RESPONSES TO CONSULTATION PAPER			
re:	**Consultation Paper on the draft Regulatory Technical Standards specifying the requirements on strong customer authentication and common and secure communication under PSD2**		
for:	European Banking Authority		
date	version	author	action
07.10.2016	v1	dLK	Responses to Consultation Paper

I DO YOU AGREE WITH THE EBA'S REASONING ON THE REQUIREMENTS OF THE STRONG CUSTOMER AUTHENTICATION, AND THE RESULTANT PROVISIONS PROPOSED IN CHAPTER 1 OF THE DRAFT RTS?

Please see the specific comments below.

II 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.

III 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?

No comment.

IV 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?

Exemptions to the application of Strong Customer Authentication (SCA) are only partially adequate to the existing and predictable future developments in commerce and payments.

As far as the exemption for contactless payments is concerned the exemption is not technologically neutral. Despite current massive growth of payments deploying NFC technology, the long-term well – established trends are proximity payments on one hand and remote payments on the other hand. Contactless payment is only one of many scenarios of proximity payment. Proximity payment remains a durably distinctive category of payments. This is valid both generally and specifically for the security layer. Due to the physical constraints of the proximity

environment (e.g. amount of goods and services that can be traded) combined with rich natural context (ability to detect irregularities in payers' behavior) the ability to commit massive fraud is substantially limited while in the remote environment the scale of fraud is actually unlimited. This advantage is inherent to all proximity payments and justifies the exemption of all proximity payments from the requirement of advanced authentication of the person behind the transaction.
The EBA is invited to consider substituting the "contactless" wording with a formula offering long-term neutrality. For the time being and in the predictable future the core of the proximity payment is that the payee's payment device must be used in the payer's presence.

As far as the exemption for remote payments is concerned, the draft RTS largely disregards the current developments in global and European e-commerce. The design of the SCA in the draft RTS results in the following procedure for completion of payments:

a) the payer's identity is verified at two checkpoints (two – factor authentication) in the primary communication modality,
b) having completed the conversation with the PSP in the primary communication modality the payer changes the communication to an alternative modality (modalities),
c) in the alternative communication modality the payer receives from the PSP the "digested" content of the communication that finally reached the PSP in the primary communication modality,
d) the payer confirms in either modality that the communication is correct.

While respecting unconditionally the mandate and commitment to fighting fraud in payments, the procedure described above is one of a number of scenarios that ensure that a two-fold ultimate goal is reached:

a) customers are secured against fraud targeted at their funds;
b) PSP are secured against systemic risk of losses resulting from liability towards customers for unauthorized payment transactions.

Over the years, thanks to increasing data on fraud, the ability to process large volumes of data retrospectively (to learn from the past) and instant availability of data representing multiple layers of payment transactions (enabling fraud to be combated in real time), the approach in which a person and transaction is represented by static data which is verified at a specific static point (points) in time is actually a modest level of security. Indeed there is no physical contact with the person that initiates the transaction. However the existing close interconnections between the stakeholders (issuers, schemes, acquirers, merchants) and the high speed and low cost (relative) of communication and data processing provide a very rich picture of the remote person and transaction. This is gradually making it possible to identify correctly the payer without static information like login and password. These developments have opened the way for tailoring payment services to the specific needs of e-commerce and interconnected commerce (commerce with a seamless transition between the remote and proximity dimensions of trade) where the act of payment does not obstruct otherwise successful trade.
All of the considerations discussed so far were covered thoroughly in the feedback to the EBA from the payment industry. Despite these considerations being highly relevant the draft RTS effectively disregards the "acquis" of risk-based transaction handling and imposes an extremely strict static authentication requirement regardless of the outcome of the risk-based techniques. It follows from the EBA's public hearing that took place on 23rd September 2016 that the reason behind leaving aside this "acquis" is the lack of a common objective parameter that might apply across all business models that successfully differentiates between mostly secure conduct and mostly risky conduct. The draft RTS fails however to explain why the self-explanatory objective parameter which is the empirical fraud rate of a payment service was apparently disregarded.

The EBA is invited either to consider the fraud rate approach (described below) or clarify why this approach was rejected if in fact it was considered.

In the fraud rate approach the PSP would apply authentication other than SCA where the fraud rate does not exceed the predetermined fraud target. The fraud target would be established by the RTS either at uniform level across all business models or specifically for the small number of the most regular business models. Taking into account that the immediate reason for European authorities intervening in payment security was the increase in the fraud rate after 2011, the 2011 fraud rates might be the preferred objective parameter (0.036% of value and 0.016% of volume in the case of card fraud – see the European Central Bank's "Fourth report on card fraud"). In this scenario the PSP would apply authentication other than the SCA where:

a) the fraud rate in the preceding primary reconciliation period (rather long, e.g. a quarter) was under the target fraud rate;
b) the ratio of transactions questioned by users in the preceding second level reconciliation period (rather short, e.g. one week), both in terms of volume and value, to the total transactions in the preceding second level reconciliation period does not exceed the target fraud rate;
c) none of the circumstances of the transaction known to the PSP (including at a minimum the geographical location of the payer and merchant, relative location thereof in the communication network used for transaction initiation, time of transaction initiation, device, amount of the transaction, and the change in those circumstances compared to recent transactions) make it unlikely that the transaction is initiated by a legitimate payer.

V 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?

No comment.

VI 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?

No comment.

VII 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?

Based on the existing draft RTS and the explanation offered by the EBA officers in the public hearing of 23rd September 2016, it is understood that the current draft of the RTS:

a) requires each ASPSP offering payment accounts with direct online access for the user to implement an online interface that effectively uses a European or international standard of communication, with explicit reference to ISO 20022 as a possible solution;
b) requires that once an ASPSP effectively implements an interface entirely compliant with the RTS (including with respect to the availability of the interface specification, testing environment, support, performance of the interface benchmarked by the direct online access, and terms and conditions of use of the TPP services by the user), the ASPSP does not have to accept an attempt by a TPP to access the account by means other than via the interface, and such conduct does not constitute discrimination of the TPP services (the question remaining open however is whether in such a case under Article 68.5 of the PSD2 the ASPSP is required to notify the conduct to the payer and to the competent authorities);
c) does not limit the user's right to make use of TPP services provided other than via the interface (including via the user emulation by the TPP in the ASPSP's online banking, often referred to as "webscraping" or "screenscraping") where the ASPSP failed to implement the interface or where the interface offered is not RTS

compliant, including due to a non-compliant standard of communication or underperformance when compared to online banking.

The approach described above restricts the room for maneuver that the European legislators seem to have offered the EU providers in the PSD2. Indeed the PSD2 was expected and understood to mandate change in the patterns for access of accounts on one hand and for making accounts available to such access on the other hand. However the scope and impact of the change was expected not to exceed the most narrow set of policy instruments that ensure that the access of the TPP is limited to the account and transactions information instead of all information available in online banking (which seems to have been the key underlying purpose of the PSD2 in the dimension of risk mitigation). The "minimum set" approach offers the advantage of business continuity for existing TPPs and moderate investments on the part of the ASPSPs that have no ambition to enter the TPP environment (passive compliance). In the "minimum set" scenario a passive ASPSP instead of the unconditional requirement to implement an interface different from online banking would comply with the PSD2 by providing any communication facility that limits the information available to the TPP to accounts and transactions. If this passive ASPSP chose to designate an existing online banking interface as a PSD2 interface the ASPSP would need to adopt specific and effective measures to ensure that the information available to the TPPs is filtered, e.g. by issuing two set of credentials to the users wishing to use the TPP services where the "TPP set" would limit the online banking content to accounts and transactions only (or in any case differentiating between the credentials that are intended for use with the TPP).

If the final version of the RTS however follows the reasoning presented at the beginning of this section, insofar as the RTS requires that once the RTS enters into force the RTS' method for accessing the account is the interface newly provided by the ASPSP without the TPP having time to prepare to connect to the interface (under the draft RTS the ASPSP is not required to make available the interface and the specification thereof before the RTS is live) the RTS actually expose to uncertainty the business of the existing TPP for an unpredictable period of time. The requirement to use the interface is therefore equivalent to the requirement of authorization by the competent authorities. The reason for this is that in both cases the factors that impact a TPP's compliance with new regulations are beyond the TPP's control. In such a case the proportionality principle requires that an adequate transitory period is ensured. This period needs to take into account the usual time needed to decode a specification of an IT interface and develop the component needed to connect to the interface. The adequate period is not less than six months after the ASPSP either has made available the interface or made available the specification and testing environment, whichever occurs later.

VIII 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 reference to "at least European or international standard" gives precedence to existing communication standards. It will be hard to consider any new standard with at least pan-European aspiration which is created in a single EU country to be a RTS compliant standard before it is used by any provider outside that country. The RTS fails to clarify when a standard aspiring to pan-European or international level is understood by the RTS to be one which complies with the RTS when used in the interface.

IX 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?

No comment.

X 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.

A frequency of two requests per day will limit substantially the functionality of the AIS services. The limit of two requests per day practically eliminates any kind of "push" AIS services, i.e. an AIS service that actively informs the user of important changes on the account (e.g. that an important payment arrived intraday on the account). Where the AIS may update the account balance no more frequently than before and after the user's close of business, the only way to ensure reasonable use of the AIS service will be to manually push the "update" button inside the AIS application.

The maximum number of requests (if any) should reflect the usual patterns of online banking usage including those where important changes take place on the account. The closest benchmark is a mail fetching feature offered by the top global e-mail service providers. In those services the e-mail box of a third-party provider is checked for new e-mails at least once every hour.

Therefore the EBA is invited to consider combining the perspective of the usual online usage including periods of important changes and the mail-fetching benchmark referred to above. Those perspectives justify a maximum number of requests of between 7 and 24 requests daily.