EBA CONSULTATION PAPER ON THE IMPLEMENTATION OF THE DRAFT EBA GUIDELINES ON THE SECURITY OF INTERNET PAYMENTS PRIOR TO THE TRANSPOSITION OF THE REVISED PSD2

DEADLINE FOR COMMENTS: 14 NOVEMBER 2014

MASTERCARD'S COMMENTS

MasterCard would like to thank the EBA for the opportunity to comment on the draft EBA guidelines. Below MasterCard provides its views on the consultation question, as well as its comments parts of the draft EBA guidelines as they relate to card payments. As you will see below:

- On the consultation question: MasterCard recommends a one-step approach (which would avoid the complexities of introducing a first set of changes, followed by another set of changes once the national legislations transposing the PSD2 will come into force). However the EBA guidelines should incorporate the principles that will be set out in the final version of the PSD2 (not those that appear in the current *draft* version of the PSD2, which are still subject to change). In addition, PSPs should be given sufficient time in order to comply with the updated EBA guidelines, and in any event at least one year.

- On the principles contained in the EBA guidelines: while MasterCard is supportive of the general direction set out in the draft EBA guidelines which emphasises the importance of strong customer authentication to fight against payment card fraud and increase consumer trust in internet payment services, MasterCard considers that strong authentication for every single card transaction is not an optimal solution; be it for merchants (who bear the risk of consumers dropping off and not making a purchase), consumers (who favour payment solutions that are as convenient as possible, while of course remaining secure), Payment Service Providers (PSPs) or payment card schemes. Instead MasterCard favours a "Risk Based Assessment" (RBA) where, depending on a set criteria, a transaction should, or should not, be subject to strong authentication. In a way, strong authentication should be the exception – not the norm – contrary to what is provided for in the draft EBA guidelines.

Should the EBA wish to discuss any of the below, please reach out to Scott McInnes, Senior Counsel Regulatory Affairs, based in Waterloo, Belgium (+32.2.352.53.00 or scott_mcinnes@mastercard.com).

MasterCard's key principles regarding strong authentication

Before MasterCard provides its specific comments on the EBA consultation question and on some aspects of the draft EBA guidelines, we believe it would be helpful to describe some of the key principles that we believe are relevant when considering strong authentication – and which guided us in our more specific comments below. They are as follows:

1. **Appropriate balancing of friction at checkout versus fraud reduction**. MasterCard has developed a view based on feedback from a number of interested parties that we should look at the consumer and merchant experience as part of our determination on when to strong authenticate. With advances in technology, there are a number of data points that allow one to judge the risk of each transaction based on factors such as transaction amount, geolocation, shopping patterns,

transaction profile, etc. By considering such types of factors, one can determine the risk of the transaction and apply strong authentication where the risk is assessed as high. This provides the protection that a consumer and merchant would expect ensuring that the solution can be tuned to significantly reduce fraud whilst avoiding the need to strongly authenticate every transaction.

2. **Need for a multi-channel approach**. A focus on browser-based e-commerce alone does not support the true need of consumers and merchants. There is a clear demand from consumers that they be provided with safe and convenient ways to shop in any channel and through any device. A busy commuter may choose to do regular purchases over a mobile application, call to pay a bill over the same phone to a call-centre, and then on arriving home use a tablet/notebook or PC to shop online. As we develop strategies to fight fraud, MasterCard needs to ensure that it provides a safe simple and secure solution across all these channels, with as common a solution as possible so that we do not confuse the consumer. Again, this strategy delivers a double impact as it is aimed at fighting fraud but also at simplifying the consumer experience so that it may encourage greater use.

3. **Need for technology independence**. The development of new devices and security within those devices is an area of great expansion and rapid development. There is also considerable advancement in identifying the device itself as a trusted device used by the consumer. Due to this complexity, MasterCard believes in setting standards that technology providers have to meet or exceed and in monitoring the results to see if this “bar” should be raised. We do not believe that it is a good idea to be prescriptive in how technology is used but we should be clear on both the intent and the minimum standard. This is especially true as we look to support any channel and any device as the technology and security will differ even if we aim to have a consistent consumer / merchant experience.

MasterCard’s comment on the EBA consultation question

In response to the EBA’s consultation question, MasterCard recommends a one-step approach, and therefore that the EBA guidelines include the same requirements that will be contained in the national legislations that will implement the PSD2 (assuming those national transpositions will be in line with the PSD2). Indeed, it would be more complex and more costly for all stakeholders (PSPs, merchants, card scheme, etc) to have to first comply with a set of EBA guidelines that would ignore the text of the PSD2, and then have to upgrade their systems in order to comply with national legislation implementing the PSD2.

However, it would not make sense for the EBA guidelines to be updated to include the *current* draft provisions of the draft Payment Services Directive 2 (PSD2) on security when those provisions are still subject to a lot of debate and will therefore continue to evolve of the coming months (e.g. until at least Q2 2015). Instead, the EBA guidelines should incorporate the principles set out in the final version of the PSD2 – and thereby ensure the above-mentioned one-step approach for all stakeholders.

In order to be able to comply for the principles in the updated EBA guidelines, PSPs should be given sufficient time. One year would seem to be reasonable in order to allow stakeholders to necessary system changes and financial investments.

MasterCard’s comments on the specific EBA guidelines

Scope of application of EBA guidelines

It is not entirely clear to MasterCard whether the EBA guidelines will apply, or not, to payment card schemes. On the one hand, the EBA Consultation document states that "*References to payment* *schemes, their Governance Authorities (GAs), and the oversight thereof have not been incorporated in the draft EBA guidelines, as payment schemes are not covered by PSD1*"[1].

On the other hand, the draft EBA Guidelines do contain some guidelines that would apply to payment card schemes (e.g. paragraph 7.6: "*All payment schemes should promote the implementation of strong customer authentication by introducing a liability regime for the participating PSPs in and across all European markets*"; paragraph 10.2: "*Card payment schemes in cooperation with acquirers should elaborate a harmonised definition of e-merchant categories and require acquirers to implement it accordingly in the PSP's authorisation message conveyed to the issuer*").

MasterCard would therefore welcome clarity on the scope of application of the EBA Guidelines.

Alignment of ECB recommendations to EBA guidelines

Irrespective of whether the EBA guidelines will apply to card schemes or not, it is clear that the ECB (SecuRePay Forum) Recommendations for the Security of Internet Payments will apply to payment card schemes. It is MasterCard's expectation that those recommendations and the EBA guidelines will ultimately be aligned so as to be absolutely identical. For example, should the draft EBA guidelines be amended as a result of this Consultation and/or in order to mirror the final text of the PSD2, MasterCard would expect the ECB recommendations to be amended accordingly.

In particular, the ECB recommendations contain a key principle of "comply or explain"[2] to the benefit of PSPs and schemes. However the draft EBA guidelines do not contain this "complain or explain" principle to the benefit of PSPs (they only provide that "*competent authority must notify EBA as to whether they comply or intend to comply with these guidelines, or otherwise with reasons for non-compliance*" – however this is not addressed to PSPs). This is a significant difference compared to the ECB recommendations. We believe PSPs should benefit from the "comply or explain" principle in the EBA guidelines to the same extent that PSPs and card schemes benefit from this principle under the ECB Recommendations for the security of internet payments. MasterCard would therefore welcome the inclusion of the "complain or explain" principle in the EBA guidelines[3].

Point 7.3 of the draft EBA guidelines: definition of "support"

It is not entirely clear to MasterCard what is meant in paragraph 7.3 of the draft EBA guidelines (and in the ECB Recommendations for the Security of Internet Payments) by the use of the word "support".

[1] Page 9.

[2] "*Addressees are expected to comply with both the recommendations and the KCs or need to be able to explain and justify any deviation from them upon the request of the relevant competent authority ("comply or explain" principle)*" (ECB Recommendations on the Security of Internet Payments, 2013, page 4).

[3] MasterCard notes that mobile payments, other than browser-based ones, are excluded from the scope of the draft EBA guidelines (as well as from the ECB Recommendations for the Security of Internet Payments). Those types of mobile payments are covered elsewhere, namely in the draft ECB Secure Pay Forum Recommendations for the Security of Mobile Payments (http://www.ecb.europa.eu/paym/cons/pdf/131120/recommendationsforthesecurityofmobilepaymentsdraftpc201311en.pdf). We encourage the ECB to ensure that both set of recommendations (on internet payment and on mobile payments) will be aligned, as well as with the EBA guidelines, as there is a clear market trend towards convergence between mobile browser-based mobile payments and not-browser-based mobile app payments (as well as convergence between card-present and card-not-present payments). Such convergence will most likely imply that consumers will demand unified authentication solutions across what might initially be seen as distinct environments.

If this word should be interpreted as meaning that PSPs should "support, but not always necessarily apply" strong authentication on every card transaction, MasterCard would fully agree with this guideline.

However, if "support" should be interpreted to mean "apply" strong authentication for every card transaction, MasterCard would have severe reservations with such a requirement. MasterCard's comments below are provided on the basis of this interpretation of "support".

Rationale for the EBA guidelines: "consumer convenience" is missing

The draft EBA guidelines mention two main rationales for these guidelines: "*to contribute to fighting payment fraud*" and "*enhancing consumer trust in internet payment services*"[4].

MasterCard welcomes and supports these objectives which emphasise the importance of strong customer authentication to fight against payment fraud and increase consumer trust in internet payment services. However, MasterCard also believes that one third, and equally important, objective should be added: that authentication should be convenient for consumers.

We are very conscious of the practical difficulties, as well as importance, of optimally balancing strong security with consumer convenience, while taking into account risk management and liability framework considerations. As illustrated by our more detailed additional comments on the various parts of the proposed EBA guidelines (see below), we respectfully believe that the current EBA guidelines do not (yet) strike a good balance between these objectives. We fear that the current proposed guidelines, if left unchanged, may have the unintended consequence of imposing additional heavy and awkward authentication procedures to consumers, which may end up discouraging them from using internet payments.

As you may know, MasterCard has been promoting strong authentication solutions based on SecureCode and other solutions for many years. Our experience is well summarised in a Wikipedia article on 3D Secure, where it is stated that "*Many users view the additional authentication step as a nuisance or obstacle, which results in a substantial increase in transaction abandonment and lost revenue* [for merchants]"[5].

MasterCard strongly supports and promotes SecureCode and other strong authentication measures, but seeks to do it in a balanced manner without losing sight of the consumer convenience objective. We encourage the EBA to adopt a similar approach, and make "consumer convenience" an explicit rationale of its guidelines.

It is to be noted that the draft EBA guidelines state that "*The 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, as referred to in the Payment Services Directive*"[6]. This is somewhat similar to the "Risk Based Assessment" (RBA) approach that MasterCard is supportive of and which is described in more detail below – except that in MasterCard's view the principles should be inverted: RBA should be the norm, and strong authentication should be the exception (whereas the draft EBA guidelines provide for the opposite).

[4] Page 8.

[5] http://en.wikipedia.org/wiki/3-D_Secure

[6] Paragraph 7.8.

The general principle that "initiation of internet payments […] should be protected by strong customer authentication" (page 9) should be balanced with risk, liability, and consumer convenience considerations

Rather than strong authentication on every single card transaction, MasterCard recommends to perform a RBA; what is referred to in the EBA Consultation paper as "*Transaction risk analysis*" consisting in the "*evaluation of the risk related to a specific transaction taking into account criteria such as, for example, customer payment patterns (behaviour), value of the related transaction, type of product and payee profile*"[7].

This is the approach that has been adopted in other jurisdictions, such as the U.S. for example, where:

- For non-business customers, it is sufficient that financial institutions implement a layered approach, consistent with the risk for covered consumer transactions[8];

- For business customers only, strong authentication (so-called "multi-factor authentication") is recommended (but not mandated) for internet transactions.

In MasterCard's view, a RBA should depend on a variety of factors such as:

- *Risk considerations*. As indicated in some parts of the draft EBA guidelines, some internet payments pose more risk than others (e.g. based on transaction amount, the extent to which the same consumer has been previously authenticated in ways that are relevant for the current transaction, the presence/absence of likely fraud indications, etc). In our opinion, strong customer authentication should be optional for payments whose risk is not high.

- *Liability considerations*. In case fraud would occur despite the multiple protections that the various stakeholders have in place, MasterCard has a clear liability framework in place that determines which party is liable for this fraudulent transaction; generally it is the card issuer which is liable (but in some cases the merchant). The cardholder is never liable for fraud, except in some exceptional circumstances[9]. While we welcome and promote the application of strong customer authentication in general, we do not understand why when a PSP (more precisely the card issuer) is prepared to bear the liability in case of fraud, that PSP should not be permitted to decide for itself which level of authentication it wishes to apply – provided of course that the card issuer respects some minimal authentication guidelines and/or does not incur excessive fraud levels. In MasterCard's view, there is no need to mandate upon card issuing PSPs a strong authentication requirement on every transaction when they bear the risk of fraud (as opposed to the merchant, or the cardholder). We believe that less restrictive minimum requirements,

[7] Page 14.

[8] Federal Financial Institutions Examination Council, Supplement to Authentication in an Internet Banking Environment, 2011, pp. 3, 4, available at: http://www.ffiec.gov/pdf/auth-its-final%206-22-11%20(ffiec%20formated).pdf.

[9] As regards liability protection for the consumer, according to Art. 60 and 61 of the PSD1, the liability for unauthorized payment transactions lies in principle with the card issuer (the payer/cardholder is only liable up to max. 150 EUR, in certain special circumstances such as a failure to report his card as lost or stolen payment instrument or if he failed to keep personalized security features safe). In the current draft PSD2, it is proposed that this amount be reduced to 50 EUR, and Art. 66 of the current draft PSD2 specifically states that where the card issuer does not require strong authentication the cardholder does not bear any financial risk unless he acted fraudulently.

complemented by an active monitoring to ensure that fraud levels remain within acceptable limits, are more appropriate.

- *Consumer convenience*. As mentioned above, we believe that a requirement for strong authentication for every card transaction must be balanced with considerations related to consumer convenience, including taking into account the transaction scenario. For example, authentication solutions that involve special hardware devices (such as CAP readers or digipasses) may be appropriate for when consumers are transacting from their home computer; but they are not appropriate for transacting with mobile devices "on the go" or "in-store". More generally, a range of factors can be taken into account to determine the risk of a certain transaction (e.g. consumer having to login in the context of a digital wallet, checking that the consumer device being used for the current transaction is a device previously associated with this consumer, the presence or absence of other risk indicators, etc). We propose that PSPs be permitted to take such type of factors and/or the transaction amount into account to limit the (typically less convenient) strong authentication to the more risky transactions only.

The points that MasterCard made above about why having strong authentication for every card transaction is not recommended apply all the same in the case of a card transaction performed through an e-wallet, such as MasterCard's e-wallet ("MasterPass"). In that scenario, the need to have due consideration for the consumer convenience is all the greater since it is precisely for this convenience that consumer will, or will not, gradually move towards those more innovate means of payments (to the benefit of merchants since e-wallets are expected to reduce the instances of consumers dropping out from website without purchasing, for example because of strong authentication requirements that are impossible, or at least very difficult, to comply with e.g. when making a mobile payment "on the go"). MasterCard is therefore particularly against the requirements in paragraph 7.8. to "*support*" strong authentication either when the consumer logs into its wallet (which is nothing more than the consumer opening his physical wallet in real-life, containing his payment cards – i.e. not a payment transaction as such) or carries out the payment transaction.

It is to be noted that the draft EBA guidelines state that "*The 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, as referred to in the Payment Services Directive*"[10]. This is somewhat similar to the RBA approach that MasterCard has described above – except that, as indicated above, in MasterCard's view the principles should be inverted: RBA should be the norm, and strong authentication the exception (whereas the draft EBA guidelines provide for the opposite).

Registration of a card into an e-wallet

MasterCard generally recommends the use of strong authentication when a consumer stores an additional card in his e-wallet, as referred to in paragraph 7.7[11]. However, it is important to note that there are exceptions where strong authentication is neither reasonably practical (e.g. when the issuer does not offer a practical way for the wallet provider to request it) or not necessary (e.g. when the subsequent payments with the registered cards in those wallets must anyway be subject to strong

[10] Paragraph 7.8.

[11] As a minor/editing comment, MasterCard notes that that the draft EBA guidelines limited this requirement to "legitimate" cardholders, which presumably is an editorial mistake (as otherwise it would mean that issuers should would not be required to perform strong authentication in presence of an illegitimate cardholder trying to register a card into an e-wallet).

authentication at transaction time). For this reason, MasterCard recommends that the EBA does not mandate the use of strong authentication for registering a card into an e-wallet, but make this optional.

Strong customer authentication should be defined in a way that will be aligned with the final text of the PSD2

As indicated above, the final EBA guidelines should be aligned with the final text of PSD2 – and for that reason the final version of the EBA guidelines should not be adopted before the adoption of the final text of the PSD2. It would be particularly unhelpful if the EBA guidelines and the final text of the PSD2 would contain different definitions of "strong authentication".

For example, one of the recent versions of the compromise text for the PSD2 defined strong authentication as an authentication that meets the following conditions:

- "*based on the use of two or more elements categorised as knowledge, possession and inherence*"
- Each of the elements used "*are independent, in that the breach of one does not compromise the reliability of the others*"
- "*is designed in such a way as to protect the confidentiality of the authentication data*"[12].

However the draft EBA guidelines define strong authentication as an authentication that meets the above conditions, plus the additional condition that at least one of the elements used should be:

- "*non-reusable*"
- "*non-replicable (except for inherence)*"
- "*not capable of being surreptitiously stolen via the internet*"[13].

While we acknowledge that the characteristics added in the EBA definition of strong authentication represent desirable characteristics of strong authentication, we believe that the practical difficulties that they raise in today's world make them unfit for inclusion in the definition of strong authentication:

- Most, if not all, objects (possession) and biometrics (inherence) are in principle both reusable and replicable (i.e. both objects and physical attributes can be used many times. Biometric features can likely be replicated through genetic cloning and anyway simpler forms of biometric replication can be likely developed – just think of all the fingerprint marks one leaves on a device with a touchscreen).
- Similarly, there exists no 100% guaranteed protection against being surreptitiously stolen via the internet (except for not using the internet, of course).

Therefore the additional conditions contained in the draft EBA guidelines, if kept without any limitations, would result in the fact that no authentication procedure for internet payments would be considered as "strong" under the EBA guidelines.

Also, and as indicated in the Consultation paper itself, some recent versions of the draft PSD2 compromise text contain an additional requirement that "*payment service providers apply strong customer authentication that shall include elements dynamically linking the transaction to a specific*

[12] Art. 4(22) of the draft PSD2, compromise text of 30 October 2014.

[13] Page 9.

amount and a specific payee"[14]. As mentioned above in our comments to the EBA consultation question, we would welcome a clear alignment also on this point between the PSD2 and the EBA guidelines. In addition, given the controversial nature of this specific point, MasterCard's view is that the EBA should wait until the adoption of the final text of the PSD2.

Also note that if these elements dynamically linking the transaction to a specific amount and specific merchant are to be considered required, then MasterCard would welcome additional clarity on their definition. For example: should these dynamic elements be generated by the same hardware device where the cardholder physically enters its authentication credentials; or would it be sufficient that a downstream system generates them? In the case of a card transaction, would the issuer authorisation approval code qualify as such a dynamic element – which we recommend it should?

Clearer definition of mutual independence of authentication elements

The definition of strong authentication, as stated above, includes the criteria that the authentication elements used are "*independent, in that the breach of one does not compromise the reliability of the others*"[15].

While MasterCard agrees with the intention behind this statement, we propose that the EBA clarifies what authentication elements are deemed "independent" when one is not *directly* compromised as a result of the breach of the other. In other words, we propose that the EBA clarifies that the risk that the compromise of one authentication element might just make it *easier* for a fraudster to breach the other is not sufficient to consider them as failing the independence test. Allow us to illustrate this point with the example of a "Digipass"-based authentication solution:

- The "Digipass" generates a one-time password after the consumer enters a static password (knowledge or "something you know") on a special hardware device that is uniquely associated with the consumer (possession or "something you have").
- If one imagines that a fraudster succeeds in compromising the "Digipass" hardware device in such a way that it modifies the device hardware (breaking the device's tamper resistance) so that, next time the modified device is used, it communicates the static password entered by the legitimate consumer (un-aware of the hardware compromise) to the fraudster.
- This example shows that the compromise of a hardware device can be made in such a manner so as to *ease* the compromise of other authentication elements processed by that same device.

Similar examples can be made when a mobile phone device is used to capture and/or verify biometrics elements or static passwords/PINs. Does this mean that solutions that track a device and use the same device to input or otherwise process other authentication elements always fail the independence test? MasterCard submits that it does not.

In our opinion, such solutions are sufficiently strong (at least when the execution environment for the other element is reasonable protected). MasterCard respectfully requests clarification by the EBA on whether solutions involving these types of situations are deemed "independent" or not.

Clarity is welcomed regarding one-time-passwords

[14] Art. 81(1a) of the draft PSD2, compromise text of 30 October 2014.

[15] EBA Consultation paper, page 9.

MasterCard would welcome clarifications from the EBA on how one-time passwords should be assessed in light of the proposed definitions. In our opinion, one-time passwords, in of themselves, do not directly authenticate consumers as they are machine-generated. What authenticates consumers is the authentication procedure that gives them access to the machine (or system) that generates and/or communicates the one-time password. MasterCard believes that this is an important consideration because some one-time password systems are stronger than others because of this.

As an example, consider the following three different types of one-time-password solutions: cap reader, SMS with one-time password, and e-mail with one-time password:

- The CAP reader solution relies on the possession of the physical plastic/chip card (something you have) and the knowledge of the PIN (something you know).
- The SMS solution relies on the possession of the SIM card corresponding to the phone number (something you have) and its associated mobile phone PIN (something you know).
- But the e-mail solution typically only relies on the static password required to access the e-mail account (something you know).

MasterCard proposes that the EBA clarifies how the authentication strength of one-time password systems is to be assessed.

Transaction Monitoring

MasterCard fully supports paragraph 10.1 of the draft EBA guidelines that transaction monitoring mechanisms designed to prevent, detect and block fraudulent payment transactions should be operated before the PSP’s final authorisation, and that suspicious or high risk transactions should be subject to a specific screening and evaluation procedure.

However, MasterCard wishes to draw the EBA’s attention to Article 20 (“Measures based on profiling”) of the draft General Data Protection Regulation (“GDPR”), which could potentially restrict payment schemes’ and PSPs’ ability to implement this guidelines and effectively fight against fraud.

Profiling under Article 20 of the GDPR is very broadly defined and could apply to numerous legitimate activities such as fraud monitoring and prevention activities. In practice, payment schemes and PSPs could be required to obtain the cardholder’s express consent to conduct transaction monitoring and anti-fraud activities, unless those activities are expressly authorised by a EU or Member State law. Obtaining consent is not a workable solution, given that consent – to be valid – must be explicit, specific and can be withdrawn by the individual at any time. It is therefore critical that, at a minimum, payment schemes and payment service providers are expressly authorised in the PSD II to process personal data for anti-fraud purposes.

We very much welcome the latest compromise text of the PSD II (Art. 84) which reverts back to the data protection provision in PSD I (Art. 79) and provides that payment schemes and payment service providers are permitted to process personal data for anti-fraud purposes. This being said, it is unclear whether this permission will be specific enough to legitimise the transaction monitoring mechanisms recommended by the EBA and meet the test under GDPR.

In order to provide for a more appropriate and flexible regime, we are of the view that the GDPR and in particular Article 20 should reflect a Risk Based Approach. Profiling is not negative *per se*; it is the use of profiling that can have negative implications for the consumers, depending on the context – e.g. whether it is used for marketing or anti-fraud purposes. Implementing a Risk Based Approach would ensure effective data protection while enabling the use of transaction information for innovation, including for deploying sophisticated anti-fraud solutions.

In light of the above, we would encourage the EBA to reach out to MEPs and Council representatives responsible for drafting the GDPR to educate them about the potential concerns raised by the proposed profiling rules and to promote a Risk Based Approach, so as to allow the processing of personal (transaction) data to contribute to "*fighting payment fraud and enhancing consumer trust in internet payment*"[16].

Incident monitoring and reporting

MasterCard, as a technology company, is of course highly engaged in the raising of security standards and supports the need for incident monitoring and reporting as provided for in paragraphs 3.1 to 3.4 of the draft EBA guidelines, in order to ensure the overall trust in the Digital Economy.

There is however a crucial need to coordinate and streamline reporting and notification obligations that exist under current or future regulatory regimes (including the PSD II, NIS Directive, and GDPR). Otherwise, there is a risk that payment schemes and PSPs would be subject to multiple incident reporting obligations in multiple countries, to multiple authorities, requiring different types of information in different formats and sometimes in different languages. Payment schemes and PSPs would then need to dedicate an enormous amount of time and resources to those reports, rather than focusing on the appropriate management and containment of the incident.

[16] Page 8 of the EBA Consultation paper.