these Guidelines on how to use the ESAs Information System as well as on the exchange of relevant data the ESAs aim at fostering an efficient exchange of information between competent authorities.

The flow and exchange of information relevant to the assessment of the fitness and propriety of a person of interest should work as follows:

- The ESA's Information System will hold limited information on persons who are subject to a fitness and propriety assessment under EU sectoral provisions.
- The (national) competent authorities performing such assessments will include the relevant information consistent with these Guidelines in the ESAs Information System.
- The aim of the ESAs Information System is to support (national) competent authorities identifying other competent authorities that have conducted such an assessment process for a person of interest.

At a high level, the Guidelines are divided into two main parts:[8]

1. The first part focuses on how competent authorities should input the data and use the ESAs' information system, including on how to search for the fit and proper assessments of persons of interest that had already been made by other competent authorities.

2. After having identified that a relevant assessment has been made by another competent authority, the second part of the Guidelines clarifies how these two authorities should cooperate to exchange the relevant information.

The actual exchange of information that is relevant to the assessment of the fitness and propriety of a person of interest will be made between the relevant competent authorities in line with the applicable regulatory framework outside of the ESAs Information System. Furthermore, the ESA's Information System and the Guidelines will be in compliance with the applicable data protection requirements.

While these Guidelines support the request and exchange of information between competent authorities when conducting a fitness and propriety analysis the provision of information does not release the competent authority from their obligation to make their own assessments of fitness and propriety. Each assessment needs to follow the applicable sectoral requirements and is to be considered in the context in which an assessment is made.

Outlook and next steps

The developments summarised above mark an important step towards clarifying on how to apply legislative and regulatory rulemaking instruments, standards and guidance issued in respect thereof in financial markets that are getting more digitised by the second. By giving clear answers to the raised questions, the EBA is stepping in to safeguard that SCA can be conducted properly. Subsequently, payment service providers or third parties acting on their behalf shall review their existing customer authentication systems under the light of the clarified standards and adapt them in order to comply with the EBA's standards.

Also, the ESAs seem to adapt and move towards a more digitised financial world by establishing their common information system and fostering a facilitated way of exchanging relevant information for the assessment of the fitness and propriety of a person of interest between competent authorities. It is expected that by the end of 2023 the ESAs will publish their final Guidelines on information sharing, paving the way for

[7] See here.
[8] The press release can be found here.

a joint EU digital financial framework. It also remains to be seen whether the tentative yet welcome first steps on the ESA's Information System could be applied further and beyond this initial focus.

About us

PwC Legal is assisting a number of financial services firms and market participants in forward planning for changes stemming from these developments.

If you would like to discuss any of the developments mentioned above, or how they may affect your business more generally, please contact any of our key contacts or PwC Legal's EU RegCORE Team via de_regcore@pwc.com or our website.

Dr. Michael Huertas
Tel.: +49 160 973 757-60
michael.huertas@pwc.com

www.pwclegal.de