Visa response EBA public consultation on the draft RTS on Strong Customer Authentication

Background

The revised Payment Services Directive (PSD2) mandates to perform Strong Customer Authentication (SCA) for all electronic payments. PSD2 also includes a mandate to the EBA to draft the Regulatory Technical Standards (RTS) clarifying the requirements of SCA and possible exemption to the mandate to perform SCA.

On the 12 August the EBA published the draft RTS for public consultation. The draft RTS are available here: https://www.eba.europa.eu/documents/10180/1548183/Consultation+Paper+on+draft+RTS+on+SCA+and+CSC+%28EBA-CP-2016-11%29.pdf/679054cf-474d-443c-9ca6-c60d56246bd1

Here below, you can find the contribution of Visa. Please note that Visa responded only to selected questions impacting directly or indirectly payment cards.

Visa's submission

Q1: 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?

Visa shares the objective of the revised Payment Services Directive (PSD2) to promote electronic payment transactions and prevent fraud. Visa – along with the entire European payments industry - invested heavily in adopting chip and PIN technology (EMV standards). For remote payments, Visa created the standard 3D Secure used for electronic commerce payments that enable Strong Customer Authentication (SCA) in the sense of PSD2.

Visa made the standard 3D Secure available to the industry which has been widely adopted. Now 3D Secure is maintained by the global organisation EMV Co. Currently, EMV Co is developing 3D Secure 2.0, to improve the use of authentication in new forms of the digital space (e.g. mobile payments).

In addition, Visa promotes the use of 3D Secure through the platform *Verified by Visa* that provides the necessary infrastructure for payment service providers (and the final users) to secure remote payment transactions.

Visa welcomes the efforts of the EU legislator to improve security of electronic payments, including face-to-face and remote payments and welcomes the proposal of the EBA to translate the principles set forth in the PSD2 into applicable requirements. However, as explained in more detail in our response Visa also has significant concerns in relation to certain aspects of the proposed approach, especially in relation to the exemptions to the mandate to perform SCA.

Visa would like to comment on various aspects of the rationale accompanying the draft Regulatory Technical Standards (the draft RTS) as well as the proposed provisions published for consultation by the EBA.

1. Scope of the mandate to perform Strong Customer Authentication (SCA)

a) Paper-based payment transactions, mail orders or telephone orders

Visa agrees that the mandate to perform SCA should only apply to payments initiated through "*electronic platforms or devices*". Recitals 95 of PSD2 clarifies that "*Paper-based payment transactions, mail orders and telephone orders*" do not need the "*same level of protection*" and, thus should not be subject to the mandate to perform SCA. Visa believes that this clarification should be included in the draft RTS.

b) Payments initiated by the payee

Visa welcomes the clarification included in paragraph 17 of the rationale. This paragraph states that the mandate to perform SCA does not apply to "*payments initiated by the payee only, such as direct debits*".

Visa would like to remind the EBA that card-based payment instruments can also be used by the payees to initiate payments. This is even recognised in PSD2. For example, Article 75 of the PSD2 refers to "*payment transaction is initiated by or through the payee in the context of a card-based payment transaction*".

In fact, payment cards are widely used for standing instructions where the payee pulls transactions from a payment card according to the conditions agreed with the payer. This would be the case for subscriptions to services, such as multimedia platforms on the internet or payment of utilities; payments in instalments; or top-up of a closed loop account (e.g. a card usable for public transport services).

In addition to standing instructions, there are a number of cases where payees pull payments from a payment card according to the conditions agreed between the payer and the payee, for example "no shows" at hotels.

In order not to hamper use of payment cards as described above, Visa would request the EBA to include a recital in the draft RTS clarifying that "payments initiated by the payee, that can also include card-based payment transactions, are not subject to the mandate to perform SCA".

Visa would also like to suggest a clarification in the draft RTS in relation to direct debits. According to the Q&A document of the European Commission on the first PSD *"[a] transaction initiated through the payee is a transaction which is initiated by the payer through the payee*". In some payment systems, the payer will initiate a payment (through a set of credentials in remote transactions or through a physical device – card or other – at a point of sale) for an individual payment that will trigger a one-off direct debit. Visa believes that the draft RTS should clarify that, in these cases - in line with paragraph 18 of the draft RTS - SCA should be required.

2. Liability of the payee and the payee's PSP

Visa notes the following statement included in para. 19(b) of the rationale "*The EBA understands that Article 74(2) of PSD2, which allows the payee or the payee's PSP the option not to accept SCA, only applies during the* *short period between the application of PSD2 (13 January 2018) and the application date of the RTS under consultation (in October 2018 the earliest)."*

Visa does not agree with this interpretation. In the opinion of Visa, such a statement has no legal basis under PSD2. In addition, Visa questions whether it is within the EBA mandate to engage in a wider interpretation of PSD2 in the context of SCA.

Visa has sought external counsel from the law firm Baker & McKenzie in this regard. In the opinion of our external counsels:

"It can be concluded from the foregoing that (i) the essential elements of legislative acts can never be subject to delegation (Article 290 TFEU), and that (ii) the EBA RTS are required to be technical, cannot imply strategic decision or policy choices and their content is delimited by the PSD2 (Article 10 EBA Regulation).

First of all, in the case at hand, Article 98 PSD2 clearly delimits EBA's competence to draft RTS with regard to Article 97(1) and (2) to "the requirements of the strong customer authentication" referred to in that article. Determining who is required to ensure that SCA is supported, i.e. acquirers/payees on top of issuers, is not a (technical) requirement of the SCA itself.

EBA can in any case not amend/supplement Article 74(2) PSD2, as it is not granted any competence to draft RTS with regard to that article.

Furthermore, it can be argued that these amendments of the PSD2 are not technical, but consider essential elements of the PSD2 and imply strategic decisions/policy choices."

During the public hearing on the draft RTS – held by the EBA in London on 23rd September – Visa noted that the European Commission stated that in case a payment service provider (PSP) had indications that the transaction benefiting from an exemption may be fraudulent, the PSP should do SCA "*because of the liability regime*". In the opinion of Visa, this statement further indicates that the liability regime set forth set forth in Article 74(2) cannot be deemed as transitory.

Visa would welcome a statement of the EBA withdrawing the clarification included in paragraph 19(b) of the rationale.

Also in relation to Article 74(2) of the PSD2, Visa disagrees with the approach taken by the EBA in paragraph 41 of the rationale explaining that payees and PSPs of the payees will not be able to adopt "*alternative methods of authentication*".

The draft RTS should reflect that the payee and the PSP of the payee should be able to adopt "*alternative methods of authentication for low-risk transactions*" in exchange of taking liability for unauthorised payment transactions. This is in line with paragraph 7.5 of the EBA Guidelines for the security of internet payments, as well as the original ECB/Eurosystem SecuRe Pay Recommendations, and Article 74(2) of the PSD2.

Visa would like to remind the EBA that the ability of payees and their PSPs to make a decision on the authentication of customers based on the risk of the payment is the basis of very successful business models that are boosting e-commerce in Europe (i.e. card on file or "one click" payments).

This is further explained in our response to question 4.

3. Global reach of the SCA mandate

At the public hearing on the draft RTS Visa asked about the interpretation of the mandate to perform SCA and the requirements for the so-called "one-leg transactions" (Article 2 of the PSD2, Scope).

The response was that, in case a European consumer wanted to purchase from a merchant outside the EU (acquired by a PSP established outside the EU) and SCA was not required, the obligation of the issuer of the card (the PSP of the payer) would be to decline the transaction.

Visa does not agree with this interpretation and would like to highlight consequences, namely the discrimination of European consumers that may not be able to use their payment cards outside of the EU. For example, in the US and a number of countries of Latin America chip and PIN has not been implemented at the point of sale. In addition, European consumers will not be able to shop in electronic commerce merchants outside the EU. This would have a serious impact on international trade. For example, during the first quarter of 2016, 19 million Visa cards where used outside the EU/EEA.

In the opinion of Visa, in case the acquiring side of the transaction (payee and payee's PSP) is carried out outside the EU, it should not be deemed that the issuer of the payment card should decline a payment in case SCA is not supported or requested. Such an approach would go beyond the scope of PSD2.

On the contrary, the draft RTS should reflect that the responsibility of the issuer PSP is to implement SCA for all its cards and to strongly authenticate the customer "*on request of an acquiring PSP*". This is the reasonable approach, which is in line with paragraph 7.3.3 of the Assessment Guide for the Security of Internet Payments published by the ECB/Eurosystem in February 2014.

In relation to payees and payees' PSPs established in the EU, they should not be forced to support SCA for customers from outside the EU. It has to be taken into account that probably no other jurisdiction in the world would impose a legal obligation to provide SCA to payers according to the definition of PSD2.

Visa would like to remind the EBA that, as a global payment system, Visa has implemented global rules to protect the payers irrespective of the location of issuers, acquirers and payees. Accordingly, in order to better protect consumers, Visa established a liability regime ensuring that the PSP of the transaction that does not require SCA takes liability for unauthorised payment transactions. This ensures that consumers would always be protected, in line with Article 74(2) of the PSD2.

4. Characteristics of the "authentication code"

The draft RTS have introduced a new element in the authentication process. According to the draft RTS the combination of two or more factors based on possession, knowledge or inherence shall result in the generation of an "authentication code" to the payer's PSP that is only accepted once by the PSP for the same payment services user.

Article 1(2) of the draft RTS indicate that *"[t]he authentication code shall be characterized by security features including, but not limited to, algorithm specifications, length, information entropy and expiration time"*.

Visa believes that, in order to preserve innovation and respect the principle of technological neutrality, the RTS should not set an exhaustive list of features for the "authentication code". Accordingly, Visa would request the EBA to replace "shall" by "should".

For example, in the case of chip cards – which have a number of security features -, neither the chip nor the chip reader has a clock that allows an expiration time.

5. "Authentication code" and PINs

Article 1(3)(b) of the draft RTS set forth that SCA mechanism shall "*exclude that any of the elements of strong customer authentication can be identified as incorrect, where the authentication procedure has failed to generate an authentication code for the purposes of paragraph 1"*.

In a chip and PIN transaction it would be impossible to *"exclude that any of the elements of strong customer authentication can be identified as incorrect*", since the payer will always be informed that the PIN is not correct. In the opinion of Visa, this should be taken into account in the draft RTS for the convenience of the payer.

6. The "Authentication Code" and magnetic stripe transactions

Card-based payment transactions performed with a magnetic stripe do not allow the generation of such an "authentication code". Although Europe has fully implemented chip and PIN technology, magnetic stripe transactions still exist as a "fallback" solution in case the chip and/or the chip reader fail.

Visa believes that magnetic stripe transactions and signature as a valid factor of authentication have to be allowed under the RTS. This would be important for European consumers as a "fallback" mechanism to ensure that the payment can be initiated, but also for non-European consumers that do not have a chip card.

As explained in previous section 3, Visa does not believe that PSD2 or the draft RTS can impose on payees or their PSPs an obligation to refuse a transaction in case a payer's PSP (in this case, an issuer of a payment card established outside the EU) has provided the payer with a magnetic stripe card.

7. Sensitive payment data

Paragraph 49 of the rationale states that "*account numbers do not constitute sensitive payment data*". PSD2 defines sensitive payment data as data that can be used for fraud.

The card payments industry has always treated card numbers as "sensitive payment data" and the industry has self-regulated the protection of such numbers and has built the PCI data security standards.

In the opinion of Visa, "account numbers" have not been considered sensitive payment data so far, because they were used and transmitted through two trusted institutions (PSPs). However, new products and services (such as payment initiation services) would rely on account numbers. In addition, new payment services based on payment accounts could be developed not only for remote payments, but also for face-to-face payments using the account numbers to initiate payments at a point of sale in the physical environment.

In the opinion of Visa, expanding the use of account numbers (like IBANs) increases the risks associated to account numbers and, accordingly, it should be considered sensitive payment data and standards similar to PCI-DSS should be developed to foster for this.

Q2: 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.

1. Dynamic link to the amount and the payee

Visa supports the flexibility in respect of the interpretation of the dynamic link to the amount and the payee as explained in paragraph 24 of the rationale.

This flexibility is necessary for card-based payments where there is no standard way of identifying the payee across the industry (different from SEPA credit transfers and direct debits where the payee can be identified through the IBAN).

In this regard, Visa welcomes the clarification included in paragraph 25 of the rationale clarifying that *"[i]n any case, the authentication procedure should ensure that the payer is always made aware of the amount and payee of the transaction he is authorising and should be tamper-resistant to prevent any manipulation of the amount and of the payee during the initiation of the payment transaction so that any change to the amount or payee shall result in a change of the authentication code."*

Visa suggests that this flexible interpretation is reflected in the Recitals of the draft RTS.

2. Mobile payments and segregation of channels

Visa welcomes the clarification in paragraphs 30 and 31 of the rationale, indicating that the EBA is of the view that mobile devices could be used *"as authentication element as well as a device allowing the reading or storage of another authentication element"*.

In the opinion of Visa, such flexibility has to be reflected in the draft RTS and Article 2(2)(b) should be clarified.

Article 2(2)(b) sets forth that *"[t]he channel, device or mobile application through which the information linking the transaction to a specific amount and a specific payee is displayed shall be independent or segregated from the channel, device or mobile application used for initiating the electronic payment transaction."*

Visa would request a clarification in the draft RTS in relation to "*independent or segregated*", indicating that that different channels (mobile app versus SMS) or different mobile applications in the same mobile device would be considered compliant with the authentication requirements provided that the *"authentication procedure mitigates the inherent risks of the mobile device being compromised*".

In this regard, Visa would also welcome a clarification regarding what would be considered "*separated trusted execution environments*" in the sense of Article 6(3)(a) of the draft RTS.

3. Dynamic link for blocking of funds and transaction amount not known in advance

In relation to Article 2 paragraphs 3 and 4 of the draft RTS, Visa believes that the dynamic linking procedure needs more flexibility to reflect real-life scenarios, e.g. :

- Items may be ordered in a foreign currency and the settlement amount may vary in the cardholders currency
- A supermarket home delivery order differs as the goods selected are not available and the supermarket has permission from the consumer to substitute a slightly more expensive item.

In these situations the amounts settled need to differ from the amount contained in the SCA authentication.

Q3: 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?

Visa does not have any further comments on Articles 3, 4 and 5.

Q4: 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 mandate of the EBA in relation to SCA is clearly spelled out in Article 98 of the PSD2, setting forth that the draft RTS should specify the exemptions to the mandate to perform SCA based on: (i) the level of the risk involved in the service provided; (ii) the amount, the recurrence of the transaction or both; (iii) the payment channel used for the execution of the transaction.

In the opinion of Visa, in order to fulfil its legal mandate the EBA has to include exemptions in the draft RTS based on all three criteria included in Article 98 of the PSD2. Currently, the draft RTS only include exemptions based on amount and recurrence.

Visa is especially surprised about paragraph 54 of the rationale stating that "*the EBA was not able to identify which minimum set of information the RTS should require for such transaction risk analysis to be sufficiently reliable to allow a specific exemption from the application of SCA, while also ensuring a fair competition among all payment service providers. Against this background, the EBA has concluded for the Consultation Paper not to propose exemptions based on a transaction-risk analysis performed by the PSP.*"

Visa believes that the exemptions proposed in Article 8 of the draft RTS are primarily dedicated to payment instruments different from payment cards and are very much focused on "*maintain fair competition among all payment service providers*". This is reflected in paragraph 54 of the rationale and also in paragraph 44 where the EBA states that against the opinion of the majority of respondents - to the discussion paper on authentication published last December - the EBA took the view of "*several other respondents, in particular payment initiation services providers, expressed a strong support for a clear and limited list of exemptions*". In addition, paragraph 53 establishes a link – which, in the opinion of Visa, is not clearly reflected in PSD2 - between Article 97(4) of the PSD2 with the exemptions to the mandate to perform SCA and the obligation of no discrimination of ASPSP versus payment initiation and account information service providers.

Visa would like to remind the EBA that, along with maintaining fair competition between PSPs, Article 98 of PSD2 lists other objectives that need to be taken into account in the draft RTS and are not necessarily reflected in the text proposed, notably: "*ensure an appropriate level of security for payment service users and payment service providers, through the adoption of effective and risk-based requirements*"; "*ensure technology and business-model neutrality*"*; and, above all,* "*allow for the development of user-friendly, accessible and innovative means of payment*".

As further explained here below, Visa firmly believes that the draft RTS should include an exemption based on the risk involved in the service provided in line with Recital 96 of the PSD2: "*The security measures should be compatible with the level of risk involved in the payment service*".

1. The level of the risk involved in the service provided

Visa understands the difficulty of the task given to the EBA and agrees when the EBA indicates that there are important trade-offs between security and convenience when it comes to authentication methods. In order to avoid such trade-offs, the card payments industry has developed global innovative methods of authentication based on the analysis of the risks of the transaction.

This approach provides the right balance between security and convenience and eases electronic payments. In other words, this approach facilitates payments while preserving security, in line with the objectives of the EU Digital Single Market that promotes "*better access for consumers and business to online goods*".

The approach based on risk is not exclusive of the card payments industry, but a global trend for the financial industry, including their regulators and supervisors. For example, G20/OECD Task Force on Financial Consumer protection released in September 2014 the report "Effective approaches to support the implementation of the remaining G20/OECD high-level principles on financial consumer protection". Paragraph 33 of this report states that "*in order to be responsive, efficient and cost effective, financial* *consumer protection regulators and supervisors adopt a risk-based approach where resources are concentrated in areas of high risk to consumers, and is complemented by a problem-solving approach where regulators and supervisors can focus on harmful behaviours, and potential and/or emerging risks that lie within the mission and responsibility of the regulator/supervisor*".

As explained here below, the exemptions based on the risk of the transaction are essential to ensure the best consumer experience, to reduce friction on payments and to preserve innovation. Furthermore, in opinion of Visa, not allowing exemptions based on the risk of the transaction would hamper electronic payments in Europe, would damage electronic commerce and risks moving payments from the electronic space to cash or unregulated payment methods, such as virtual currencies.

According to the above, Visa would request the EBA to reconsider its position and include in the draft RTS: (i) an exemption for the issuer of the card (i.e. the payer's PSP) not to perform SCA depending on the risk of the transaction; and (ii) an exemption for the payee and the card acquirer of the payee (the payee's PSP) to "*adopt alternative methods of authentication for low-risk transactions*" in exchange of taking liability for the transaction.

a) <u>Exemption for the issuers (payer's PSP) or the "Risk Based Authentication"</u>

The way people pay really matters, especially in remote transactions. All parties have come to expect a quick, easy checkout process. As a result the industry has globally sought to remove friction from electronic payments and, at the same time, deploy a wide repertoire of risk management techniques. This is the so-called "Risk Based Authentication" (RBA).

The way RBA works is simple. For example, when an e-commerce transaction is attempted a series of instantaneous checks are performed. These may include device checks (for example, is this the same handset the consumer usually uses? Or the same browser? Do we recognise the IP address? Or the location?). They may also use behavioural checks (for example, does this consumer typically buy online? Do they typically make this type of purchase? Do they typically transact in this currency?). And, on the basis of these checks the PSPs will often be satisfied that a genuine consumer is conducting a legitimate transaction. This means that for routine, low-value or frequently occurring payments, SCA rarely needs to be invoked.

If, however, there is any element of doubt, SCA can be invoked, which provides an additional layer of security.

This selective, layered approach to SCA has benefits for all players:

- The speed, simplicity and convenience of the checkout process is improved – which translates to a better customer experience
- For higher-risk transactions, step-up authentication is invoked – which can bring a sense of reassurance to more cautious online shoppers

Irrespective of whether SCA is used, the consumer is always protected and never liable (unless gross negligence or fraudulent behaviour is proven) – a principle that has been applied by the card payment systems for years and that remains enshrined and even improved in the PSD2 that guarantees that unauthorised payment transactions will be refunded to payers within one business day.

RBA has proven to be effective. A useful case study is provided by the UK market where the main PSPs have been using RBA for the last few years experiencing benefits for all stakeholders:

- Cardholders: improved customer experience (85% reduction in checkout time)
- Merchants: better sales conversion (70% reduction in payment abandonment)
- Banks: Fraud and Costs reduction (0% increase in total fraud when compared to previous SCA solution; 85% fewer inbound calls relating to password resets)

When comparing the uptake of transaction authentication in the different European markets a strong correlation between transaction abandonment rate and authentication uptake is noted. In markets where the authentication experience is not optimised and fragmented e.g. Spain (abandonment rates 13.8%) the market share of e-commerce authenticated transaction is 15% of total e-commerce sales. Meanwhile in the UK where, thanks to RBA, the transaction abandonment is less than 2.5%, the share of e-commerce authenticated transaction is 60% of total sales.

Furthermore, Visa observed that independently of the SCA method used (SMS, Password, Bank credentials, etc.) when customer intervention is requested the abandonment rate is between three to five times higher than when authentication happens frictionless via RBA.

Accordingly, Visa strongly believes that the EBA should reconsider its position and include an exemption for the payer's PSPs based of the risk of the service provided for card-based payment transactions. Visa would like to propose the following addition to Article 8:

"Exemptions of transaction risk analysis should be allowed. The transaction risk analysis should be based on models which are:

(a) based at minimum on comprehensive real-time risk analysis taking into account should include, where possible:

(i)an adequate transaction history that evaluates the customer's typical spending and behavioural patterns ,

(ii) information about the customer device used and

(iii) a detailed risk profile of the payee and the payee's device ,

(b) proven to be efficient for fighting against fraud and assessed according to Article 7,

(c) continuously reviewed according to fraud rates and improved in order to address new fraud scenarios and new technological threats."

Visa understands that including a flexible provision for this exemption can be challenging, especially in terms of monitoring compliance. For this reason, Visa suggests that the EBA also includes in the draft RTS the principle of "assessment based on performance" of the PSP as part of the "*Review of strong customer* *authentication procedure"* mandated in Article 7 of the draft RTS. Accordingly, when the different PSPs self-assess or audit their authentication systems they could also evaluate the performance of the transactions authenticated through RBA (against the fraud levels of transactions authenticated with SCA). Similar levels of performance will prove that RBA is equally effective to fight against fraud.

b) Exemption for the payee and the PSP of the payee to adopt "alternative methods of authentication"

As outlined in the response to question 1, Visa does not agree neither with the interpretation of PSD2 included in paragraph 41 of the rationale stating that the EBA understands that "*the exemptions to SCA as defined in the RTS under consultation constitute a part of the authentication procedures performed by the payer's PSP (also referred as ASPSP) and should therefore be applied by the ASPSP only*"; nor with paragraph 19(b) of the rationale indicating that the liability regime of Article 74(2) of the PSD2 is only applicable in the transitional period between the entry into force of PSD2 and the applicability of the RTS.

Visa believes that Article 74(2) of the PSD2 is essential for the correct application of the mandate to perform SCA and should not be deemed to be a temporary regime.

Provided that, according to Article 74 of the PSD2 the payer will always be protected in case of unauthorised payment transactions (i.e. fraud) and that the liability regime for SCA is clearly established, in the opinion of Visa, there is no objective reason to take away from payees and PSPs of payees the possibility to adopt alternative methods of authentication. On the contrary, depriving payees and payee's PSP from such a possibility would hamper "*technology and business-model neutrality*" and the "*development of user-friendly, accessible and innovative means of payment*", both objectives of the draft RTS according to Article 98 of the PSD2.

Article 74(2) of the PSD2 should be considered the basis for payees and payees' PSP to actively decide whether SCA is needed to secure a transaction according to the risks involved, in exchange of taking liability for unauthorised transactions in case of fraud.

As outlined in the previous section, systematic request of SCA increases the abandonment of transactions. For this reason, payees have always been reluctant to adopt SCA. The possibility for the payee (and the payee's PSP) to make decisions based on the risk, is the basis of extremely successful business models that have helped develop electronic commerce in Europe and globally (e.g. card on file or "one-click") that should not be taken away by the draft RTS.

Similar to PSP, many payees already have sophisticated fraud-screening programmes alongside well-established customer relationships. This provides the payee with extensive information enabling a very comprehensive risk analysis and allows payees to assess the transaction and decide whether SCA is needed or not.

Like RBA for payers' PSPs, systems developed by and for the payees have also proven to be efficient. As described in the response of CyberSource, a major retailer selling across Europe and the rest of the world managed to reduce their fraud to sales ratio from a 7% to 0.08% by implementing Decision Manager, the CyberSource tool which allows merchants to analyse transactions and score them for risk, without requesting SCA for all transactions.

According to the above, Visa believes that, in line with paragraph 7.5 of the EBA Guidelines for the security of internet payments, the draft RTS should re-instate the ability of the payees and payees' PSPs to "*use of alternative authentication measures could be considered for pre-identified categories of low-risk transactions, e.g. based on a transaction risk analysis, or involving low-value payments*".

1. Exemptions based on the amount of the transaction

Visa welcomes the inclusion in the draft RTS of exemptions based on the amount of the transaction. As explained in the previous section, this is part of the mandate given to the EBA in Article 98 of the PSD2 (along with exemptions based on the risk of the service provided, the channel, the amount and the recurrence of the transaction).

a) Exemptions based on the amount of the transaction for contactless payments

Article 8(1)(b) of the draft RTS exempts from the SCA mandate contactless transactions at a point of sale under euros 50. Visa generally supports the threshold proposed.

However, the EBA should take into account that there would be cases where the payment could be higher than euros 50 and SCA could not be performed. For example, certain transactions in toll roads, parking or mass transit environments may be higher than euros 50. As explained elsewhere in this document, the point of sale cannot always be equipped with a PIN-pad, particularly in unattended terminals (e.g. toll roads).

In the opinion of Visa, the draft RTS should clarify that such transactions (higher than euros 50 with no SCA) are allowed in accordance with the liability regime set forth in Article 74(2) of the PSD2. In this case, if the payee (the merchant) and the payee's PSP cannot request SCA for payments higher that euros 50, these transactions should be allowed to progress provided that the payee's PSP and the payee take liability for unauthorised transactions.

Regarding the cumulative value of euros 150. The EBA should take into account that not all contactless transactions are authorised in real time by the issuer of the card or payer's PSP (i.e. payments under euros 20 are authorised by the card-based payment instruments – card, mobile, etc - themselves, on the basis of security mechanisms implemented in the device). This means that any cumulative transaction monitoring, as drafted, would need to be performed by a combination of the internal capabilities of the card-based payment instrument and the information hosted by the issuer of the card. At any point in time it is therefore impossible to ensure compliance with the proposed euros 150 cumulative transaction threshold without either reissuance of the vast majority of contactless payment devices (e.g. contactless cards) or implementation of "zero floor limits" (i.e. authorisation in real time by the issuer) for all contactless transactions – both of which have significant implications for the issuer and payee's PSP.

Accordingly, Visa suggests that the cumulative transaction value of euros 150 is provided in the draft RTS as a baseline for issuer risk management purposes instead of being defined as an express requirement.

b) Exemptions for "contact payments" at a point of sale

In the opinion of Visa, all transactions at the point of sale – irrespective of the technology used - should benefit from the same exemption proposed for contactless transactions.

Moreover, if such an exemption is not granted, the draft RTS risk creating major disruption for payments that, for practical reasons (e.g. speed) and technological reasons (impossibility to install a PIN-Pad), cannot use SCA. This would be the case for various environments, such as vending machines, parking lots and toll roads. As an example, in 2015 toll roads in France registered 140 million card payment transactions.

In addition, from a card-based payment perspective, there is no difference in the technology used and the security mechanisms for contactless payments and "contact" payments (i.e. when the card is introduced into a point of sale), so a difference is not justified.

Please also see our comments in previous section regarding payments higher that euros 50 and cumulative value.

c) Exemptions based on the amount of the transaction for remote payments

Visa does not agree with the threshold of euros 10 proposed. In the Visa network only 30% of remote transactions are euros 10 or less. This implies that 70% of remote transactions would need SCA. This would impose friction and servicing cost on the system, without guaranteeing a specific fraud outcome. Using data from the UK rollout of RBA and the volume forecast of euros 509.9 billion from the *European B2C Ecommerce Report* (which was commissioned by Ecommerce Europe and created by the Ecommerce Foundation), Visa calculates that the EBA draft proposal would equate to additional abandoned transactions amounting to euros 11.2 billon.

In addition, the exemption proposed risks creating an unlevelled playing field with payment transactions of a "communication network" – very similar to remote payment transactions - which, up to euros 50, are not subject to PSD2, according to Article 3(l) of PSD2.

Accordingly, Visa would propose that the threshold for remote transactions is euros 50, in line with payments at a point of sale and the exemption granted for "communication networks".

Regarding the cumulative value, Visa proposes that the cumulative value is established at euros 150 (in line with the exemptions at the point of sale) and is considered a daily limit.

2. Exemptions based on the recurrence of the transaction

Article 8(2) of the draft RTS set forth exemptions for credit transfers based on the recurrence of the transactions. Visa believes that these exemptions should be applicable to all payment instruments and not only credit transfers.

In the opinion of Visa, it should be possible for a payer to establish a "white list of payees" with the payer's PSP for card payments. In addition, it should also be possible to establish a relationship with a trusted merchant so that the first transaction is subject to SCA or the initial load payee system is subject to SCA, and subsequent transactions are exempted from SCA, but subject to risk-based analysis of the issuer.

Q5: 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 the exemptions?

Visa has extensively commented on the exemptions proposed in the response to question 4.

Following the discussion at the public hearing on the draft RTS, Visa understands that question 5 refers to the discussion on whether applying the exemptions proposed should be considered mandatory or not.

Visa believes that PSP should be able to determine the appropriate authentication method for every transaction, irrespective of the amount.

In addition, Visa believes that an exemption from a requirement has to be understood as the state of not being subject to a responsibility. Thus, exemptions should never be considered as mandatory.

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?

Visa would welcome a clarification in relation to Article 17(1) of the draft RTS. In the opinion of Visa, the draft RTS should clarify that this provision does not apply to card-based payment transactions at a point of sale.

In the EMV standards and technology, the card-based payment instrument does not authenticate the payment terminal. Such functionality is not needed from a payments security perspective, is operationally impractical and easily circumvented by criminals.

Implementing such a requirement would imply a major overhaul of the EMV technology that would cause a global replacement of existing terminals and cards.