Securing Internet Payments
The current regulatory state of play
In recent years the European Union (EU) institutions have shown a growing interest on the security of electronic payments. This interest has materialised in two overlapping documents: the European Banking Authority (EBA) Guidelines on the security of internet payments¹ (the EBA Guidelines) and new provisions included in the revised Payment Services Directive (PSD2)². Both documents include a mandate to perform Strong Customer Authentication (SCA) prior to the initiation of the payment.

The purpose of this paper is to shed some light on Visa Europe’s interpretation of the requirements regarding SCA and the scope of the exemptions that are or will be allowed. It also intends to clarify what is the expected impact for the Issuers, Acquirers and merchants, as well as the position and status of Visa Europe within the context of these new requirements.

**Executive summary**

### The EBA Guidelines

The current EBA Guidelines in force as of August 2015 mandate the use of SCA for all internet payments. SCA is defined as a two factor authentication based on the combination of elements of knowledge, possession and/or inherence. They also require the use of the so-called “one-time-passwords”.

The EBA Guidelines exempt “low risk transactions” from the mandate to perform SCA. These transactions are defined as low value payments and transactions for which a risk analysis has been conducted.

Local Supervisors are tasked with ensuring that the EBA guidelines are implemented by Issuers and Acquirers. All Member States – except the United Kingdom, Estonia and Slovakia – intend to ensure compliance with the EBA Guidelines. However, up to now, local Supervisors have chosen to do comparatively little in this regard.

### The revised Payment Services Directive (PSD2) and new, additional EBA guidance

PSD2 also includes a provision mandating to perform SCA for certain payment transactions. Under PSD2, the scope of this mandate is broader, since it applies to all electronic payments (face-to-face and remote environments). PSD2 does not mandate the use of a ‘one-time-password’. However, for remotely initiated payments, PSD2 requires that one of the factors of the authentication is linked to the amount and the payee.

Exemptions to the application of SCA are equally allowed under PSD2. These exemptions are based not only on the risk and the amount of the transaction, but also on the recurrence of the payment and the channel used for its execution. It will be up to the EBA to further develop these exemptions in the coming months.

In the 12 months following the entry into force of PSD2, the EBA will have to publish further guidance on various aspects in relation to authentication. The EBA will clarify the extent of the exemptions and also the use of the above-mentioned link to the amount and the payee required for remote electronic payments.

### Visa Europe position

Visa Europe actively promotes the security of internet payments and believes that the key for the growth of e-commerce resides in striking the right balance between payment security and users convenience. In this sense, Visa Europe believes that ‘adaptive methods of authentication’ based on the assessment of the risk involved in a transaction should be both permitted and promoted at the EU level.

Visa Europe will proactively engage with EU and national regulators to strongly support a careful review of the requirements of the EBA Guidelines and PSD2 to ensure that they are applied consistently and allow the flexibility needed to apply different methods of authentication depending on the risk involved in the transaction.

---

Strong Customer Authentication (SCA) under the current EBA Guidelines

The EBA Guidelines were published in December 2014⁵ and formally came into force in August 2015. The EBA Guidelines are aimed at establishing a set of minimum requirements relating to the authentication and security of internet payments. Among these requirements, the EBA Guidelines mandate the use of SCA.

What is the scope of the mandate to perform SCA?
Under the EBA Guidelines, the requirement to perform SCA applies to “internet payments”. In the case of card payments, it is specified that the requirements of the EBA Guidelines – including the obligation to perform SCA – are applicable “to payments on the internet, including virtual cards, as well as the registration of card payment data for their use in a ‘wallet solution’”⁶.

However, the EBA Guidelines are not applicable to “payments where the instruction is given by post, telephone order, voice mail or using SMS-based technology” and to “mobile payments” other than browser-based payments”.

What is the definition of SCA?
The definition of SCA in the EBA Guidelines is based upon the core principles of something a customer knows, something a customer has and something a customer is⁸. The EBA expects two out of three of these factors to be used in authentication (i.e. two-factor-authentication).

In addition to the two factor authentication defined above, the EBA Guidelines also require that “[a]t least one of the elements should be non-reusable and non-replicable (except for inherence), and not capable of being stolen via the internet”. This requires in practice the use of so-called “one-time-passwords”.

What are the obligations for Issuers and Acquirers regarding SCA?
In relation to the obligation to perform SCA the EBA Guidelines set forth that:

- **Issuing PSPs**: should support SCA of the cardholder (all cards to be technically capable of / registered to use SCA); and
- **Acquiring PSPs**: should support technologies allowing the issuer to perform SCA of the cardholder for the card schemes in which the Acquirer participates. Acquiring PSPs should also require e-merchants to support solutions that allow the issuer to perform SCA.

The EBA Guidelines also indicate that “providers of wallet solutions should require strong authentication by the issuer when the legitimate holder first registers the card data”.

---

⁵ The first document dealing with security of internet payments was the SecuRe Pay recommendations issued by the ECB in 2012. That document was subsequently turned into the EBA Guidelines with minor adjustments.

⁶ The EBA Guidelines define “wallet solutions” as “solutions that allow a customer to register data relating to one or more payment instruments in order to make payments with several merchants”.

⁷ The EBA Guidelines do not define what a “mobile payment” is. However, the ECB has previously defined mobile payments as “payments for which the payments data and the payment instruction are transmitted and/or confirmed via mobile communication and data transmission technology through a mobile device between the customer and the provider of the service, digital or physical goods and services, or between the customer and an e-merchant, or between the customer and an Acquirer”. They are not covered by the EBA via Europe would consider mobile payments, as defined by the ECB, out of the scope of the EBA Guidelines.

⁸ The EBA Guidelines define strong customer authentication as “a procedure based on the use of two or more of the following elements – categorised as knowledge, ownership and inherence: i) something only the user knows, e.g. static password, code personal identification number; ii) something only the user possesses, e.g. token, smart card, mobile phone; iii) something the user is, e.g. biometric characteristic, such as a fingerprint. In addition, the elements should be used in a mutually independent manner (i.e. the breach of one does not compromise the others). At least one of the elements should be non-reusable and non-replicable (except for inherence), and not capable of being surreptitiously stolen via the internet. The strong authentication procedure should be designed in such a way as to protect the confidentiality of the authentication data”.

⁹ A payment service provider in the sense of the Payment Services Directive, i.e. an entity licensed to issue or acquire payment instruments, including credit, institutions, e-money institutions and payment institutions.
What are the exemptions to perform SCA?
The EBA Guidelines allow the use of “alternative methods of authentication” (i.e. different from SCA defined as two factor authentication) for “low-risk transactions” (based on a transaction risk analysis or low-value transaction amounts).

Following the publication of the 2012 SecuRe Pay Recommendations, the ECB published the “Assessment Guide for the Security of Internet Payments” in February 2014⁹. The Assessment Guide, even if not issued by the EBA, can be used – according to the ECB – to interpret the EBA Guidelines. In this Guide the ECB clarifies two important aspects in relation to the exemptions to the requirement to apply SCA:

(i) low value payment transactions are payments up to EUR 30;

(ii) the risk analysis for pre-identified low risk transactions should take into account “the nature of the products/services sold (e.g. physical vs. digital goods and services), the delivery channel, customer behaviour, the fraud monitoring skills of the e-merchant, etc., and is a transactions risk analysis conducted against those categories.”

The Guide also suggests that the conditions for the application of alternative methods of authentication should be set out in the contracts between the actors concerned (payment schemes/acquirers/e-commerce merchants).

The Guide of the ECB clarifies that the providers of wallet solutions should require SCA by the issuer when the cardholder first registers the card data or at least when the first transaction with the card is initiated. Subsequently, SCA should also be required when the cardholder logs into the wallet or when a payment transaction is initiated. However, for these subsequent payments with the wallet, alternative methods of authentication can be used for “low-risk transactions”.

Therefore, according to the above in the opinion of Visa Europe, the mandate to apply SCA should not apply to:

- Transactions under EUR 30 irrespective of the conditions of the transaction or the type of e-merchant;
- Transactions in which a risk analysis has been conducted;
- Recurring payments, including payment of utilities – e.g. electricity bill, car insurance – as well as subscriptions for physical or digital goods and services – e.g. subscription for a pay per view media internet platform – for goods or services agreed on the internet, for which only the first transaction (and not the subsequent payments) should be considered subject to the SCA requirements.

What are the consequences on non-compliance with SCA mandate?
The consequences of non-compliance with the EBA Guidelines depend on local Supervisors. In theory, non-compliance with the EBA Guidelines could even entail fines for Issuers and Acquirers.

The majority of EU Member States have stated that they comply or intend to comply with the EBA Guidelines. Only Estonia, Slovakia and the United Kingdom reported that they will not enforce the EBA Guidelines in their jurisdictions¹⁰. Cyprus and Sweden reported that they intend to comply with the EBA Guidelines partially (this partial compliance does not impact the implementation of the core requirements of the EBA Guidelines).

Up to now, many Supervisors have chosen to do comparatively little with the EBA Guidelines mandates and appear to be awaiting the PSD2 position. This is already the case of the UK who stated, as part of the explanation of the reasons why they did not intend to enforce the EBA Guidelines, that “implementation of the Guidelines will require some providers to make significant changes to their systems and controls and significant additional changes are likely to be necessary following implementation of PSD2”.

The majority of EU Member States have stated that they comply or intend to comply with the EBA Guidelines. Only Estonia, Slovakia and the United Kingdom reported that they will not enforce the EBA Guidelines in their jurisdictions¹⁰.

---


The revised Payment Services Directive (PSD2) also includes a mandate to perform SCA. This Directive will not be applicable until it is turned into national law in all the Member States of the EU (i.e. expected to be around January 2018).

The mandate to perform SCA in PSD2 is similar to the one included in the EBA Guidelines. However, there are significant differences between both documents. The table below outlines these differences.

---

### Strong Customer Authentication (SCA) under PSD2 – new, additional EBA guidance

<table>
<thead>
<tr>
<th></th>
<th>EBA Guidelines</th>
<th>PSD2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scope</strong></td>
<td>Payments on the internet</td>
<td>All electronic payments (including face-to-face and remote environments)</td>
</tr>
<tr>
<td><strong>Definition of SCA</strong></td>
<td>2 factor authentication, plus a “one time password”</td>
<td>2 factor authentication. For remote electronic payments one of the factors linked to the amount and the payee</td>
</tr>
</tbody>
</table>
| **Exemptions to the application of SCA** | Low-risk transactions:  
• Under EUR 30  
• Risk assessment | Different factors:  
• the level of risk involved in the provided service;  
• the amount and/or the recurrence of the transaction;  
• the payment channel used for the execution of the transaction. |
| **Consequences of Non-compliance** | Depends on local Supervisor (e.g. Central Banks) | Local Supervisors; and can be directly invoked by private persons before a National Judge |
| **Liability**                 | Remains silent                                                                | The actor in the payments chain that decided not to apply SCA is liable. This is expected to be the Issuer, the Acquirer or the merchant in Visa payments. The consumer is not held liable for unauthorised transactions |
| **Implementation**            | EBA to draft Regulatory Technical Standards in the 12 months following publication of PSD2. Regulatory Standards to be implemented within the 18 months following their formal adoption |                                                                       |
| **Applicability**             | August 2015                                                                    | January 2018                                                          |
The differences explained in detail:

**Scope**
Under the EBA Guidelines, the obligation to perform SCA applies to "internet payments". In PSD2, the mandate to perform SCA is broader, since it applies to all "electronic payment transactions" (i.e. face-to-face and remote).

**Definition of SCA**
The EBA Guidelines and PSD2 define SCA as a procedure based on the combination of two or more elements categorised as knowledge, ownership and inherence. Both documents also require that the breach of one factor does not compromise the reliability of the others.

Different from the EBA Guidelines, PSD2 does not require the use of "one-time-passwords" for the authentication. However, PSD2 includes an additional requirement for SCA. For "remote electronic payment transactions"11 PSD2 mandates a link of one of the factors of the authentication with the amount of the transaction and the payee. In the EBA Guidelines, such a link is only included as a "best practice" (i.e. not mandatory). The use of the above-mentioned link required for remote electronic payments is unknown for the moment. It will be up to the EBA to clarify this requirement in the Regulatory Technical Standards to be drafted after PSD2 entry into force.

**Exemptions to the application of SCA**
Under the EBA Guidelines, the requirement to perform SCA could be exempted for low risk transactions. PSD2 also allows exemptions to the requirement to perform SCA according to various factors:

- the level of risk involved;
- the amount and/or the recurrence of the transaction;
- the payment channel used for the execution of the transaction.

PSD2 mandates the EBA, in cooperation with the ECB, to develop further guidance (Draft Regulatory Standards)12 on authentication that will clarify the extent of the above-mentioned exemptions.

The Regulatory Standards would have to be developed within 12 months following the entry into force of PSD2. Once formally approved, the Regulatory Standards would have to be implemented in all EU Member States within the following 18 months. Therefore, the new guidance from the EBA on SCA and the exemptions to its application will not be implemented by EU Member States at least until October 2018.

**Visa Europe position regarding the implementation of PSD2**
Visa Europe fully supports the objectives of the EU legislator to improve security of electronic payments. However, in the opinion of Visa Europe, the future Regulatory Standards on Authentication to be drafted by the EBA should ensure enough flexibility when implementing the mandate to perform SCA. This is essential not to hamper the overall objective of PSD2 of promoting electronic payments and also to "allow for the development of user-friendly, accessible and innovative means of payment" as set forth in PSD2 itself.

Accordingly, SCA should not be required for low value amounts irrespective of the channel (i.e. including contactless transactions). In addition, actors involved in the transaction should be able to determine the amount of a low value payment according to the conditions of the payment.

With regard to the assessment of the level of risk involved in the transaction, the Regulatory Standards should remain technologically neutral and should take into account that the risk assessment could be performed in a number of ways, some of them based on technological developments that are still unknown.

In addition, the Regulatory Standards should ensure that the mandate to perform SCA does not put at risk the continuity of commercial transactions in channels where executing SCA would be too burdensome or, in some cases, unfeasible. This is the case of recurring payments13.

For recurring payments, the Regulatory Standards should reflect that SCA (or an alternative acceptable method) should be applied only when the cardholder enters the contractual agreement originating the recurring charges and not for the subsequent payments unless cardholder details change. This should be the case because, in most cases, the cardholder will not be reachable when the payments are triggered –by the payee- according to the conditions agreed with the cardholder.

For mail and telephone orders, the Regulatory Standards should clarify that they are out of the scope of the mandate to perform SCA, in line with the Recitals of PSD2.

Finally, Visa Europe believes that the Regulatory Technical Standards should reflect that, taking liability for unauthorised payments is the only reasonable consequence for the actor in the payments chain (Issuers or Acquirers) that does not support SCA. On the one hand, this would ensure that more convenient methods of authentication can be developed. On the other hand, it would provide Issuers, Acquirers and merchants the freedom to decide what methods of authentication are more suitable according to the conditions of their transactions.

---

11 PSD2 defines "remote payment transactions" as "a payment transaction initiated via internet or through a device that can be used for distance communication”.
12 The main difference between current EBA Guidelines and the Draft Regulatory Standards is that the EBA Guidelines need the intervention of local Supervisors to be applied. However, the Regulatory Standards are similar to legislation and, accordingly, would be directly applicable without further intervention of local authorities.
13 For the purposes of this note and in line with Visa Europe Rules, "recurring payments" should be understood as Recurring Transactions (i.e. the payment of utilities or subscriptions), Instalment (i.e. the payment of goods or services in instalments according to the conditions agreed between the merchant and the cardholder) and Card-on-file payments (i.e. payments in which the merchant stores the card data).
Visa Europe has supported spontaneous and recurring payment using card based products in remote channels, where the cardholder and merchant are not both directly present, since before the internet’s inception. Visa Europe promotes the security of electronic and internet payments. We allow electronic commerce payments which provide the opportunity for full authentication by the Issuer (3DSecure processed as ECI 5 & 6) and payments which are only authorised by the Issuer with minimal authentication data (processed as ECI 7-9).

In addition, the liability scheme set out in PSD2 supports Visa’s current chargeback regime which allows liability to be passed back to an Acquirer where VbV has not been used for the disputed transaction.

a. From a Verified by Visa (VbV) perspective:
This infrastructure is entirely compatible with the SCA requirements that are being proposed and is flexible enough to allow such authentication in conjunction with relevant risk based solutions.

We would strongly recommend that Issuers review their authentication approach, and consider with their own local Supervisors whether the approach they are taking, or are moving to, is likely to be compatible with the regulators thinking on what they will be looking to introduce.

A detailed summary of this solution is attached to this document as Appendix A.

b. From the perspective of electronic commerce transactions which are not processed via 3DSecure:
This channel does not meet the proposals for SCA which is likely to mean that it will not be possible for a consumer transacting in this manner to be held liable by any party for fraud, as is the case already today, according to the requirements of the first Payment Services Directive.

There are requirements within the EBA Guidelines which expect Acquirers to require SCA support for merchants, but accepts that a risk based approach can be taken based on detection profiling and some other factors, such as, for example, customer payment patterns (behaviour), value of the related transaction, type of product and payee profile.
Impact for Issuers
Issuers are already familiar with the increasing level of regulatory requirements and should be in conversation with their local Supervisor regarding their plans to enforce EBA Guidelines and future PSD2 requirements.

Impact under the EBA Guidelines
Visa Europe believes that the expectation for e-commerce transactions is that all Issuers will be asked to enrol their cards in a SCA method (3DSecure) and to have the ability to use 3DSecure for all traffic.

The issue of how much of the Issuers traffic needs to be based on SCA is a more difficult question to determine, because Issuers can only sensibly support SCA where the merchant is completing a VbV transaction.

Potential impact under future PSD2
After publication of PSD2, the EBA will release Regulatory Standards on the implementation of the authentication requirements that allow different methods of authentication according to the risk of the transaction, the amount, the recurrence and the channel used for the execution of the transaction.

Under PSD2, Issuers that did not register their cards into a SCA method (i.e. 3DSecure) will have to account for this decision to their local Regulators and will be held liable before consumers for unauthorised payment transactions.

Impact for Acquirers and merchants
Acquirers will be expected to ensure that their merchants support SCA (3DSecure) albeit again there is scope within the current proposals to allow flexibility on how this is delivered.

Impact under the EBA Guidelines
For Visa transactions, the current expectation was that all merchants will need to support VbV as of 1 August 2015, in line with the timeline set by the EBA Guidelines, if this position is being supported by their local Supervisors.

The rules do however, appear to provide scope for merchants accepting transactions to manage the risk via appropriate detection and profiling capabilities. This means that merchants with strong risk assessment capabilities will be able to stream their business between low and higher risk and only require authentication for higher risk transactions.

Potential impact under future PSD2
The requirements for the Acquirers will be subject to further clarification from the Regulatory Technical Standards of the EBA to be written during 2016.

Acquirers are likely to need to report to their regulators on merchant performance and demonstrate that the risk based controls are indeed appropriately targeting low risk business.

This change could have a dramatic impact on the way some merchants undertake their business but may allow Acquirers to extend their services to the wider provision of risk tools and solutions.

Under PSD2, Acquirers will need to account to their local Supervisor for fraud performance where 3DSecure is not used. In addition, consumers will not be held liable for unauthorised transactions where 3DSecure was not used. In these cases, the Acquirer or the merchant (depending on the party that decided not to apply SCA) will be held liable for unauthorised payment transactions.
Conclusions and next steps

The change in the regulatory positioning from the EBA Guidelines to PSD2 is substantial and may lead to some significant changes in the market place. There is also a risk that differing Regulators positions may lead to subtle but significant differences in expectations between markets.

Visa Europe will continue to work with the European Commission, EBA, ECB, National Regulators and Central Banks to seek continued support for flexibility for the development methods of strong customer authentication that strike the right balance between security and consumer convenience within the Visa payment system in Europe. We believe that the EBA Regulatory Standards written post PSD2 will be key to how this legislation is applied and we would ask all members to seek to support flexibility in this activity when engaging with their Regulator and local Supervisors, stressing the importance of not hampering innovation by over imposing two factor authentication as currently defined by the EBA and PSD2.

Visa Europe will proactively engage with EU and National Regulators to strongly support a careful review of the requirements of the EBA Guidelines and PSD2 to ensure that they are applied consistently and allow the flexibility needed to apply different methods of authentication depending on the risk involved in the transaction.

Visa Europe will provide further updates on this issue as thinking and positioning by the regulators matures.

Visa Europe will provide further updates on this issue as thinking and positioning by the regulators matures
The Verified by Visa (VbV) infrastructure is compatible with the proposed strong authentication requirements. VbV is flexible enough to allow Issuer choice regarding strong authentication options, in addition to risk-based solutions.

The objective of VbV is to benefit all participants by providing Issuers with the ability to authenticate cardholders during an online purchase, thus reducing the likelihood of fraudulent usage of Visa cards.

Verified by Visa is based on the 3-D Secure Protocol. 3D-Secure is a three-domain model where the Acquirer Domain and Issuer Domain are connected via the Visa Interoperability Domain for the purpose of authenticating a cardholder during an electronic commerce transaction.

In order to facilitate the continued growth of e-commerce and m-commerce, it is essential to provide payment solutions that strike the right balance between consumer convenience and the risks involved in the transactions. The European – and the global – payments industry continues to seek such balance by developing intelligent risk-based authentication solutions.

The widespread use of risk-based VbV authentication solutions in the UK has significantly improved the consumer experience and resulted in fewer abandoned transactions, with no negative effects on security.

To comply with the proposed strong authentication requirements, a risk assessment of each transaction has to be performed and strong authentication for transactions that are identified as high-risk.

- Risk based authentication engine with SMS OTP step-up for high risk transaction is an option Issuers could consider implementing among others, in order to comply with SCA requirements.

Visa Europe’s VbV strategy is to work with stakeholders, across Europe, to continue the rollout of risk-based authentication for VbV transactions, combined with the capability to ‘step-up’ to strong authentication for transactions identified as high risk.

It should be noted that Visa continues to work within EMVCo to deliver an enhanced 3DSecure message standard, normally referred to as 3DSecure version 2. This will allow greater support for VbV to merchants offering Electronic Commerce payments outside of the traditional browser environments.

Appendix A: Verified by Visa

The Verified by Visa (VbV) infrastructure is compatible with the proposed strong authentication requirements. VbV is flexible enough to allow Issuer choice regarding strong authentication options, in addition to risk-based solutions.

The objective of VbV is to benefit all participants by providing Issuers with the ability to authenticate cardholders during an online purchase, thus reducing the likelihood of fraudulent usage of Visa cards.

Verified by Visa is based on the 3-D Secure Protocol. 3D-Secure is a three-domain model where the Acquirer Domain and Issuer Domain are connected via the Visa Interoperability Domain for the purpose of authenticating a cardholder during an electronic commerce transaction.

In order to facilitate the continued growth of e-commerce and m-commerce, it is essential to provide payment solutions that strike the right balance between consumer convenience and the risks involved in the transactions. The European – and the global – payments industry continues to seek such balance by developing intelligent risk-based authentication solutions.

The widespread use of risk-based VbV authentication solutions in the UK has significantly improved the consumer experience and resulted in fewer abandoned transactions, with no negative effects on security.
This paper is Visa Europe’s current view on regulatory and legislative positioning as at January 2016. However, it should be noted that this is an area where discussion on primary legislation and interpretation is still ongoing and as such the expectation is that this document will be updated iteratively.