EMA RESPONSE TO THE EBA CONSULTATION ON THE DRAFT REGULATORY TECHNICAL STANDARS SPECIFYING THE REQUIREMENTS ON STRONG CUSTOMER AUTHENTICATION AND COMMON AND SECURE COMMUNICATION UNDER PSD2

1. List of Questions

Question 1: Do you agree with the EBA's reasoning on the requirements of strong customer authentication, and the resultant provisions proposed in Chapter 1 of the draft RTS?

The EMA finds the definition of the strong customer authentication ("**SCA"**) procedure to be overly narrow and prescriptive. The requirement – that the SCA should result in the generation of an authentication code ("**AC"**) ***that is accepted only once*** for a given PSU – appears to go beyond the SCA definition that appears in PSD2 {Art 4(30)}. Indeed, the attainment of SCA as defined in the PSD2 text can be delivered through the combined use of independent, secure, static authentication elements (passwords, device-specific certificates or credentials, biometric authentication etc.) without the need for a fresh, one-time AC to be generated for every SCA interaction.

We would request that the EBA affords more implementation flexibility to PSPs on how they can deliver SCA as defined in PSD2 text. We would expect the draft RTS to focus on the security requirements that the SCA procedure has to meet (as detailed in ***Art. 1.3*** of the draft RTS) rather than prescribe a specific SCA authentication procedure mechanism involving the generation of a one-time AC.

Different payment products and use cases will favour differing approaches to SCA, and vulnerabilities that may be introduced by user behaviour or by new security attack methodologies will need to be addressed through a variety of authentication mechanisms. Introducing regulatory provisions for a specific method of undertaking strong customer authentication can introduce systemic weaknesses that are better avoided.

More detailed comments on the text in Articles of the draft RTS are provided below:

- The language used in ***Art. 1.2*** ("*The authentication code shall be characterised by security features including, but not limited to, algorithm specifications, length, information entropy and expiration time*, ensuring that...") is confusing and does not appear to relate to security features of the AC. We suggest that the underlined text is removed altogether and that the Clause focuses on the security properties of the AC, instead.
- The reference to "*HTTP over TLS*" at ***Art. 1.3(d)*** as a minimum requirement to protect communication sessions during SCA has already been superseded by the launch of successful attacks against some HTTPS/TLS implementations (v1 and v1.1). It is advisable that the text is revised to refer to "*standardised, secure communication protocols resistant to known attacks*".
- The list of mechanisms detailed at ***Art. 1.3(e)*** appears to describe payment transaction anti-fraud mechanisms. It is not clear how these fit

into the SCA procedure that ***Art. 1*** describes. We would expect that the focus of the text would be on mechanisms to prevent and detect attempts to carry out customer authentication fraud rather than detect fraudulent payment transactions. We propose that the text in this Article is revised to focus exclusively on PSU authentication fraud attempts.

- The text at ***Art. 2.2(b)*** that introduces a requirement for the *device, channel or mobile application* displaying a dynamic linking code to be independent or segregated from *device, channel or mobile application* used to initiate an electronic payment transaction is overly limiting. The adoption of such an approach by PSPs would add very significant friction to the customer experience for mobile payment service users and lead to significant drops in payment transaction completion/conversion rates for most PSPs. We believe that channel segregation/independence on its own is adequate to deal with attacks that seek to compromise PSP-PSU communication sessions. We propose that the text underlined above, is revised to remove references to segregated *device or mobile application*.
- The text at ***Article 6.3*** appears to list a number of minimum, mandatory measures that are required to be deployed on multi-purpose devices used to store SCA elements. This list of measures is very prescriptive; the majority of mobile customer devices that are currently in the market do not include all the security controls detailed here. The EBA is encouraged to acknowledge that PSPs have limited control over the software that is executing on customer devices; in fact, most PSPs assume that customer devices have been compromised and rely on their own, back-office controls to limit the scope of any attacks/fraud that can be carried out from a customer device. We propose that the mitigating measures in this Section are listed as examples of good practice rather than as mandatory requirements. We would also advise that the reference to "*trusted execution environments*" is revised to avoid confusion since there is an existing cross-industry, mobile device standard developed by Global Platform http://www.globalplatform.org/specificationsdevice.asp with the same name. For example, a reference to *"segregated execution environments"* could be introduced to replace "*trusted execution environments*".

Question 2: In particular, in relation to the "dynamic linking" procedure, do you agree with the EBA's reasoning that the requirements should remain neutral as to when the "dynamic linking" should take place, under the conditions that the channel, mobile application, or device where the information about the amount and the payee of the transaction is displayed is independent or segregated from the channel, mobile application or device used for initiating the payment, as foreseen in Article 2.2 of the draft RTS.

The EMA welcomes the flexibility afforded to PSPs on the timing of the dynamic linking. We believe this is appropriate to support the many different types/models of payment interactions supported by PSPs.

As noted earlier in our Response to Question 1, we remain concerned that the requirement to segregate mobile applications or devices that are used to initiate a payment from those that are used to display the dynamic linking code are overly limiting. Our view is that channel segregation is adequate to ensure the required security properties of integrity and authenticity.

We are concerned that the text in ***Article 2.1(b***) that refers to an "*authentication code generated in accordance with Article 1*" that "*shall be specific to the amount of the transaction and the payee agreed to by the payer when initiating the transaction*" is actually an ***Authorisation Code*** rather than an Authentication Code. This is an important distinction that is not clearly identified in the text in Article 2.

Our understanding is that this Authorisation Code (and the dynamic linking requirement) will only apply to the subset of SCA interactions when an electronic remote payment transaction takes place (PSD2, Art. 97.2). We would propose that changes be introduced to the text at ***Art. 2*** to highlight the distinction between an Authentication Code (introduced in ***Art. 1***) and an Authorisation Code generated to achieve dynamic linking as introduced in ***Art. 2***.

Additionally, we seek further clarity from the EBA on the generation of a dynamic linking code in Use Cases where the final beneficiary/payee of a payment transaction is different to the owner/operator of an intermediate account where the funds will be transferred (e.g. a consolidated account that a PSP has established with a banking institution).

Question 3: In particular, in relation to the protection of authentication elements, are you aware of other threats than the ones identified in articles 3, 4 and 5 of the draft RTS against which authentication elements should be resistant?

The EMA is concerned about the impact of the new requirement introduced in ***Article 3.1*** (requiring knowledge-based authentication elements to comprise ***non-repeatable characters***). This requirement diverges from current security industry best-practice on the format of static knowledge-based authentication elements (e.g. passwords and passphrases); see <https://www.nist.gov/cnst/nanofab/other-operating-procedures-passwords-and-security>.

In addition to significant disruption for PSUs and PSPs, this requirement may actually increase rather than decrease security risks! A number of security industry studies have indicated the need to balance security requirements with usability when knowledge-based authentication standards are established. In the absence of such a balance, users often choose to write down overly complex passwords that are too difficult to remember.

Our view is that the reference to non-repeatable characters should be removed from this Article. The requirement to ensure resistance against the risk of compromise of knowledge-based authentication elements is already satisfied by the earlier references to length, complexity and expiration time.

On a different topic, we would advise replacing the phrase "***guarantees*** *resistance against unauthorised use of the elements*" in ***Art. 5.2***. There are no security measures that can guarantee resistance against security threats; instead, we would advise that the highlighted text is replaced by "*provides*".

Question 4: Do you agree with the EBA's reasoning on the exemptions from the application of Article 97 on strong customer authentication and on security measures, and the resultant provisions proposed in Chapter 2 of the draft RTS?

The EMA is concerned that the EBA's decision to exclude the provision of any SCA exemptions based on a transaction-risk analysis performed by the PSP will have a very detrimental impact to existing PSP service delivery models. This EBA decision has the effect of restricting existing PSD2 text

that appeared in PSD2 Art. 98.3(a) supporting SCA exemptions based on "*the level of risk involved in the service provided*". This could also be regarded as narrowing of the scope of the maximum harmonisation Directive, and one that is not in the gift of the EBA in Level 2 text.

The EBA in its introduction rationalises this exclusion on the basis of it being unable to define a set of criteria for exemption. A number of transaction risk analysis parameters are already available to PSPs to allow them to carry out effective transaction risk analysis. These include consumer device characteristics, communication session characteristics, payment application settings, payer/payee risk profile data, threat environment data, industry blacklists etc. The EBA appears to acknowledge the effectiveness of some of these risk analysis parameters by listing them in Art.1.3(e). We would encourage the EBA to re-introduce risk-based SCA exemptions to the list of SCA exemptions detailed in ***Art. 8***.

The EMA believes that a list of SCA exemptions triggered by static transaction thresholds will quickly become outdated leading to a poorer PSU experience and decreased transaction security levels. Additionally, it is not clear how the EBA chose the static SCA exemption transaction thresholds listed in ***Articles 8.1(b) and 8.2(d)***. We would encourage the EBA to remove references to static transaction thresholds from the list of SCA exemptions in these draft RTS articles. A list of static SCA exemptions will not be future proof and will prevent future innovations in fraud prevention analysis.

The list of static SCA exemptions in Art. 8 appear to apply only to payer AS-PSPs. The EMA would like the EBA to comment on the scope of its existing mandate to remove:

a) The SCA exemption that applied to acquiring PSPs in Guideline 7.5 of the *EBA Guidelines on the security of internet payments* (EBA GL/2014/12) and,

b) The ability of payee PSP to process a payment transaction without SCA while accepting the liability for any financial loss caused to the payer's PSP as detailed in PSD2 Article 74.2

The removal of the ability of payee PSPs to apply exemptions to the requirement to complete SCA will severely impact the interactions of users of digital wallets; these are becoming increasingly popular as a means of limiting the sharing of payment credentials with multiple parties while allowing an increasing number of small/medium size EU enterprises to accept electronic remote payments. Specifically, payment transactions that are used to fund digital wallet accounts could be subject to two (2) SCAs carried out back-to-back (by the wallet provider followed by the issuer of the underlying payment instrument that is used to fund the wallet account). Such an arrangement would limit the usability and appeal of these popular e-commerce payment products.

Our view is that the EBA's PSD2 mandate does not extend to the restriction/removal of Level 1 (PSD2 text) or of provisions introduced in other EBA Guidelines introduced as recently as August 2015. Therefore, we propose that the list of SCA exemptions is extended to allow payee PSPs to apply SCA exemptions after conducting transaction risk analysis.

The EMA would welcome further clarification on the definition of the term "*electronic mandate*" in the context of a direct debit transaction as it appears in ***Rationale Clause 18***. At present, there is still considerable confusion in the industry on whether the term "*electronic mandate*" as used in this rationale Clause refers to an *e-mandate*? E-mandates are used by a number of direct debit schemes across the EU to establish/change the terms of a direct debit arrangement agreed between the payer, the payee/payee PSP and the payer AS-PSP.

The EMA would encourage the EBA to consider the impact of the proposed static SCA exemptions on a range of payment products that are

currently treated as lower-risk products by PSPs such as payment products/services where the payer is a legal person or a business entity rather than an individual (e.g. commercial payment cards, payments on B2B e-marketplaces etc.).
It must be noted that PSD2 text (Art. 38 & 61) permits contractual derogations to all of Title III and most of Title IV for payment services provided to persons other than consumers hence covering (a) Legal persons and, (b) Natural persons acting in a professional or business capacity (*which by extension applies to the notion of a commercial card defined in EU Regulation 2015/751 on interchange fees for card-based transactions*). The blanket application of the static SCA exemptions detailed in ***Art. 8*** to such products, would penalise such providers/users even though the fraud risks they are facing are demonstrably lower and better mitigated. In this context, additional SCA exemptions for payment interactions initiated by or behalf of legal persons should be considered by the EBA.

The EMA also wishes to offer the following comments on the text of ***Article 8***:

- It is not clear why the SCA exemption on payee whitelists {in ***Art. 8.2(a)***} is limited to PSU-generated payee whitelists. It seems sensible to allow an AS-PSP to generate its own whitelists to reflect ongoing customer behaviour, the risk-profile of the payee, the frequency of such payments etc. We propose that AS-PSPs are also allowed to generate such payee/beneficiary whitelists that can be exempted from SCA.
- Building on the concept of PSU-generated payee whitelists that are exempt from SCA, we believe it would be useful to allow PSUs to define their own payment transaction thresholds for transactions that are exempted from the need to do SCA. These user-defined thresholds would be lower than upper PSP-defined limits that reflect the risk profile of individual PSUs. The process of setting/changing PSU-defined risk acceptance parameters should itself be protected by SCA.
- We would welcome any insights that the EBA may be able to offer on the choice of the two different sets of SCA exemption transaction thresholds listed in ***Articles 8.1(b) and 8.2(d)***. If such static SCA exemption thresholds are used, they should at least be harmonised to ensure consistent PSU behaviour. Additionally, they should be aligned with the low value payment instrument definition that appears in PSD2 Article 42.

Question 5: Do you have any concern with the list of exemptions contained in Chapter 2 of the draft RTS for the scenario that PSPs are prevented from implementing SCA on transactions that meet the criteria for exemption?

The EMA would really welcome clarity from the EBA on whether the SCA exemptions listed in ***Art.8*** are minimum requirements for PSPs; that is, whether PSPs can choose to carry out SCA even for payment interactions that would normally benefit from the SCA exemptions defined in ***Art.2***?

EMA members are concerned that AS-PSPs may choose to apply SCA more frequently or strictly to payment account interactions initiated through an AIS or PIS provider leading to a poorer customer experience for users of such services.

We invite the EBA to work with national competent authorities to ensure that payment account interactions initiated through an AIS/PIS are not disadvantaged by the discriminating application of SCA exemptions on the part of AS-PSPs.

Question 6: Do you agree with the EBA's reasoning on the protection of the confidentiality and the integrity of the payment service users' personalised security credentials, and the resultant provisions proposed in Chapter 3 of the draft RTS?

The EMA is broadly satisfied with the requirements on the confidentiality and integrity protection afforded to Personalised Security Credentials (PSCs) detailed in Chapter 3 of the draft RTS. The EMA has some specific comments to offer on text that appears in Chapter 3 of the draft RTS:

- The reference to "*tamper resistant devices and environments*" in ***Art.9.1(c),*** should be clarified. We would encourage the EBA to consider the cost/impact of having to store all secret cryptographic material used to encrypt PSCs in tamper-resistant environments (typically HSMs, smartcards or other hardware tokens). The adoption of the specific approach required by this text would preclude the wide use of other popular mechanisms (e.g. secret key fragmentation with fragments stored in different systems with no single-party access to all systems) to protect secret cryptographic material.
- In ***Art. 12(b)*** there appears to be a cyclical requirement for a PSP to perform SCA when associating a PSU's identity with his/her assigned PSCs via a remote channel. It is not clear how this process will work since these PSCs are likely to be used to drive the SCA in the first place! We invite the EBA to provide more clarity on the subject of associating a PSU to a set of PSCs over a remote channel. In this context, we would propose that the EBA requests that at least one feature of the PSCs is delivered to the PSU through a different channel than the one used to associate his/her identity with a set of PSCs to limit the scope of successful account takeover attacks.
- In ***Art. 14,*** we believe that the PSC lifecycle management scenarios listed here raise different risk implications. The use case of scheduled renewal of expiring credentials is different to the replacement/re-activation of credentials that may have been compromised from a risk management perspective. In the latter case, we would suggest that the security requirements listed to the delivery of PSCs (listed in Articles 12 & 13) should apply.

Question 7: Do you agree with the EBA's reasoning on the requirements for common and secure open standards of communication for the purpose of identification, authentication, notification, and information, and the resultant provisions proposed in Chapter 4 of the draft RTS?

The EMA supports the approach taken by the EBA in ***Chapter 4*** of the draft RTS to specify the requirements that must be satisfied by every communication solution used for the secure communication between PSPs while remaining technologically neutral.

The EMA has concerns about the use of explicit references to standards (ISO 20022, ISO 27001) that have not previously featured prominently in the service roadmap of many PSPs offering online payment services.

A set of more detailed comments in Chapter 4 of the draft RTS is listed below:

- In ***Art. 17.1,*** the EBA is asked to clarify the use of the term *secure bilateral identification* between the payer's device and payee's payment acceptance device. Typically, bilateral authentication would be required to deliver such a secure bilateral identification. In turn, this would

require the secure delivery and verification of public-key cryptographic material to the payer and payee devices. Is this what is intended by this requirement?

- In ***Art. 19.7,*** we are concerned that some AS-PSPs may discriminate against certain PISPs/AISPs that have not established contractual commercial relationships with the AS-PSPs when carrying out functional integration testing using the inter-PSP communication interface. We would welcome any guidance that the EBA can provide to national competent authorities on the need to ensure a consistent provision of interface testing & support services by the AS-PSP to all PISPs/AISPs that wish to access it.
- In ***Art. 21.1,*** we would ask that the EBA clarifies the reference to "*strong and widely recognised encryption techniques*" that appears at the end of this Clause. Does the EBA propose to publish/maintain an updated list of such encryption techniques? It could be advisable to consider referencing existing international financial cryptography standards that describe such techniques.
- In ***Art. 21.6,*** the text appears to introduce a requirement for compliance with the ISO 27001 Information Security Management Standard (ISMS) for AIS/PIS providers. This is not a current authorisation or supervisory requirement for credit institutions, for electronic money institutions, nor for payment institutions, and it is unclear why this should be made mandatory for payment initiating and account information service providers. We would also note that ISO 27001 is an organisational information security standard; compliance requires the use of external, certified auditors and can be an expensive exercise that needs to be repeated every 3 years. Our view is that it would be appropriate to afford flexibility to the PSPs on the "*common security standards*" to use to protect PSCs/ACs that routed or processed through their systems. Therefore, we propose the removal of the explicit reference to ISO 27001 from the end of the last sentence in ***Art 21.6***.

Question 8: In particular, do you agree that the use of ISO 20022 elements, components or approved message definitions, if available, should be required to ensure the interoperability of different technological communication solutions implemented between PSPs for the provision of AIS, PIS or for the confirmation on the availability of funds? Do you see any particular technical constraint that would prevent the use of such industry standards?

The EMA wishes to highlight the fact that the use of ISO 20022 financial messaging data formats is much less widespread in the online PSP space compared to other financial service industry communication networks (e.g. ISO 8583-based interbank financial messaging networks, payment card messaging networks etc.). In contrast, the use of communication interfaces based on JSON (JavaScript Object Notation) described in the IETF RFC 1759 standard https://tools.ietf.org/rfc/rfc7159.txt is very popular among the online PSP community.

We are concerned that the explicit reference to a standard whose use is very limited in the online PSP world may lead to online PSPs being disadvantaged (or limited) in their choice of communication interface to use to access payment account data held by some AS-PSPs. We propose that the text of Art 8.3 is changed to read:

> "*Account servicing payment service providers shall ensure that their communication interface uses elements components or approved message definitions as well as standards of communication which are developed by international or European standardisation organisations*".

Question 9: With regards to identification between PSPs, do you agree that website certificates issued by a qualified trust service provider under an e-IDAS policy would be suitable and allow for the use of all common types of devices (such as computers, tablets and mobile phones) for carrying out different payment services?

The EMA supports the view that an e-IDAS Qualified Trust Service provider (***QTSP***) can potentially be used to issue PSP server certificates that are used to enable secure identification and authentication of PSPs. However, a set of additional requirements would also need to be satisfied to deliver these security properties:

- The scope/quality of the identification of the PSP carried out by the QTSP should be detailed. This should be consistent across QTSPs,
- The detail/accuracy of the PSP role identification that appears on the QTSP certificate. Here, it is worth noting that many PSPs will have multiple/changing roles (e.g. AS-PSP, PISP, AISP etc.),
- The robustness of the certificate revocation processes of the QTSP,
- The effectiveness of the access controls used to protect the PSP secret key.

The EMA is concerned about the availability of multiple QTSPs to service PSP certification requests in the period running up to the adoption of these RTS. The presence of a limited number of QTSPs can lead to increased PSP certification costs. We believe that explicit contingency provisions should be included in the draft RTS to address the lack of availability of e-IDAS QTSPs in EU markets.

We also note that the use of a e-IDAS Public Key Infrastructure (to allow PSUs to access payment services (after verifying the identity of the PSP) is dependent on the inclusion of an e-IDAS top-level CA certificate in the list of CA certificates supported by most common Internet Browsers. Finally, it is worth highlighting that payment interactions initiated by most consumer devices will continue to be vulnerable to a range of software-based attacks that aim to imitate a legitimate PSP.

Question 10: With regards to the frequency with which AIS providers can request information from designated payment accounts when the payment service user is not actively requesting such information, do you agree that the proposed limit of no more than two times a day achieve an appropriate balance between allowing AISP to provide updated information to their users while not negatively impacting the availability of the ASPSP's communication interface? If not, please indicate what would be in your view the appropriate frequency and rationale for such frequency.

The EMA understands that reasonable limits should be established to the frequency of automated AIS payment account requests that are not directly initiated by a PSU.
We would propose that the number of such access requests that will be serviced by the AS-PSP is increased to ***hourly (1 per hour) for a given payment account***. We feel that this provides appropriate balance between AIS service priorities and the desire of the AS-PSP to ensure optimal

performance of the communication interface it provides to its payment account management platform.
If the frequency is made lower, users will simply be prompted to seek updates manually. The usefulness of most account information services will depend on the freshness of the information. Out of date transaction information could result in users drawing false conclusions and in undermining the utility and appeal of such services, altogether.

EMA members strongly support the text in Art. 22.5(b) that requires AS-PSPs to service ***every*** account information update request initiated directly by the AIS provider user.

General Comments

1. After reviewing Section 5.1 of the Consultation Paper (*Draft cost-benefit analysis/impact assessment*) we have found little detail on the impact assessment of the requirements in the draft RTS on the operations of PSPs across the payment industry as assessed by the EBA.

   Therefore, the EMA would welcome an EBA statement on (i) their assessment of the industry costs of the introduction of these requirements (ii) the size of the projected benefits for PSUs and for PSPs (e.g. decrease of transaction fraud losses, wider user adoption of electronic and remote payment services) and finally (iii) the outcome of the comparison of the costs vs. benefits that was carried out in the course of drafting these RTS.

2. Many global PSPs and online merchants have stated that the introduction of these requirements will force them to ring-fence EEA consumers from the rest of their user base and lead to reduced service access and a poorer customer experience for PSUs in the EEA. Therefore, we believe that it is important to ensure maximum flexibility in achieving specific security properties while avoiding prescriptive definitions of the mechanisms to use to meet security requirements.