Valdis Dombrovskis
Vice-President for the Euro and Social Dialogue, Financial Stability, Financial Services and Capital Markets Union
European Commission
Rue de la Loi 200
1040 Brussels, Belgium

25 November 2016

Dear Vice-President Dombrovskis,

We are writing to you collectively from across various sectors and all players in the payments value chain with regard to the European Banking Authority's ("EBA") proposed draft Regulatory Technical Standards ("standards") on Strong Customer Authentication ("strong authentication") and secure communication, under the revised Payment Services Directive (PSD2). We fully support the aims of the PSD2 to ensure fair competition, innovation and security in the payment services sector. The PSD2 and the EBA standards are important steps towards a Digital Single Market (DSM) in Europe. We endorse the objectives of the standards and appreciate the difficulty the EBA has faced in trying to find the right balance between security and customer convenience. However, we have strong concerns that if the EBA's standards were implemented in their current form, it would create unnecessary hurdles for a number of different industries, especially e-commerce.

We believe that the EBA diverges from its mandate under the PSD2 by not allowing for the risk-based approach to authenticate customers and authorize transactions to avoid fraud. The PSD2 under article 98 requires an exemption from strong authentication based "on the level of risk involved in the service provided". We would encourage the EBA to introduce more flexibility within its standards to support the industry with all of the positive work that has been achieved in combatting fraud through risk-based approach. A reduction in fraud rates in the EU confirms that the industry has actively worked to manage fraud well through this approach as the move to digital commerce has massively expanded in the past few years. A recent study[1] shows that in the UK and France combined, fraud rates for online transaction value of cards issued have declined at an average rate of 13.5% per year, an overall decline of 51%. Online fraud rates at single country level confirm this downward trend.

We are fully aligned with regulatory objectives to reduce fraud to the lowest possible level which is in the interest of all parties in the payments chain. Our concern is that by choosing a very blunt approach and disregarding some of the highly innovative approaches to authentication and risk management – which are already demonstrably working in the market – this goal will not be achieved and the consequences will be highly disruptive. Today, a risk-based approach enables the merchant and the Payment Service Provider (PSP) to combine consumer intelligence and security decisions by analysing dozens of elements. For example, if you enter a website to purchase a product, the merchant may recognise your transaction as low risk because you are a regular returning customer to whom they have previously and successfully provided a service or delivered a product, or a PSP may recognise that you have previously purchased from that site using that particular computer or mobile device. Whereas uncharacteristic or unusual behaviour – such as changes to the customer's personal or security details in the online account – would trigger additional checks.

A risk-based approach also enables the appropriate party – be it the merchant, the card issuer or the PSP – to implement the right decision for their business and their customers. If it fails, the consumer is fully protected, unless proven to act fraudulently or with gross negligence. The industry has worked very hard to ensure that customers do not become the victim of fraud. Consumer confidence and payment security are an essential part of our businesses. Nevertheless, we must also keep the customer experience frictionless. A consumer survey by Populus found that 61% of consumers would abandon their purchases if supplementary steps were added to the checkout process[2]. This would be particularly damaging for small merchants who need every sale they can get and who are key to the further growth of the e-commerce sector in Europe.

Currently, the EBA is taking a more prescriptive approach by mandating strong authentication for all remote payment transactions over 10 euros, regardless of their risk. Strong authentication is a process which typically requires the customer to authenticate a payment by using two elements, for instance by utilizing additional codes generated through their card reader or received on their mobile device. Strong authentication may make sense for some payments which have a higher transactional risk. However, for low-risk transactions (which are not necessarily low value), strong authentication introduces disproportionate and unnecessary friction to the customer shopping experience.

This will make online shopping much more onerous than it is today and have a wider and chilling effect on the DSM. It will have a negative impact upon a wide variety of industries, in particular SMEs, FinTech and other start-ups. At the same time, it will not improve overall security. Institutionalizing a single method of authentication over many different and innovative ways of authenticating the customer will potentially make transactions more prone to fraud as fraudsters are more likely to effectively target rigid rules that do not evolve quickly. Moreover, European PSPs

[1] CleverAdvice study: https://www.ecommerce-europe.eu/press-item/3870/
[2] Populus consumer survey: https://vision.visaeurope.com/blogs/disruption-for-europes-online-shoppers

may be forced to decline payments by European customers on foreign websites which do not offer strong authentication. This will result in an increase in consumer harm by reducing customer trust in their payment methods, the choices open to them and restricting competition.

We therefore urge the European Commission to work with the EBA to incorporate in their draft standards a results-oriented and technology-neutral risk-based approach, as detailed in the Annex, rather than a threshold-based technology-specific approach. The risk-based approach will foster a continued decline in fraud for the benefit of all stakeholders and the European economy alike, without enforcing hard rules that would stifle sales and significantly impact the consumer shopping experience. We are committed to cooperating with the relevant authorities to demonstrate our effectiveness in preventing fraud.

The undersigned 39 European and national organisations representing e-commerce, small merchants, start-ups, ICT and digital technology, payments and FinTech, cards, telecoms, foreign trade, and leisure and travel industries


ECOMMERCE
EUROPE


DIGITALEUROPE


EPIF
European Payment Institutions Federation aisbl


ECPA
European Card Payment Association


EuroCommerce


AIRLINES
FOR
EUROPE


ecta


ETTSA
EUROPEAN TECHNOLOGY & TRAVEL SERVICES ASSOCIATION

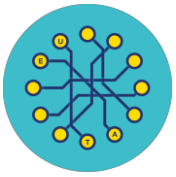

European
Holiday Home
Association


FTA
Foreign Trade Association


EDiMA


COADEC


EMOTA
The European eCommerce
& Omni-Channel Trade
Association


European Tech Alliance


Financial Fraud Action UK
Working together to prevent fraud


bevh


Choice in
eCommerce
Initiative for Choice and
Innovation in Online-Trade


BVOH
e.V.


PaymentsUK


adigital
SPAIN DIGITAL ECONOMY ASSOCIATION


techUK


Händlerbund


Computer & Communications
Industry Association
Tech Advocacy Since 1972


fevad
www.fevad.com
fédération e-commerce
et vente à distance


netcomm
IL CONSORZIO DEL COMMERCIO ELETTRONICO ITALIANO


THE
UKCARDS
ASSOCIATION


be commerce
GUARANTEED


thuiswinkel
.org


pif


VERKKOTEOLLISUUS
ECOMMERCE FINLAND


bvzi
Bundesverband der
Zahlungsinstitute


CBII


VIR
VERBAND
INTERNET
REISEVERTRIEB
WWW.V-I-R.DE


BRC


bank
axept


P/D
Prepaid
Verband
Deutschland


HDE
Handelsverband
Deutschland


PaySys
Consultancy GmbH

EPSM

List of co-signing organisations and links to their websites:

1. A4E (Airlines for Europe)
2. Adigital
3. Bank Axept
4. BeCommerce vzw
5. British Retail Consortium
6. Bundesverband der Zahlunginstitute (BVZI)
7. Bundesverband E-Commerce und Versandhandel Deutschland e.V (BEVH)
8. Bundesverband Onlinehandel e.V. (BOVH) / Choice in eCommerce
9. Computer and Communications Industry Association (CCIA)
10. Confederation of British Industry
11. DigitalEurope
12. E-Commerce Europe
13. Eurocommerce
14. European Association of Payment Service Providers for Merchants (EPSM) e.V.
15. European Card Payment Association (ECPA)
16. European Competitive Telecommunications Association (ECTA)
17. European Digital Media Association (EDiMA)
18. European eCommerce and Omni-Channel Trade Association (EMOTA)
19. European Holiday Home Association (EHHA)
20. European Payment Institutions Federation (EPIF)
21. European Tech Alliance (EUTA)
22. Financial Fraud Action UK
23. FTA (Foreign Trade Association)
24. Handelsverband Deutschland (HDE)
25. Händlerbund
26. IK Interessengemeinschaft Kreditkartengeschäft
27. La Fédération du e-commerce et de la vente à distance (FEVAD)
28. Le Groupement des Cartes Bancaires (CB)
29. Netcomm
30. Payments UK
31. Prepaid International Forum (PIF)
32. Prepaid Verband Deutschsland
33. TechUK
34. The Coalition for a Digital Economy (Coadec)
35. The European Technology and Travel Services Association (ETTSA)
36. The UK Cards Association (UK Cards)
37. Thiuswinkel.org
38. Verband Internet Reisevertrieb e.V. (VIR)
39. Verkkoteollisuus

Annex

1. Risk-based approach (RBA) is demonstrably as effective as Strong Customer Authentication (SCA) at reducing fraud. Imposing SCA on all payment transactions would be disproportionate.

RBA gives payment service providers (PSPs) greater flexibility and ability to detect and prevent attempted fraud. If fraud is not intercepted, the PSD2 itself includes a number of provisions which provide significant protection to the consumer regardless of whether SCA is applied or not. RBA has been used successfully by the payments industry for a number of years and is the market standard in some EU countries.

It uses sophisticated tools such as risk profiling which assesses multiple elements, for example: (1) device checks – Which device? Is it their regular device? Is it located at their home address?; (2) behavioural checks – Is this a 'normal' transaction for this customer? Is it their home currency? Have they purchased from this merchant before?; and (3) merchant checks – What sort of purchase are they making? Is the type of transaction common for the merchant? Has there been significant fraud at the merchant? All these factors and many more are used by the various stakeholders in the payment process to decide whether to either: (a) allow the payment to pass; (b) interrupt the transaction for additional verification; or (c) block the payment entirely.

RBA is demonstrably as effective as SCA in preventing fraud. For example, Barclays allows the authorisation of approximately 95% of transactions through a risk-based approach, reducing the level of friction experienced by the consumer. RBA has succeeded in containing fraud across all sectors at approximately 0.1%. There has been no change in the headline rate of fraud relative to when SCA was used. Carpooling service BlaBlaCar initially applied strong authentication on transactions over a certain amount. When they increased the threshold in a significant way, they saw two things: (1) no change in the fraud rate (i.e. risk-based approach was equally effective); and (2) better customer experience led to much larger conversion.

Moreover, a one-size-fits-all approach cannot be adopted when different businesses and business models present inherently different risks. For example, the top 10 of e-commerce fraud prone merchant sectors represent over 50% of the total UK domestic e-commerce fraud, and over 45% of the total international e-commerce fraud. In contrast, the 10 merchant sectors with the least fraud represent less than 0.01% of domestic and international e-commerce fraud combined. The European Banking Authority's (EBA) Draft Regulatory Technical Standards (RTS) would apply the same authentication model to all of these merchants which would be largely disproportionate.[3]

2. Legitimate customer transaction rates decrease when SCA is used.

The industry experience suggests that SCA will result in a much higher abandonment of transactions by genuine customers and significantly decrease merchant sales. SCA can discourage fraudulent customers but also regular customers who may get frustrated about cumbersome security requirements. A recent consumer survey found that 61% of consumers would abandon their purchases if supplementary steps were added to the checkout process[4]. According to Ecommerce Europe[5], the European B2C ecommerce market will pass the €500 billion mark in 2016. The EBA's Draft RTS would have a significant detrimental impact on this flourishing segment of the European economy.

3. The Payment Services Directive (PSD2) does not require SCA on all transactions over €10, as included in the Draft RTS.

Article 98 (1) and (3) of the PSD2 requires the EBA to specify exemptions to SCA based on the level of risk, the amount and recurrence of a transaction, and the payment channel:

Article 98
Regulatory technical standards on authentication and communication
1. EBA shall, in close cooperation with the ECB and after consulting all relevant stakeholders, including those in the payment services market, reflecting all interests involved, develop draft regulatory technical standards addressed to payment service providers as set out in Article 1(1) of this Directive in accordance with Article 10 of Regulation (EU) No 1093/2010 specifying:
(a) the requirements of the strong customer authentication referred to in Article 97(1) and (2);
(b) the exemptions from the application of Article 97(1), (2) and (3), based on the criteria established in paragraph 3 of this Article; […]

3. The exemptions referred to in point (b) of paragraph 1 shall be based on the following criteria:
(a) the level of risk involved in the service provided;
(b) the amount, the recurrence of the transaction, or both;
(c) the payment channel used for the execution of the transaction.

[3]Calculated on the basis of the FFA UK fraud report (January-June 2016): https://www.financialfraudaction.org.uk/wp-content/uploads/2016/07/October-2016-fraud-figures-bulletin-final.pdf
[4] Populus consumer survey: https://vision.visaeurope.com/blogs/disruption-for-europes-online-shoppers
[5] European B2C Ecommerce Report 2016: https://www.ecommercewiki.org/Prot:European_B2C_Ecommerce_Report_2016

In the Draft RTS which were consulted on until 12 October 2016, the EBA has only included exemptions based on the transaction amount and the recurrence. In order to comply with the EBA mandate in the PSD2, the RTS should include an exemption based on the risk involved in the service provided in line with Article 98. This is also explained in Recital 96 of the PSD2 which says that "the security measures should be compatible with the level of risk involved in the payment service".

4. The EBA RTS should incorporate the RBA by including an exemption based on the "risk of the service provided" and by explicitly acknowledging the use of alternative authentication methods for low-risk transactions.

We strongly recommend that the EBA makes the following two changes in order to comply with its mandate and the objectives of the PSD2.

1. Include an exemption for the PSP based on the "risk of the service provided".

Article 98 of the PSD2 requires that the EBA include exemptions to perform the SCA based on the "risk of the service provided". This exemption is key for PSPs to adopt a risk-based approach to their customers' transactions. In order to ensure competition and not to hamper innovation in this space, a flexible approach to this exemption is needed. A flexible approach would facilitate competition and innovation in this space, whilst enabling PSPs to adapt their risk analysis to the conditions and the threats that vary widely from market to market. Monitoring – which is the current practice under the ECB SecuRe Pay Recommendations and the EBA Guidelines for the security of payments on the internet – can ensure that the risk-based approach is being properly applied.

These measures can be included in the Draft RTS by introducing the following wording in 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 of that customer to evaluate the latter's typical spending and behaviour patterns, (ii) information about the customer device used and where applicable (iii) a detailed risk profile of the payee and the payees device ,
(b) proven to be efficient for fighting against fraud and assessed according to Article 7,
(c) are continuously reviewed according to fraud rates and improved in order to address new fraud scenarios and new technological threats."

2. Explicitly acknowledge the right of merchants and their PSPs to adopt alternative methods of authentication for low-risk transactions.

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. According to Article 74 of the PSD2, the payer will always be protected, unless gross negligence or fraudulent behaviour is proven, and the liability regime for SCA is clearly established. There is no objective reason to take away from payees and PSPs the possibility to adopt alternative methods of authentication. On the contrary, depriving payees and PSPs of 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 PSPs to actively decide whether SCA is needed to secure a transaction according to the risks involved, in exchange for taking liability for unauthorised transactions in case of fraud. From a legal point of view, the PSD2 is the level 1 legislation that can only be amended by another Directive, not by level 2 measures like the RTS. The terms of article 74.2 are therefore valid for the entire validity period of the PSD2. The EBA suggestion that the provisions of article 74.2 are provisional are therefore questionable from a legal point of view and likely to be challenged.

In line with the EBA Guidelines for the security of internet payments and the PSD2, the Draft RTS should re-instate the ability of the payees and 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".