German Banking Industry Committee

Die Deutsche Kreditwirtschaft

Comments

regarding Consultation Paper on draft regulatory technical standards amending the Commission Delegated Regulation (EU) 2018/389 supplementing Directive (EU) 2015/2366, EBA/CP/2021/32, 28 October 2021

Register of Interest Representatives
Identification number in the register: 52646912360-95

Contact: Anna Miriam Schütt
Telephone: +49 30 20225- 5368
Telefax: +49 30 20225- 5345
E-Mail: anna.miriam.schuett@dsgv.de

Berlin, November 25, 2021

The **German Banking Industry Committee** is the joint committee operated by the central associations of the German banking industry. These associations are the Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR), for the cooperative banks, the Bundesverband deutscher Banken (BdB), for the private commercial banks, the Bundesverband Öffentlicher Banken Deutschlands (VÖB), for the public-sector banks, the Deutscher Sparkassen- und Giroverband (DSGV), for the savings banks finance group, and the Verband deutscher Pfandbriefbanken (vdp), for the Pfandbrief banks. Collectively, they represent more than 1,700 banks.

Coordinator:
German Savings Banks Association
Charlottenstraße 47 | 10117 Berlin | Germany
Telephone: +49 30 20225-0
Telefax: +49 30 20225-250
www.die-dk.de

I. General remarks

Principle of risk management by the ASPSP could be weakened

Article 1 Delegated Regulation (EU) 2018/389 (RTS)[1] states that the regulation establishes the requirements to be complied with by **payment service providers** for the purpose of implementing security measures which enable them to apply the procedure of strong customer authentication (SCA) in accordance with Article 97 of Directive (EU) 2015/2366 (PSD2)[2] and exempt the application of the security requirements of strong customer authentication, subject to specified and limited conditions inter alia based on the level of risk. Therefore, the decision to exempt the requirement of strong customer authentication – within the limits of the regulation – is solely based on the risk-assessment of the account servicing payment service providers (ASPSPs). The proposed mandatory exemption is in contradiction to Article 1 Delegated Regulation (EU) 2018/389.

Erosion of the PSD2 security concept

One of the major goals of PSD2 was to improve the security of online banking. Further calibrations of already existing exemptions or possible new exemptions should not erode this principle. The suggested changes might set in motion a spiral for the erosion of this principle at the disadvantage of both payment service users (PSUs) and the trust in the entire system.

Holistic approach needed

The suggested changes of the Delegated Regulation (EU) 2018/389 touch upon basic principles of the PSD2. They address only particular interests of a certain group of PSPs, while at the same time preventing a holistic approach reflecting all market experiences (e.g. distinct business needs of corporate clients). Hence, the aspects as proposed by EBA should be discussed at the upcoming review of the PSD2 to ensure a coherent approach reflecting the interests of all parties involved (PSUs and PSPs).

II. Specific comments

Q1. Do you have any comments on the proposal to introduce a new mandatory exemption for the case when the information is accessed through an AISP and the proposed amendments to Article 10 exemption?

- We strongly support that the EBA foreclosed the initially discussed approaches proposed by some market participants. In particular the delegation of SCA to account information service providers (AISPs) and the requirement of SCA only for the first time the user connects through the AISP (para 16 and 17 of the Consultation Paper). The obligation and responsibility to perform SCA lies solely on the ASPSP (see Article 97 PSD2) and it

[1] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 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.
[2] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (PSD2).

is the ASPSP that issues the personalised security credentials. Therefore the ASPSP cannot rely on the AISPs to conduct SCA on the ASPSP's behalf (para 19, 22). We welcome that EBA gives clear guidance in that matter and confirms the unambiguous responsibility of ASPSP as laid down in PSD2.

- A mandatory exemption to SCA as suggested in section 3.2.2 would significantly violate the principle of equivalence of treatment. ASPSPs would be prevented from the application of SCA when PSUs access through AISPs although many ASPSPs require SCA every time the PSUs is accessing their account information directly, thereby curtailing PSD2-mandated decisions based on security considerations and product designs. ASPSPs are hindered in their own risk assessment to provide a higher level of security.

- In case that ASPSPs have decided to apply SCA every time the user accesses his account directly it has to be taken into account that fraudsters will be able to undermine the security barriers of ASPSPs by using AISPs for getting access to user accounts. In case of special exemptions from this rule for AISP fraudsters could undermine the security policy of ASPSPs. So the proposed amendment would have serious impact on the security considerations of ASPSPs.

- EBA claims that ASPSPs failed to provide user-friendly SCA methods so that the application of SCA in most cases causes friction in the customer journey. This is however unsubstantiated for the German market: even before 2016 ASPSPs progressed their digital services and constantly explored and developed convenient and secure SCA methods for their customers thereby making use of biometry and possession elements as proposed in the Delegated Regulation (EU) 2018/389 rather than solely relying on knowledge factors like static passwords or authentication codes that have to be typed in by the user. Many ASPSP solutions meanwhile conveniently perform a full SCA with 2-factors by clicking a single button on a smartphone from a user's perspective. For access to corporate payment accounts, some ASPSPs even fully switched to 2-factor-solutions only. Thus, technically eliminating the possibility of the exemption for their customers and thereby retaining the highest possible level of security.

- The mandatory exemption when the PSU access through an AISP may lead to even more conflicting situations and irritations on the PSUs level since this leads to different experiences regarding the application of SCA if the PSU is accessing his account directly: The less PSUs understand whether they are expected to provide SCA (or not), the more vulnerable they are to both phishing and social engineering attacks. A consistent SCA scheme maintained by an ASPSP - whether an account is accessed directly or through a TPP - strengthens the PSU's security.

- If introduced, the mandatory exemption should only be applied when the ASPSP also offers this exemption in the direct customer interface which would be in line with Article 67(3)(b) of Directive (EU) 2015/2366 i.e. that the ASPSP should treat AISP without any discrimination.

Q2. Do you have any comments on the proposal to extend the timeline for the renewal of SCA to 180-days?

- As of today, we do not see any need for the extension of the timeline for SCA renewal. Member banks of our associations have not reported the current 90-day period to be any obstacle for product offerings or a reason for customer complaints. As mentioned above, many banks do not even make use of the 90-days exemption period when clients access their account directly.

- The prolongation jeopardises the ideas of Open Banking, which should achieve equal benefit of all market participants. The 90 days are already a heavily discussed compromise. Originally 30 days were suggested. We regard today's exemptions of the PSD2 as the frame for market driven Open Banking activities not as free of charge examples. ASPSPs need to invest some amounts that these exemptions can be used in practice. Moreover, all market participants can make use of these exemptions in the OpenFinance API standardisation as they are ongoing e.g. within the Berlin Group Initiative. No market failure can be identified here. Market participants agree the conditions among themselves. Therefore, every unbalanced regulatory expansion of services for one market side could hamper successful digital ecosystems to emerge.

- A further extension to 180 days could have the potential to reduce PSUs' sovereignty over their data and increase risks: The renewal of SCAs acts as both a security mechanism as well as a warning and information function. A period of 6 months without renewal of SCA or direct action of the PSU for third party data retrieval does not meet these requirements and will be at the disadvantage of PSUs. It could lead to a greater loss of confidence to the detriment of all market players.

- We strongly suggest that any extension should only be reconsidered in a few years' time, once PSPs, PSUs and authorities have gained more experience with customer needs, security concerns and related data protection aspects to evaluate all impacts thoroughly.

- We suggest also to consider the on-going assessment of data sharing principles and not precluding any conclusions before an agreement on an EU framework for Data Governance as well as for Open Finance is concluded.

Q3. Do you have any comments on the proposed 6-month implementation timeline, and the requirement for ASPSPs to make available the relevant changes to the technical specifications of their interfaces not less than one month before such changes are required to be implemented?

- EBA suggests a 6-month implementation timeline and informs that the amendments are estimated to take effect from Q4 2022 onwards. This planning does not take into account that many ASPSPs have already fixed their implementation plans for the upcoming year, making it in most cases impossible to accommodate additional requirements. Therefore, a minimum implementation period of 12 months after the adoption of any revised regulation is essential.

- Furthermore, clear transitional rules are required: SCA-based consents given prior to the application of amended regulations may stay valid under the regulations then in effect until the PSU gives a new consent under the new regulations.