Bundesverband der Zahlungsinstitute e.V. Im Uhrig 7 60433 Frankfurt a.M.

European Banking Authority
One Canada Square (Floor 46)
Canary Wharf

London E14 5AA

Im Uhrig 7
60433 Frankfurt am Main

Telefon: (069) 95 11 77-15
Telefax: (069) 52 10 90
www.bvzi.de
info@bvzi.de

VR 14320
Amtsgericht Frankfurt am Main

Präsidium (Vorstand):
Stephan Neuberger (Sprecher)
Dr. Karsten von Diemar
Stephan Dumröse
Christof Kohns
Dr. Claudia Willershausen

Response to Consultation Paper on the draft Regulatory Technical Standards specifying the requirements on strong customer authentication and common and secure communication under PSD2

EBA/CP/2016/11 dated 12 August 2016

Frankfurt am Main, 12 October 2016

Dear Sir or Madam,

The German Federal Association of Payment Institutions (**BVZI**) represents the interests of the Payment and E-Money Institutions established in Germany.

We welcome the opportunity to comment on European Banking Authority's (**EBA**) Consultation Paper on the draft Regulatory Technical Standards on strong customer authentication and common and secure communication under the revised Payment Services Directive (**PSD2**) (hereinafter **Consultation Paper**) published on 12 August 2016.

Our response includes some general comments by the BVZI as well as detailed answers to Q1 – Q9 in the Consultation Paper. We have included our general comments in our answer to Q1 since EBA's website for submitting comments only provides for fields for answers to specific questions. We nevertheless want to take the opportunity to outline some general thoughts and considerations. A digital version of our responses has been sent to EBA using the "you're your comments" button on EBA's website.

We have prepared this document in close cooperation with Dr. Richard Reimer, partner at Hogan Lovells International LLP.

Bankverbindung:
Commerzbank AG
IBAN: DE30 5004 0000 0580 2442 00
BIC: COBADEFFXXX

Response to Q1 – Q9

Part I – Strong Customer Authentication Requirements

1. **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?**

We generally appreciate EBA's approach towards technology neutral Strong Customer Authentication ("**SCA"**) requirements. However, we do not think that the current Draft RTS possess the necessary degree of clarity and coherence. In addition, we think that the Draft RTS do not reflect the needs of market participants, such as consumers, merchants and payment service providers, and do not provide for technically sound SCA requirements. In addition, we are of the view that the current Draft is missing the business model neutrality. In the following, we would like to discuss why we are of the opinion that the Draft RTS should be thoroughly revised.

General Remarks

Before going into detail, we would like to stress that we have concerns regarding how the public can contribute to the consultation. The consultation form on EBA's website only provides for fields for specific answers. There is no field for general remarks or additional comments. This may lead to the false impression that the public may only answer to and comment on EBA's specific questions but may not comment on other issues and the draft in its entirety. This may discourage fruitful contributions to the consultation by members of the public. In our opinion, future consultations should have a broader scope in order to better reflect Article 10 (1) subparagraph 3 of the Regulation (EU) No. 1093/2010 ("**EBA-Regulation**") which calls for an "open public consultation".

Scope of SCA (Rationale 16 et seqq., Recitals 1 and 2 to the Draft RTS)

We recommend adding some clarifications to the Recitals of the RTS regarding the scope of SCA. In accordance with Article 97 (1) PSD2 and Recital 95 to PSD2 ("[…] *security of electronic payments* […]"), SCA only applies to electronic payments. This is also reflected in the Recitals to the Draft RTS. However, we recommend clarifying that not all transactions involving some form of electronic transmission of transaction data fall under the scope of SCA because these transactions are often paper-based from a legal point of view. In particular, SEPA Direct Debits generated at the point-of-sale by means of the payer's debit card are not an initiation of an electronic payment within the meaning of Article 97 of PSD2 and/or SCA since the SEPA mandate, is not given electronically but by personally in writing at the point-of-sale. The signed SEPA mandate is a valid authorisation of a payment order in accordance with Article 64 (1) PSD2. This shows that the transaction is in fact not an electronic payment transaction which falls under the scope of SCA but a paper-based payment transaction. The fact that the payment data necessary for the settling of the debt are transmitted electronically to the payer's payment service provider for clearance does not mean that the SEPA Direct Debit is an electronic or otherwise remote payment transaction because the actual payment order is always on paper. Hence, SCA does not apply.

The same rationale applies to credit card transactions where the payer authorises a payment transaction by signing a credit card slip/receipt. The only difference to direct debits is that the debt is not settled against the payer's current account but against the payer's credit account with the issuer of the credit card.

In fact, where a customer challenges a direct debit transaction or a credit card transaction authorised by signing a credit card slip, a payee is required to produce the signed mandate or credit card slip to demonstrate proper authorisation of the payment transaction initiated through the payee. This clearly shows that these kinds of transactions are not electronic payment transactions within the meaning of SCA even though payment data are transmitted electronically.

Role of Acquirers and Article 74 (2) of PSD2 (Rationale 19 (b))

We do not share the view that card acquiring payment service providers ("**acquirers"**) when payments are initiated by or through the merchant should require payees in card-based payment transactions ("**merchants**") to support SCA for all payment transactions. In our understanding of PSD2, the SCA requirement concerns the account servicing payment service provider of the payer but does not bind acquirers. Even less are merchants concerned. Rather, acquirers and merchants may make a deliberate decision to not apply SCA and to bear the risk of ultimate liability pursuant to Article 74 (2) PSD2 instead.

Firstly, a payment transaction may not only be authorised prior to the execution of a payment transaction, but may also be authorised by the payer after the execution of a payment transaction (cf. Article 64 (1) sentence 2 PSD2). The clear wording of Article 64 (1) of PSD2 shows that there can be transactions where a payee initiates a payment transaction without a formal authorisation by the payer. Consequently, there is no room for a strict obligation to support SCA for every transaction when the payment is initiated by or through the payee. This is currently not fully reflected in the Draft RTS even though the RTS is delimited by PSD2 and should therefore mirror the PSD2-framework.

Secondly, we strongly disagree with EBA's view that Article 74 (2) of PSD2 is only applicable until the RTS enter into effect. It cannot be argued that acquirers are obliged to require merchants to support SCA based on the argument that Article 74 (2) of PSD2 only applies during the transitional period. Neither Article 74 (2) of PSD2 nor Article 115 of PSD2 on transposition contains any indication to that effect. Quite to the contrary, Article 115 (4) of PSD2 contains a detailed provision on the timeframe for implementing the RTS. This provision does not contain any reference to Article 74 (2) of PSD2. In particular, this provision does not state that Article 74 (2) of PSD2 merely applies prior to the implementation of the RTS. Moreover, the European Commission already included the provision of Article 74 (2) of PSD2 (= Article 66 of the Commission's Proposal for PSD2 COM/2013/547 (final)) in the first draft of PSD2 without a specific transitional period for SCA. It is therefore safe to assume that European legislators had no intention of applying Article 74 (2) of PSD2 only during the transitional period.

Rather, European legislators have designed Article 74 (2) of PSD2 to generally provide for a shift of liability where SCA is not used because either the payee (e.g. a merchant) or the payee's payment service provider does not support SCA. There is no time limit to this shift of liability. We understand that the provisions set forth in Article 74 (2) of the Draft RTS are an indispensable element to achieve the objectives of the PSD2, namely to fully protect payers from damage through unauthorised payments and to allocate the liability

for unauthorised transactions to the responsible party. This being said, a payee or the payee's payment service provider may – at their own discretion – accept and process payment instructions even where neither the payer nor the payer's payment service provider have requested SCA.

Moreover, the decision to apply Article 74 (2) of PSD2 only during the phasing-in of SCA and the RTS may not be taken by EBA or by means of Regulatory Technical Standards adopted by the Commission as Regulatory Technical Standards may only specify technical details but may not imply strategic decisions or policy choices. Furthermore, the content of Regulatory Technical Standards is delimited by the legislative acts on which they are based (cf. Article 10 EBA-Regulation). It is therefore not possible to deviate from the European legislators' decision to generally apply Article 74 (2) of PSD2.

Thirdly, there is no compelling reason why acquirers or merchants should be obliged to always request SCA prior to accepting a payment instrument. We understand that the SCA requirement exclusively concerns the relationship between the payer and an issuer of a payment instrument/an account servicing payment service provider. As a general rule, the payer has to be authenticated by means of SCA when payers initiate a payment transaction through their account servicing payment service provider (**ASPSP**) (Article 97 (2) (b) of PSD2). If the payment service provider of the payer fails to apply SCA, then Article 74 (2) sentence 1 PSD2 applies and payers are only liable for fraudulent activities. In other words, the payment service provider of the payer fully bears the risk of unauthenticated transactions. Thus, the payment service provider of the payer is incentivized to only accept SCA-authenticated payment transactions from his customer. If however the payment transaction is initiated by or through the payee, the payment service provider of the payee may at its own discretion ask the ASPSP of the payer for authentication of the payer. Subsequently the ASPSP of the payer can refuse to execute non-SCA-authenticated transactions. Alternatively, the ASPSP may accept the non-SCA-authenticated transaction and assume liability vis-à-vis the payer for the transactions amount. In the event of an unauthorised transaction, the payer's payment service provider than is indemnified by the payment service provider of the payee and ultimately the merchant. This shift of liability or chain of liability demonstrates that SCA provides for an allocation of risk. As a consequence of this shift of liability, payers are generally protected against unauthorised transactions – either because SCA is used when authorising a payment transaction or because the payer's payment service provider has assumed liability. In addition, this demonstrates that the need for SCA and the subsequent allocation of liability depends on whether a payment is initiated through the payee or through the ASPSP of the payer. Whereas a layered security is inherent to pull payments (i.e. initiated by or through the payee) as all three parties involved in the execution of a payment transaction, i.e. the merchant, the acquirer and the issuer, may apply appropriate security measures to provide for secure, convenient and cost-efficient payments, push payments (i.e. initiated by payers through their the ASPSP) draw primarily on the measures which the ASPSP applies. The different nature of push payments and pull payments should be reflected in the requirements for of SCA. In particular, the RTS should address the fact that pull-payment involve more than one payment service provider and that the ASPSP, the payment service provider and the payee can all apply suitable security measures. For the sake of business and technological neutrality, EBA should chose a neutral approach rather than the current one-size-fits-all approach. This being said, we do not see the need to require acquirers or merchants to support SCA for every payment transaction. Rather, they should be permitted to make a deliberate decision not to apply SCA (and to assume liability vis-à-vis

the payer's payment service provider). This mechanism provides for an equitable solution since payers are protected against the consequences of unauthorised transactions while maintaining a risk-based (and cost-efficient) application of SCA by acquirers and merchants.

Fourthly, there can be no general obligation of acquirers (and merchants) to only accept SCA-authorised transactions since Title III of PSD2, including Article 97 of PSD2, also applies to one-leg-transactions (cf. Article 2 (4) of PSD2). In accordance with Article 2 (4) of PSD2 most provisions in Title III of PSD2 apply to one-leg transactions where only one payment service provider is situated in the European Union in respect to those parts of the payment transaction which are carried out in the European Union (cf. Article 2 (4) of PSD2). If for instance a Swiss issued payment card is accepted by a merchant in the European Union, PSD2 will apply to the acquiring part of the transaction. Since Article 2 (4) of PSD2 does not exclude Article 97 of PSD2, the acquiring part of the transactions would be subject to SCA requirements if acquirers and merchants were obliged to only accept SCA-authenticated transactions. However, a third-country issuer may not provide SCA as defined in the RTS. Thus acquirers and merchants are not able to support SCA when accepting and processing these payment transactions. In our opinion, this shows that there should be no general obligation of acquirers and merchants to support SCA every time a payment transaction is initiated. In any event, it should be clarified that third-country issued payment instruments may be accepted by EU merchants and acquirers without SCA.

Technology neutrality (Rationale 20 et seqq.)

We highly appreciate that EBA opted for a technology neutral approach as regards SCA. However, we are of the opinion that this approach is not entirely reflected in the Draft RTS since the Draft RTS contain various minimum technical standards and require the implementation of specific so-called "security features".

For instance, Article 1 (2) of the Draft RTS specifies certain minimum "security features" ("including, but not limited to"). This is in stark contrast to EBA's general position that the Draft RTS should be technology neutral since a technology neutral provision would merely define the outcome (e.g. what is to be ensured) but would not contain technical specifications on how to achieve this goal. For the sake of technology neutrality, the specification of minimum "security features" should be deleted.

Moreover, we think that the wording "including, but not limited to" should be avoided in the final RTS because the wording generally indicates a minimum requirement and not just examples as would be appropriate for a technology neutral approach. Again, technology neutrality means that there should be no specifics on how to achieve certain results.

EMV (Chip & PIN) (Rationale 22 (b) and Article 1 (1) Draft RTS).

Article 1 (1) of the Draft RTS requires that the SCA procedure results in the generation of an authentication code which is accepted only once by the payment service provider. In our opinion, this requirement should be clarified with regard to electronic transactions at POS terminals. Where a payment is initiated through the payee, payers usually enter their authentication credentials (PIN) at the point of sale. If the transaction is an EMV transaction (Chip & PIN), the payer's authentication credentials are not necessarily verified by the payer's payment service provider, i.e. the issuer, but often at the point of

sale (e.g. by the EMV Chip and the payment terminal; so-called offline authentication). The acquirer then sends an authorisation request to the issuer which is subsequently either approved (we use the term "approval" instead of the industry specific term "authorisation" to distinct the approval of a card transaction through the issuer from the authorisation of a payment transaction through the payer in the meaning of PSD) or declined (e.g. because of insufficient funds on the payer's current account). This procedure is an integral part of the EMV technology. Rationale 52 of EBA's Consultation Paper states that the EMV technology provides for a high degree of safety. We assume that the current EMV procedure already fulfils the SCA requirements as set forth in PSD2. However, we understand that the wording of Article 1 (1) of the Draft RTS does not reflect the process of a terminal initiated pull-transaction. In particular, we do not understand which data element in an EMV transaction is considered to be the "authentication code" within the meaning of Article 1 (1) of the Draft RTS. We also do not understand to which step in an EMV transaction the phrase "*[…] that is accepted only once by the payment services provider […]*" in Article 1 (1) of the Draft RTS refers to. EBA should therefore clarify the SCA requirements with regard to terminal initiated pull-transactions.

In any event, we would appreciate a clarification of the term "authentication code" in Article 1 (1) and (2) of the Draft RTS since the exact requirements remain unclear. In addition, it should be considered whether there is actually a need to require the generating of an authentication code as this requirement limits technology neutrality. Furthermore, we believe that the SCA as provided for in Article 1 (1) and (2) of the Draft RTS are designed to apply to browser-based internet transaction (i.e. push-transaction) but do not take into account other technological environments or payment methods where electronic payment transactions are initiated differently. For the sake of technology neutrality, the Draft RTS should reflect all present and future scenarios where electronic payment transactions may be initiated by or through the payee. The Draft RTS should address common acceptance scenarios of terminal initiated transactions should be considered. In particular, but not limited to, the following payment transactions should be appropriately reflected in the RTS:

- Contact-based vs. contactless terminal transaction;
- PIN vs. no authentication method;
- offline PIN vs. online PIN transaction;
- offline authorisation vs. online authorisation; and
- credit card numbers (Primary Account Number (**PAN**)) vs. Token as proof of possession.

We would like to highlight that PSD2 provides for payment transactions initiated by the payer but also for payment transactions initiated by or through the payee.

Article 1 (3) (e) (Rationale 22 (c))

We recommend deleting Article 1 (3) (e) Draft RTS. First of all, we have doubts whether this provision is in line with the general principle of data privacy and data protection. If implemented, Article 1 (3) (e) of the Draft RTS would require that payment service providers collect additional data on payment service users. In particular, Article 1 (3) (e) of the Draft RTS would require that payment service providers collect, store and process

additional data on the payment service user's spending pattern, what devices customers use and prepare a detailed risk-assessment of the payer and the devices used by a payer. As of the moment, the payment transaction records do not contain specific information on the spending pattern of customers (e.g. their purchases). Collection, storage and processing of these data would affect the payment service user's data privacy. In accordance with data privacy principles, this would normally require a legal basis that allows payment service providers to collect, store and process these customer data. We doubt that RTS which may only specify technical details (cf. Article 10 of the EBA-Regulation) are a sufficient statutory basis for such infringement of data privacy rights. Moreover, we doubt that such infringement can be justified in the light of the liability principles provided for in Article 73 and 74 of the PSD2. As a general rule, payment service users are not liable for unauthorised transactions. According to Article 74 (1) (b), the 50-EUR liability of payment service users only applies where the payment service user was able to detect the loss, theft or misappropriation of a payment instrument prior to a payment. Furthermore, the payment service provider generally bears the burden of proof for proper authorisation by the payment service user (cf. Article 72 of PSD2) and has to refund payment service users immediately in case of an unauthorised transaction (cf. Article 73 PSD2). Thus, payment service users will be generally not liable for unauthorised payments and only have a limited interest in technically excluding all cases of payment fraud. Against this background, it remains questionable whether there is sufficient justification for interfering with payment service users' data privacy rights by demanding a comprehensive transaction monitoring by payment service providers. In any event, we think that data privacy authorities should be consulted before making any such regulatory requirement that leads to the collection, storage and processing of additional sensitive personal data of payment service users.

Moreover, we do not think that payment service providers are in a position to effectively monitor spending patterns of customers since payment service providers usually do not have access to the contract details of the underlying transaction (e.g. an online purchase of goods). In particular, payees and their acquiring payment service provider should not be obliged to send additional data or information about the underlying transaction to the issuer.

Finally, we have doubts whether the requirements are actually covered by EBA's mandate to draft RTS. Since Regulatory Technical Standards may only specify technical details and may not exceed the mandate given in the primary legislation. Thus, EBA and the European Commission are bound by the mandate in Article 98 of PSD2.

Article 98 (1) (a) of PSD2 states that the RTS shall specify requirements of SCA referred to in Article 97 (1) and (2) of PSD2. The term "strong customer authentication" is legally defined in Article 4 no. 30 of PSD2 as an authentication based on the use of two or more elements categorized as knowledge, possession and inherence that are independent, in that the breach of one does not compromise the reliability of the others and is designed in such a way as to protect the confidentiality of the authentication data. The requirements listed in Article 1 (3) (e) of the Draft RTS are not authentication measures as these requirements concern additional safeguards by means of transaction monitoring but do not concern the actual authentication, i.e. verification of identity, of the payment service user as defined in Article 4 (29) of PSD2. In particular, these requirements do not concern the three SCA elements or their mutual independence. Thus, the mandate does not cover additional safeguards.

Article 98 (1) (b) – (d) of PSD2 do not provide for additional monitoring requirements either because Article 98 (1) (b) of PSD2 merely concerns exemptions from SCA, Article 98 (1) (c) of PSD2 merely concerns data protection and Article 98 (1) (d) of PSD2 merely concerns common and secure standards for communication.

In accordance with the mandate in Article 98 (1) of PSD2, the RTS should only specify technical standards as regards the actual SCA and verification of identity of customers but may not provide for mandatory additional safeguards.

In addition, we understand that according to Article 1 (3) (e) of the Draft RTS any electronic payment transaction that is not exempted pursuant to Article 8 of the Draft RTS has to be approved by the ASPSP. Currently, there are many different electronic payment methods which do not require the approval of the ASPSP, e.g. in case of low value offline transactions at toll stations. It should be acknowledged that from a functional perspective the authentication of a payer and the approval of a payment transaction are two distinct steps in a payment transaction. These steps are independent from each other. We understand that the SCA-requirements set forth in Article 97 (1) of PSD2 only concern the authentication of the payer but does not provide for specific requirements on how a payment transaction is to be approved.

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.**

We agree that the RTS should be technology neutral as to when the "dynamic linking" in accordance with Article 97 (2) of PSD2 takes place.

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?**

In our opinion, the principle of technology neutrality is not really served by the definitions in Articles 3, 4 and 5. Besides that, we have also concerns regarding Articles 6 and 7 of the Draft RTS which we will also discuss in this section.

First of all, Articles 3 (1), 4 (1) and 5 (1) define a minimum standard ("including, but not limited to") rather than technology neutral requirements. Language like "including, but not limited to" is typical for catch-all clauses in statues or contractual provisions but do not provide for a technology neutral definition of requirements. We do not think that this language serves the principle of technology neutrality. In addition, we have doubts whether the use of catch-all clauses is in line with the purpose of Regulatory Technical Standards which is to specify technical details. We do not think that catch-all terms should be generally used in this context. Instead, technology neutral RTS should define an abstract outcome which may be further clarified by defining a non-exhaustive list of examples.

Moreover, we think that there is a real need for a comprehensive list of legal definitions. The Draft RTS use plenty of terminology which is far from self-explaining (e.g. "temper-

resistant"; "information entropy"). For the sake of legal clarity, clear definitions should be prepared by EBA as is usual in EU legislation.

As regards Article 6 of the Draft RTS, we generally appreciate that EBA sees room for the use of a single multipurpose device for SCA. However, we do not agree with the measures defined in Article 6 (3) of the Draft RTS because the measures defined as minimum standard ("including, but not limited to") are not technology neutral and are unlikely to be practically implementable. It is questionable whether there are proportionate measures available to exclude that the software or the device has not been altered by the payer or a third party. We fear that Article 6 of the Draft RTS effectively excludes the future use of mobile devices in payments. We do not think that this outcome is proportionate or desirable. Besides that, we generally object to the idea that the payment service provider is considered to be responsible for the safe use of the payer's device and in particular for changes made by the payer to the payer's own device. We understand that Article 6 (3) (b) PSD2 requires payment service providers to ensure that payers have not performed so-called "jailbreaks" on their devices. Changes made by the payer to the payer's own device are clearly in the sphere of risk of the payer. It should be noted that, as Recital 69 to PSD2 and Article 69 (1) PSD2 show, payment service users are required to protect their security credentials. Payment service users are liable if they fail to protect their payment credentials or compromise their security with gross negligence. Against this background, holding payment service providers responsible for the payment user's own actions that may compromise the authentication procedure is a major change of policy. Such change of policy falls within the prerogative of European legislators and may not be dealt with in delegated acts such as regulatory technical standards. It is therefore questionable whether Article 6 (3) (b) of the Draft RTS is in line with Article 10 of the EBA-Regulation.

Regarding Article 7 of the Draft RTS, we have similar concerns. Article 98 (1) of PSD2 provides for a mandate to develop technical details on the SCA procedure. However, this does not include auditing requirements since auditing requirements are generally not a technical detail but part of the wider supervision of payment service providers. We therefore doubt that Article 98 (1) of PSD2 covers rules on auditing and recommend deleting Article 7 of the Draft RTS.

In addition, we regret that EBA has not specifically included questions relating to Article 6 and 7 of the Draft RTS. Without specific questions – or at least a field for general comments – the public may be discouraged from commenting on these draft provisions. In our opinion, broad public feedback on Article 6 is needed since the use of mobile devices for SCA and app solutions is likely to be a key driver for the future of payments and the digital economy in general. Thus, Article 6 of the Draft RTS may shape the European payment landscape for the years to come. Yet, it is to fear that not all market participants felt that they could comment on Article 6 of the Draft RTS or EBA's reasoning regarding multipurpose devices.

Part II – Exemptions from Strong Customer Authentication

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?**

We do not agree with EBA's reasoning on the exemptions from the application of Article 97 of PSD2 and the exemptions listed in Article 8 of the Draft RTS because we do

not think that the exemptions are coherent. The Draft RTS do not reflect a transaction risk-based approach.

General Considerations (Rationale 37 – 39)

In Rationale 37 – 39 EBA cites part of the Recitals 95 and 96 to PSD2 to base its reasoning on. However, EBA does not fully take into account Recitals 95 and 96 to PSD2. In order to avoid the impression that the non-quoted parts of Recitals 95 and 96 were left out of EBA's reasoning, we recommend also including language on the remaining part of Recitals 95 and 96 to PSD2. In particular, we would appreciate it if EBA also addressed Recital 95 to PSD2 which states that

> *"[t]here does not seem to be a need to guarantee the same level of protection to payment transactions [i.e. SCA] initiated and executed with modalities other than the use of electronic platforms or devices, such as paper-based payment transactions, mail orders or telephone orders."*

These transaction modalities are a question of scope of SCA, but we think that European legislators' reasoning should also be taken into account when discussing possible exemptions from SCA.

Acquirers and merchants should be allowed to apply exemptions (Rationale 41)

We strongly disagree with EBA's view that only the payment service provider of the payer shall be allowed to apply exemptions. First of all, there is no legal indication in Article 97 (1) or Article 98 of PSD2 or any other provision of PSD2 that indicates that acquirers or merchants may not apply exemptions from SCA. Please note that we are generally of the opinion that SCA should not be obligatory for payees and their payment service providers (see our answers to Q1).

When European legislators enacted PSD2, they did so in the light of the EBA Guidelines on the security of internet payments (EBA GL/2014/12). European legislators have provided for a broader scope and additional requirements for SCA in Article 97 and 98 of PSD2 but they did not limit who may apply exemptions from SCA. Article 98 (1) (b) is therefore neutrally phrased and simply refers to exemptions. We do not think that European legislators had in mind a policy change as discussed in Rationale 41 of EBA's Consultation paper but wanted to provide for a level-playing field between different payment service providers. Furthermore, Article 98 (3) (a) of PSD2 refers to the transactional risk of the services provided. The wording "services provided" clearly refers to the underlying transaction. Only merchants have access to this kind of information. Hence, they were clearly intended to be allowed to apply exemptions from SCA in accordance with Article 98 (3) (a) of PSD2.

In addition, we do not think that there is a compelling reason why only the payer's payment service provider may apply exemptions from SCA. Quite to the contrary, it will be often the payee and the payee's payment service provider who can best decide whether an exemption applies to a specific transaction. The payer's payment service provider only has limited access to transaction data besides the data for the actual execution of a payment transaction (e.g. recipient, payment amount) but generally has no information about the underlying transaction. Therefore, the payer's payment service provider can generally not decide whether a transaction is of low-risk. The payee and the payee's payment service provider on the other hand are ultimately liable for unauthorised non-

SCA-authorised transaction in accordance with Article 74 (2) of PSD2 and thus have a genuine interest in limiting the risk of transactions. Only the payee has full knowledge of the underlying transaction and can therefore decide whether a transaction can be considered to be low-risk even before initiating a payment transaction. This is particularly true since the risk of a transaction not only depends on the value of the transaction but also on the purchased goods and services. We do not think that sharing detailed information about the goods and services purchased with the issuer is in line with European data protection and data privacy principles.

Cards scheme rules already include a "liability shift" like Article 74 (2) of PSD2 and acquiring payment service providers are liable vis-à-vis the issuers (who are themselves liable vis-à-vis the payers) for transactions which were not authenticated by using 3DS if it later turns out that the transaction was in fact unauthorised. Nevertheless, payees and acquiring payment service providers process payments without requesting SCA from the issuer for low risk transactions because empirical evidence demonstrates that risk prevention systems of payees and their payment service providers effectively detect fraudulent activity and acquirers – in their own financial interest – take all necessary care to limit fraud losses and chargeback rates.

This is exactly the reason why Guideline 7.5 of the EBA Guidelines states that acquirers and merchants may apply alternative authentication measures for pre-defined categories of low-risk transactions, e.g. based on a transaction risk analysis or involving low-value payment instruments. We do not see any reason why allowing payees and their payment service providers to apply SCA would compromise the security of payment transactions. Quite to the contrary, the same reasons why Guideline 7.5 of the EBA Guidelines was first introduced still apply. The EBA-Guidelines came only recently into force and there is currently no empirical evidence that indicates that Guideline 7.5 compromises payment security. Thus, there is no reason to provide for stricter SCA requirements and a narrower scope of exemptions. In the light of the legal principle of proportionality, we therefore think that EBA should include a provision similar to Guideline 7.5 in the RTS.

In addition, we believe that most fraud occurs due to inappropriate application of current authentication procedures rather than due to transactions at low risk merchants where merchant authenticated the customer by alternative means. Accordingly, the obligation to ask the issuer for authentication for every transaction will prevent only a marginal share of fraud; yet will come at considerably higher costs for payees (and eventually payers). We understand that the purpose of Regulation (EU) No. 751/2015 is to make electronic payment transactions more cost-efficient. The Draft RTS are likely to have the exact opposite result. In this context, we would again like to stress that RTS may not include changes of policy (cf. Article 10 of EBA-Regulation).

We think that merchants should be allowed to apply exemptions because merchants often use sophisticated fraud prevention measures which are effective in combatting payment fraud. Currently merchants, so-called payment gateways (technical service providers for online payments) and acquirers use fraud prevention systems which typically score each transaction to control the processing based on the score. Obviously, each of the parties involved make use of different sets of data and control different steps in the payment process.

In the first step, the merchant system decides – based on the score – which payment methods are offered to the customer at all. Merchants systems have most rich data at

disposal as they can use methods like device fingerprinting, behavioural analytics and other data which are drawn from the interaction during the shopping session. Before starting the payment process, merchants have all data from the customer and the sale available. For instance, the likelihood for fraud may not only depend on the value of the transaction but on the content of the cart as well. Accordingly merchants are in the best position to assess the risk of electronic payment transactions. Large e-tailers employ highly sophisticated systems and expert teams who maintain the risk systems and handle suspicious cases. These services are also offered to third parties as an outsourced service. Once the merchants risk system decided which payment methods are offered and the customer has made his choice the transaction is handed over to the "gateway".

Gateways collect data from a large number of transactions from many merchants. These data allow for statistical analysis to detect fraud patterns. Risk control systems assign a score to each transaction which reflects the risk of fraud. In addition there are rule based systems employed which control further processing based on the risk score. Whereas low risk transactions are processed without SCA, for more risky transactions SCA is requested from the issuer. In a posteriori evaluation the accuracy of rules are assessed against fraud prevented, false positives and transaction aborts through customers (due to burdensome SCA). Rules are regularly updated accordingly.

Finally acquirers check the risk which is involved with a transaction. Acquirers may in addition to the risk prevention measures of the gateway detect fraudulent behaviour across all sales channels. This provides for a comprehensive multi-level fraud prevention system that exceeds the capabilities of individual account service payment providers or issuers.

Based on their own fraud prevention measures, merchants can make a risk-based and cost-efficient decision whether to apply SCA or not (cf. Article 74 (2) of PSD2). If merchants were to be required to support SCA in every single transaction (and pay the costs of SCA), they would no longer have any incentive to provide for own fraud prevention measures because merchants will want to avoid paying for SCA and their own fraud prevention systems. We therefore think that requiring merchants to support SCA in every single transaction hampers innovation and competition because merchants can no longer make a cost-based decision whether they want to rely on the SCA provided (and charged) by the issuer or whether they want to develop and use their own fraud prevention mechanism (at the risk of ultimate liability for unauthorised payment transactions in accordance with Article 74 (2) of PSD2) or want to purchase third-party fraud prevention solutions. The outcome would not be the best practical and cost-efficient solution but the solution implemented by individual issuers who may not have an incentive to develop new technology as merchants and acquirers are legally obliged to use (and eventually pay for) the issuer's technology.

Guideline 7.5 of the EBA-Guidelines promotes innovation and competition because merchants can make a deliberate choice how to address the risk of payment fraud and incentivized to develop new cost-efficient means of fraud protection. We strongly urge EBA not to interfere with technical innovation and competition, but to provide for an open regulatory framework that promotes cost-efficient and innovative authentication solutions.

Given the clear allocation of risk and liability under the PSD2 framework, in particular according to Article 74 (2) of PSD2, we think that, as long as the measures based on a transaction-risk analysis prove successful through low fraud rates and a very limited

number of chargebacks, the current SCA requirements under Guideline 7.5 of the EBA Guidelines allocates risk appropriately.

Distinction between Article 8 (1) and (2) of the Draft RTS is artificial and misleading (Rationale 47, Article 8 of the Draft RTS)

In Rationale 47, EBA states that there should be a differentiation between exemptions from Article 97 (1) and (2) of PSD2, i.e. exemptions from the general SCA requirement and exemptions from the additional dynamic linking requirement pursuant to Article 97 (2) of PSD2. Consequently, EBA provides for two exemptions pursuant Article 8 (1) and (2) of the Draft RTS. Thus, Article 8 (1) of the Draft RTS may be interpreted to fully exempt the transactions listed from the SCA requirements, whereas Article 8 (2) of the Draft RTS may be interpreted to only contain an exemption from the dynamic linking requirement. As a consequence, only account access without display of sensitive payment data and contactless electronic transactions within the 50/150 EUR-thresholds would be fully exempted from SCA according to Article 8 (1) (a) and (b) of the Draft RTS. Whitelisting, bulk payments, transactions where the payer and the payee are identical and accounts are held with the same payment service provider, and remote electronic payment transactions where the 10/100 EUR-threshold are met would be only exempted from the dynamic linking requirements pursuant to Article 8 (2) of the Draft RTS.

We do not think that this was the interpretation intended by EBA because the exemptions pursuant to Article 8 (2) of the Draft RTS all contain language that shows that the exemptions are in fact full exemptions and not just exemptions from the dynamic linking requirement. For instance, Article 8 (2) (a) of the Draft RTS on whitelisting states in subparagraph 2 that

> *"[t]he application of strong customer authentication [Please note: not just dynamic linking!] shall not be exempted where the payer creates for the first time or subsequently amends the list of trusted beneficiaries with its account servicing payment service provider."*

This demonstrates that the exemptions listed in Article 8 (2) are in fact full exemptions from SCA. After all,it would make little sense if the exemptions only applied to Article 97 (2) of PSD2 and the dynamic linking requirement.

Still, we would appreciate it if EBA changed the proposed wording of Article 8 of the Draft RTS to avoid misunderstandings and to ensure legal certainty. We therefore recommend clarifying that the transactions listed in Article 8 of PSD2 are exempted from both Article 97 (1) and (2) of PSD2.

General exemption for low-value payment instruments (Rationale 51, 52; Article 8 (1) and (2) of PSD2).

We generally share EBA's understanding that an exemption for low-value payment instruments is necessary to provide for user-friendly and innovative payment methods. However, we do not understand why EBA sees a need to limit the exemption to contactless payment methods because there is no convincing reason for differentiating between contactless and contact-based payment methods. To start with, the risk-profile of low-value payment transactions at the point of sale is the same, irrespective of whether a traditional acceptance technology (e.g. a payment card) or a contactless acceptance technology (e.g. NFC-functionality of a smartphone) is used. For instance, it does not

make any difference whether tolls, public transport etc. are paid for by means of a contactless payment instrument or by means of a payment card. Limiting the low-value payment instrument exemption to contactless payment instruments would mean to ignore the mandate to ensure technology neutrality as set forth in Article 98 (2) (c) of PSD2. We are concerned that the result would be detrimental to consumers and businesses in the European Union. If SCA were required for every payment made with contact-based acceptance of a payment card at a toll station, long queues would be inevitable as – unlike today – every customer would have to enter his or her PIN code. We do not think that this outcome is desirable for European consumers and businesses. Moreover, low-value payment instruments, such as the German GeldKarte (an easy to use e-money product available to customers of most German Banks and mostly used for micro-payments such as for public transport or at parking lots) and other wallet solutions, would become obsolete if SCA were to apply to all card acceptance technologies. This would greatly affect innovation in the payment sectors. We do not think that it is in the interest of European customers if convenient payment solutions used for low-value transaction are abolished. This outcome would be the exact opposite of the European Union's aim to increase the acceptance of electronic payments in the European Union or as Recital 9 to Regulation (EU) No. 751/2014 states:

> *"To enable the internal market to function effectively, the use of electronic payments should be promoted and facilitated to the benefit of merchants and consumers. Cards and other electronic payments can be used in a more versatile manner, including possibilities to pay online in order to take advantage of the internal market and e-commerce, whilst electronic payments also provide merchants with potentially secure payments. Card-based payment transactions instead of payments in cash could therefore be beneficial for merchants and consumers, provided that the fees for the use of the payment card schemes are set at an economically efficient level, whilst contributing to fair competition, innovation and market entry of new operators."*

We believe that RTS should take into account that SCA has to be proportionate and has to appropriately balance the risks and benefits of payment instruments. This being said, transaction risks and the costs and burdens of SCA must be balanced to provide for a practical and cost-efficient solution. Only a general exemption for all low-value electronic payment transactions provides for user-friendly and innovative payment methods. Against this background, we strongly recommend including a general exemption for all low-value electronic payment transactions.

Besides that, we recommend clarifying that SCA and the exemptions pursuant to Article 8 (1) and (2) of the Draft RTS have to be applied in accordance with Article 63 (1) of PSD2. Article 63 (1) of PSD2 provides for derogations for low-value payment instruments and electronic money. For instance, a payment service provider and a payment service user may agree that certain provisions do not apply to low-value payment instruments that cannot be blocked or prevented from further use (cf. Article 63 (1) (a) of PSD2) or that are used anonymously or the payment service provider is not in a position for other reasons which are intrinsic to the payment instrument to prove that a payment transaction was authorised (cf. Article 63 (1) (b) of PSD2). Article 63 (1) (b) of PSD2 shows that European legislators payment instruments generally considered these payment instruments to be possible if the payment instrument is a low-value payment instrument. This legislative decision is binding and therefore must be reflected in the RTS (cf. Article 10 EBA-Regulation).

Thresholds for low-value payment transactions (Article 8 (1) and (2) of PSD2)

The proposed thresholds for low-value payment transactions in Article 8 (1) and (2) of PSD2 do not match the low-value payment instrument definition in Article 63 of PSD2. We recommend aligning the RTS with the general definition of low-value payment instruments is defined in Article 63 of PSD2. The thresholds defined in Article 63 (1) of PSD2 are as follows:

(a) a single transaction may not exceed the payment amount of 30 EUR or

(b) the payment instrument has to have a maximum spending limit of 150 EUR or

(c) the payment instrument does not store funds exceeding 150 EUR at any time.

In our opinion, the RTS should reflect the European legislators' decisions to apply these thresholds. Moreover, the RTS should also reflect different national thresholds set in accordance with Article 63 (2) of PSD2.

Applying the same thresholds as in Article 63 of PSD2 would provide for a coherent application of the various exemptions for low-value payment instruments. Besides that, we think that application of the general thresholds for low-value payment instruments in accordance with Article 63 of PSD2 is mandatory since the RTS are delimited by PSD2 and therefore have to mirror the requirements, exemptions and thresholds in PSD2 as Article 63 of PSD2 clearly provides for certain exemptions for low-value payment instruments. The European and national legislator's decisions to apply certain threshold should be taken into account by EBA.

In any event, EBA should specify the cumulative threshold of 150 EUR and 100 EUR, respectively. The Article 8 (1) (b) (ii) and Article 8 (2) (d (ii) of the Draft RTS simply state

> *"the cumulative amount of previous […] payment transactions […] without application of strong customer authentication does not exceed [150 EUR/100 EUR]."*

Thus, it remains unclear when and how long the cumulative threshold applies. It can either apply only once (which seems implausible and unpractical) or may apply until the payer initiates a payment transactions using SCA or may apply on a monthly basis.

In addition, it may be not feasible to implement the cumulative threshold in practice because many low-value payments are made in situations when even entering the payers' PIN can be unpractical, e.g. at toll stations, and many payment terminals used for accepting low-value payment instruments do not provide for SCA-compliant authentication. The mandatory nature of the exemption is too prescriptive and does not take into account the context of different countries. The 50EUR per transaction limit is not controlled by the card, but by the terminal, the applicability of PSD2 to one-leg transaction will cause interoperability issues, as the exemption cannot be implemented successfully in all countries.

Moreover, the 150 EUR cumulative limit cannot be implemented without costly development and changes. Currently, cards do not have a way to keep track of the amount of cumulative transaction. Thus, the limit would force a card to go online to reset the contactless limit. The counters that are in place can count the numbers of transaction,

but cannot force the contactless card to go online. Thus, there is a risk that the the 150 EUR limit is not observed in every transaction.

We suggest to the EBA to keep the exemption but to leave the limits to the member state.

Whitelisting

Article 8 (2) (a) of the Draft RTS contains an exemption for transactions with pre-approved payees (whitelisting). However, the wording of the exemptions indicates that whitelisting is only available to credit transfers but not to credit or debit card payments or e-mandate direct debits. In our opinion, there is no valid reason to limit whitelisting to credit transfers as the reasons for exempting a pre-approved list of payees also apply to credit or debit card transactions and e-mandate direct debits. We therefore recommend amending Article 8 (2) (a) of the Draft RTS to include all payment transactions and in particular to remove the restriction to credit transfers in accordance with a business and technology neutral approach as required by Article 98 (2) (c) of PSD2.

There should be transaction-risk-based exemptions (Rationale 54)

We appreciate that EBA in principle acknowledges the transaction-risk-based approach as required by Article 98 (1) (b) and (3) of PSD2. However, we do not think that EBA's reasoning and the Draft RTS fully reflect the requirement of transaction-risk-based exemptions. Pursuant to Article 98 (3) (a) of PSD2, exemptions from the SCA shall be based on the level of risk involved in the service provided. Hence, PSD2 clearly requires EBA to base its exemptions on transactional risk. By referring to the "services provided", Article 98 (3) (a) of PSD2 also demonstrates that the underlying transactions have to be considered when defining risk-appropriate exemptions. However, there is currently no reference to the underlying transaction in the EBA's reasoning or the Draft RTS. In line with Article 98 (3) (a) of PSD2, these considerations should be taken into account for the final RTS.

Moreover, the reference to the underlying transaction shows that European legislators had in mind that payees and their payment service providers may apply exemptions. Only the payee has knowledge of the risk-profile of the underlying transaction. The payer's payment service provider has no access to this kind of information since the payer's payment service provider only receives the payment data but no details on the underlying transaction.

Finally, EBA has not sufficiently taken into account risk-based considerations. In Rationale 54, EBA states that they were not able to identify definite criteria for transaction-risk based exemptions. In our opinion, this is insufficient to fulfil the EBA's mandate in accordance with Article 98 (3) of PSD2 which unequivocally calls for such exemption. After all, EBA is not required to define definite criteria for such exemption. As Guidelines 7.5 of the EBA-Guidelines shows, it is perfectly possible to provide for technology neutral exemptions based on a transaction-risk based approach by allowing payees and/or their payment service providers to decide whether the risk of an underlying transaction is sufficiently low to not apply SCA.

We do not understand why this option has been deleted in the Draft RTS because we do not see any reason to deviate from Guideline 7.5 of the EBA Guidelines in this respect. There is no empirical evidence that Guideline 7.5 of the EBA Guidelines affects the security of electronic payment transactions. Since the deletion of a transaction-risk-based

approach is a major change, we would have at least expected to a detailed explanation why Guideline 7.5 of the EBA Guidelines was not included in the Draft RTS.

Exemption from SCA for transactions otherwise exempted from PSD2

In accordance with Article 98 (2) (b) and (3) (a) of PSD2, the RTS should include exemptions from SCA for payment transactions that fall under Article 3 of PSD2 in order to provide for a level-playing field between regulated and non-regulated payment service providers.

Article 3 of PSD2 contains a list of exemptions from PSD2. The purpose of this provision is to exempt those payment services from regulation which do not require regulation and supervision in the eyes of European legislators. For instance, Article 3 (k) (ii) of PSD2 provides for an exemption for so-called limited networks because a payment instrument used to pay for a very limited range of goods and services has a different risk-profile than open-loop cards and poses a low-risk with regard to payment fraud or other misappropriation. European legislators have already made the legislative decision that this kind of transaction is to be considered low-risk by exempting the transactions from PSD2. As a consequence, service providers that offer limited-network instruments in accordance with Article 3 (k) (ii) of PSD2 do not have to adhere to the SCA standards as defined in Article 97 and 98 of PSD2 and the Draft RTS.

However, if a regulated payment service provider issues limited-network instruments, the payment transactions will nevertheless become subject to SCA requirements as Article 97 (1) of PSD2 obliges the payment service provider to apply SCA for every transaction unless an exemption pursuant to Article 98 of PSD2 and the RTS applies.

We do not think that this is in line with the level-playing field intended by European legislators since non-regulated service provider would gain an unjustified competitive advantage over licensed payment service providers when competing on the market for limited-network instruments.

In our opinion, it is perfectly possible to generally exempt the transactions listed in Article 3 of PSD2 and executed by regulated payment service provider from SCA. Article 98 (2) (b) and (3) of PSD2 clearly call for a transaction risk based approach. European legislators have already made a legislative decision that the transactions listed in Article 3 of PSD2 are considered to be low-risk as European legislators saw no need to regulate these transactions altogether. Therefore, there is no reason to require SCA for this kind of transaction where such transactions are offered by licensed payment service providers because the only reason why SCA applies in the first place is that the issuer is a licensed payment service provider.

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?**

We do not think that the proposed list of exemptions is coherent and meets the need of European consumers and business. Please refer to our answers to Q4 which also includes our comments on the list of exemptions in detail.

Part III –Protection of Confidentiality and Integrity of Personalised Security Credentials

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?**

We agree with EBA that a principle-based approach should be applied. Regarding the term "personalised security credentials", we propose that EBA shares its understanding to help market participants to correctly implement the requirements regarding personalised security credentials. The definition in Article 4 no. 31 PSD2 states that personalised security credentials are features the payment service provider provides to the payment service user for the purpose of authentication. This definition is relatively vague. We would therefore appreciate it if the EBA shared its understanding of the term, e.g. by providing a non-exhausting list of examples. We believe that such list would not compromise technology neutrality as it does not exclude other technical solutions and measures. A non-exhaustive list would help to ensure that all relevant payment data are treated properly in accordance with Chapter 3 of the Draft RTS.

In this context, we would also like to again raise the issue of data protection. Protection of confidentiality also concerns the payment service users' other personal data. We believe that the current Draft RTS should be revised to better address data privacy and data protection. In particular, Article 1 (3) (e) of the Draft RTS should be deleted since the additional requirements listed as minimum standard by EBA interfere with the payment service users' rights to data protection and data privacy (cf. our answers to Q1).

Part IV –Common and Secure Open Standards for Communication

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?**

We generally share EBA's understanding. Yet, we propose to revise the Draft RTS to provide for a more coherent use of terminology. We have noticed that the terms "payer", "payment service user", "payee" and "merchant" are not consistently used throughout the document. For instance, the term "merchant" is only used in Article 18 of the Draft RTS without apparent reason why the term "merchant" rather than "payee" is used.

In addition, EBA should clarify whether the term "payer's device" used in Article 17 of the Draft RTS merely refers to devices (e.g. smartphones or tablets) or also applies to payment instruments such as payment cards.

As regards Article 18 of the Draft RTS, the first sentence should be clarified to only refer to "all electronic payment transactions" since SCA only applies to electronic payment transactions (cf. Recital 95 to the Draft RTS). Article 18 (b) should read "all **necessary** transaction data" (instead of "all **relevant** transaction data") as we consider the term "relevant" as rather vague.

In this context, we would like to again highlight that the use of legal definition of the terms used in the Draft RTS would greatly improve legal certainty and coherent use of terminology.

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?**

We appreciate EBA's approach to remain technology neutral. For the sake of technology neutrality, ISO 20022 should not be a binding technical standard as currently required by Article 19 (3) of the Draft RTS. ISO 20022 should be listed as a non-binding example and the Draft RTS should refer to common market standards. This would allow for innovation and at the same time provide for interoperability.

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?**

Although eIDAS generally provides for secure and reliable certificates, we nevertheless recommend remaining technology neutral and not making eIDAS a sole and binding standard. We think that is not predictable until when eIDAS certificates will be available in practice and how eIDAS will be accepted in the market. The Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures shows that a legislative framework does not necessarily translate into widespread use of a certain standard or technology. Therefore, EBA should rather define the necessary quality of certificates rather than specific certificates. eIDAS could be listed as a non-binding example of an eligible certification framework. Such approach would provide for legal certainty while at the same time certification in accordance with the RTS would not depend on the success of eIDAS.

Please do not hesitate to contact us if you have questions or wish to discuss any of these comments further.

Yours sincerely,

Stephan Neuberger
Sprecher

Dr. Richard Reimer
Partner / Hogan Lovells International LLP