Consequences of the SCA-requirement for E-Money

Preamble

The following statements are based on the Final Report "Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2)" published by the EBA on 23 February 2017. Pages references refer to this document.

Initial statements

1. According to Article 97 (1) PSD2 Member States shall ensure that the payment service provider (PSP) applies SCA (Strong Customer Authentication) where the payer initiates an electronic payment transaction. Electronic payments could be card-based proximity transactions a physical POS or remote transactions like online payments via the internet or contactless POS-payments according to Article 4 (6).[1] SCA also plays a vital role in the liability regime established by Articles 72, 73, and 74.

2. Electronic payment transactions include e-money transactions (p. 7). Like other electronic payment transactions, e-money transactions could be card-based (e.g. prepaid cards linked to an e-money account or cards on which e-money can be stored directly) or account-based without access through a card.[2]

3. According to the Fourth AML-Directive (2015/849/EU, 4AMLD) low-risk (regarding AML and terrorist financing) e-money based payment instruments (reloadable and non-reloadable) can be issued without identification of the holder, if specific requirements (e.g. transaction monitoring) and thresholds are fulfilled (CDD exemption under Article12 4AMLD). In these cases, the holder of the product may remain anonymous.

4. PSD2 makes several derogations for anonymous low value prepaid products. Indeed, Article 63 provides that: "*1. In the case of payment instruments which … store funds which do not exceed EUR 150 at any time, payment service providers may agree with their payment service users that … (b) Articles 72 and 73, and Article 74(1) and (3), do not apply if the payment instrument is used anonymously…"* This means that, under the circumstances mentioned, the issuers are not required to prove

[1] *Remote payment transaction' means a payment transaction initiated via internet or through a device that can be used for distance communication* (Art. 4 (6) PSD2).

[2] According to the EBA „credit transfers include e-money transfers" (p. 7). We assume that this classification is only relevant for non-card based e-money transactions. Both categories are subject to the SCA-requirement, however, the distinction could have relevance for the reference fraud rates of the exemption "Transaction Risk Analysis" (TRA) according to Article 16.

transactions are authenticated (under article 72) or assume the usual liability for unauthorised transactions (under articles 73, 74(1) and (3)) for anonymous payment instruments with a maximum €150 balance.

5. If e-money is issued anonymously, an authentication defined as “a procedure that allows the PSP to verify a customer´s identity” (p. 48) is strictly speaking impossible, because the e-money user has not been identified by the issuer. The legitimacy of making an electronic payment is only based on possession (e.g. card) and/or knowledge (code).

6. Most gift cards, which are not issued in a strictly closed-loop environment, are regulated as e-money. Payments are initiated by these (usually non-personalized and transferable) cards without PIN-usage. The e-money which is stored on the card (chip or magnetic stripe) is used for electronic payments without PIN as well. PIN-based authorization would be a superfluous element regarding the low risk (usually low-value payments) and the convenience for the user (e.g. transferability of gift cards). The online payment with e-vouchers is made by entering a code, known by the user. Payments with anonymous e-money payment instruments are usually based on a “one-factor” authentication (card possession or knowledge of a code).

Consequences for e-money

7. While PSD2 explicitly foresees use cases for anonymous low-value prepaid products and provides for a specific regime to cover their specific setup, the RTS on SCA seem to overlook these products. We appreciated that, in the eyes of the European legislator, these products were not supposed to lie within the scope of the SCA requirements. However, the very generic wording in the RTS creates a level of legal certainty which might lead to serious negative consequences for a flourishing prepaid market.

8. Article 21 of the RTS clearly anticipates that the payment service user’s identity is to be associated with the personalised security credentials, authentication devices and software. Such an association will not allow the payment instrument to be used anonymously and so the RTS is in direct conflict with the PSD and the 4AMLD, which provide an exemption for anonymous e-money products.

9. Article 4 of the RTS requires the generation of an authentication code based on two or more factors. This logically requires the identification of the customer in some form and would not allow for anonymous products, in contradiction to the clear wording of Article 63 PSD2.

10. The generation of a dynamic PIN or one-time password, as required in Article 5 of the RTS for **remote transactions** with e-money products, is logically always a process separated from the e-money issuance. The dynamic linking can only be realized by at least a simplified due diligence (e.g. registration of the mobile number of the user).

The EBA requirement of dynamic linking for remote e-money transactions cannot be realized for all e-money products issued anonymous in compliance with the 4AMLD and the PSD2.

11. **Non-remote electronic card-based payment transactions** SCA in accordance with the EBA requirements (Article 4) can actually only be realized by a chip card & PIN-solution as provided by at least EMV chip standard with level DDA[3] or higher (see p. 143). Magnetic stripe cards are not compliant. Most of the card based e-money products (except the prepaid cards, issued with brands of the international card schemes) are not based on EMV DDA chip card technology. These cards will not be compliant with the SCA requirements.

12. The current non-compliance with SCA of many e-money electronic payment transactions is immanent to the specific product features (e.g. anonymity or no-PIN-usage) of the payment instrument involved. After issuance of the payment instrument, the issuer or acquirer cannot apply SCA for specific transactions generated by this instrument (e.g. after an increase of fraud). According to Article 18 (5) the PSP should always be able to apply SCA by using any of the exemptions set out in Article 10-16. These exemptions have therefore no relevance for PSP regarding e-money products which are based on one factor authentication.

Proposed solution

It is critical that anonymous e-money electronic transactions are explicitly outside the scope of the SCA RTS. We therefore strongly suggest that the RTS add anonymously issued e-money payment instruments in accordance with the 4AMLD or other anonymously issued payment instruments to the list of exemptions or to clarify that these instruments are clearly outside the scope of the PSD2.

Modification proposed by PVD

Recital 8 (p. 15)
Exemptions based on low-value contactless payments, which also take into account a maximum number of consecutive transactions or a certain fixed maximum value of consecutive transactions without SCA, allow the development of user friendly and low risk payment services and should be included in these technical standards. It is also appropriate to establish an exemption for the case of electronic payment transactions initiated at unattended terminals where the use of strong customer authentication may not always be desirable due to operational reasons (e.g. to avoid queues and potential accidents at toll gates) or safety or security risks (for instance the risk of shoulder surfing). Actions which imply access to the balance and the recent transactions of a payment account without

[3] DDA: Dynamic Data Authentication. EMV chip cards with SDA-level (Static Data Authentication) are not compliant.

disclosure of sensitive payment data, recurring payments to the same payees which have been previously set up by the payer through the use of strong customer authentication, and payments to self from a natural or legal person within accounts in the same payment service provider, also pose a low level or risk and should therefore listed as exemptions in these technical standards. **For the avoidance of doubt, SCA shall not apply to prepaid payment instruments subject to Article 63(1) point (b) of the Directive (EU) 2015/2366.**

Prepaid Verband Deutschland
Frankfurt, 30 March 2017

Dr. Hugo Godschalk
Managing Director

Prepaid Verband Deutschland e.V.
Im Uhrig 7
60433 Frankfurt
Germany
Tel.: (Germany) – 69 – 951177-17
Email: godschalk@prepaidverband.de
Website: www.prepaidverband.de