Technical Standards on online Payments continue to pose risk to European e-commerce

Ecommerce Europe remains strongly concerned about the European Banking Authority's final draft RTS on Strong Customer Authentication. The European Commission now must make the necessary changes, or put at risk the competitiveness of the European e-commerce sector.

Ecommerce Europe stresses that the draft standards fail to address the importance of the merchant side to the application of TRA. By not accounting for the customer information held by online merchants, valuable information that only online merchants have will be lost as a factor of minimizing transactional risk. More legitimate payment transactions will thus be declined as customers' PSPs/banks will not be able to pinpoint all low-risk transactions.

As Ecommerce Europe highlighted in a pan-industry letter to European Commission Vice-President Dombrovskis. players across the electronic payments value-chain agree that the merchant side should be allowed to apply Transactional Risk Analysis to the benefit of increased payment security without creating unnecessary friction to the customer checkout experience. We urge the Commission to work with the European Banking Authority and the e-commerce industry to address the below points in line with the spirit of the revised Payment Services Directive and to the benefit of the EU's Digital Single Market.

******

1. **Merchants and their PSPs must be given the option to use TRA, and their individual fraud rates must be taken into account:**

The draft technical standards only allow banks and payment service providers (PSPs) to perform the TRA; merchants are not directly allowed to use the TRA. Merchants have unique data points which provide essential warning signs to prevent fraud, for example historical information on customer (i.e. payer) behaviours, browsing and purchasing patterns. The draft standards also make the payer's PSP the ultimate decision-maker on whether a transaction should benefit from the TRA. This is not in line with Article 97 in the PSD2 which is agnostic as to which PSP (i.e. the payer's PSP or the merchant's PSP) should own the final decision. In fact, the merchant and its PSP are in an ideal position to make the decision as they have access to unique information regarding both the merchant (e.g. fraud patterns specific to the payee's activity) and the payer (see above). Furthermore, by having a say in the final decision on the application of TRA, the merchant's PSP has an economic incentive to improve its Reference Fraud Rates for a given electronic payments instrument.

2. **TRA must apply to the dynamic linking requirement:**

It is an established industry practice to provide customers with a choice to split multi-item orders into several shipments which can be sent at different dates as individual products become available. For remote transactions, customers are typically only charged when items ship (in accordance with card schemes' rules). This results in several charges of differing amounts all adding up to the total of the order. In its current form, the draft standards would not allow merchants to pursue this practice without generating and showing the customer a new 'authentication code' for each split payment. This would not be possible as customers will have already checked out of the online shopping experience and would require that the full amount of the transaction be charged at once, regardless of whether items have been shipped or not. This is not in line with Article 98(1)(b) of the PSD2 which requires that risk-based exemptions be included also for the dynamic linking requirement. The TRA exemption should therefore be applied in justified cases like multiple charges and price adjustments at checkout (e.g. reflecting final VAT rate or shipping cost). This is the case

today when split shipments are processed as multiple authorization requests when submitted with the original authentication data. The total amount of the split transaction can vary from the original authentication by up to 15%, allowing for the reflection of any additional costs associated with the items. This approach ensures security of online transactions, while providing merchants the flexibility to meet customer requirements.

3. **Fraud tolerance thresholds should be simplified, based on available industry norms and applied to all transactions, with no upper transaction limit:**

The Exemption Threshold Values (ETVs) proposed by the EBA are overly complex and it is unclear how they will be calculated. Moreover, fraudsters have been known to quickly exploit any static regulatory thresholds. Any limits based on the transaction amounts are therefore not desirable. Thresholds for the industry should be collected, categorized and set through collaboration amongst merchants, issuers and processors who remain committed to the reduction of fraud rates through an adaptive approach, for example through ambitious but achievable blended fraud rate based on the existing industry fraud rates. This fraud rate could be reviewed on a regular basis to ensure continuous progress on the part of the industry, as provided for by Article 32 of the draft standards. Alternatively, as fraud rates and risk vary significantly between countries, industry sectors and merchant sizes, a sector-specific approach could be taken to measure the fraud using available industry data.

About Ecommerce Europe

Ecommerce Europe is the association representing 25,000+ companies selling goods and/or services online to consumers in Europe. Founded by leading national e-commerce associations, Ecommerce Europe is the voice of the e-commerce sector in Europe. Its mission is to stimulate cross-border e-commerce through lobbying for better or desired policy, tabling the e-commerce sectors' demands on the agenda of those designing the necessary standards and regulations, by offering a European platform bringing the European e-commerce sector and other stakeholders together, and by providing in-depth research data about European markets. Moreover, Ecommerce Europe provides more than 10,000 certified online companies across Europe with a European Trustmark label, with the aim of increasing consumers' trust in cross-border purchases.

Website: www.ecommerce-europe.eu
Trustmark: www.ecommercetrustmark.eu

National associations that are members of Ecommerce Europe

Belgium	BeCommerce	www.becommerce.be
Bulgaria	Bulgarian E-commerce Association	www.e-commerce.bg
Czech Republic	APEK	www.apek.cz
Denmark	FDIH	www.fdih.dk
Finland	KAUPPA	www.kauppa.fi
Finland	Verkkoteollisuus	www.verkkoteollisuus.fi
France	FEVAD	www.fevad.com
Germany	Händlerbund e.V.	www.haendlerbund.de
Greece	GRECA	www.greekecommerce.gr
Hungary	SzEK.org	www.szek.org
Ireland	Retail Excellence Ireland	www.retailexcellence.ie
Italy	Netcomm	www.consorzionetcomm.it
Luxembourg	eCOM.lu	www.ecom.lu
The Netherlands	Thuiswinkel.org	www.thuiswinkel.org
Norway	Virke eHandel	www.virke.no
Poland	e-Izba	www.eizba.pl
Portugal	ACEPI	www.acepi.pt

Romania	ARMO	www.armo.org.ro
Spain	Adigital	www.adigital.org
Switzerland	NetComm Suisse	www.netcommsuisse.ch

Contact
Ecommerce Europe AISBL
Rue de Trèves 59-61, B-1040 Brussels, Belgium
Website: www.ecommerce-europe.eu
Trustmark: www.ecommercetrustmark.eu
Twitter: @Ecommerce_EU

Press contact Ecommerce Europe
Marlene ten Ham
Secretary General
Tel.: +32 2 502 31 34
Email: marlenetenham@ecommerce-europe.eu