DIGITALEUROPE

16 MARCH 2020

DIGITALEUROPE Position on transaction amount tolerance for dynamic linking in the context of Strong Customer Authentication

Introduction

DIGITALEUROPE, along with its members, is committed to the creation and enablement of a digital future for European consumers and businesses in which safety and security plays a crucial role. DIGITALEUROPE is a strong supporter of the Strong Customer Authentication (SCA) requirements in the digital payment space, as it aims to strengthen the security, and with it the foundations, of the increasingly relevant electronic payments, especially in online commerce.

As with every groundbreaking and visionary regulation, it needs to be aligned with market realities and business practices in order to bring its intended benefits while at the same time ensuring business continuity and high quality of user experience. It is for this reason that DIGITALEUROPE would like to bring to the attention technical challenges during the implementation of the dynamic linking requirement in the context of SCA. Obliging consumers to authenticate their credit card purchases for a second time risk creating inconveniences for consumers and increase costs for merchants. Our paper offers an alternative approach to second authentication where we believe will protect the security of the transaction, protect the consumer's right, and avoid lost sales for merchants and in distrust in e-commerce and electronic payments for consumers.

Transaction amount tolerance

The regulation on SCA requires that, for remote transactions, the authentication code is specific to the transaction amount and payee (Article 5(1)(b) RTS). The RTS also require that "*any change to the amount or the payee results in the invalidation of the authentication code generated*" (Article 5(1)(d) RTS).

DIGITALEUROPE would like to bring to attention that the above requirement poses significant technical challenges for card-based transactions for which the final amount of the transaction is unknown at the time of authentication. In current

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

business practice, this might be the case for online grocery shopping, shipping and miscellaneous charges, and currency conversion, among others.

For example, in case of the online purchase of groceries, a consumer may typically authenticate for a provisional amount, and agree to the final amount increasing on the basis of the actual weight of the groceries. The consumer may also agree to additions to basket, or replacement of out-of-stock products, which would typically alter the final amount of the transaction. Requiring the consumer to authenticate for a second time when the final amount is determined would create inconveniences for consumers and increase costs for merchants, as the consumer might be unable to conveniently authenticate for a second time (for example due to being offline at the time of the second authentication requirement). If the consumer delays logging on the merchant website to authenticate for a second time, or does not eventually authenticate, the purchase or shipping will be delayed or aborted. This would result in lost sales for merchants and in distrust in e-commerce and electronic payments for consumers.

Requiring the consumer to authenticate for a second time will also not increase security. The consumer has already authenticated the transaction once. The transaction is therefore legitimate and secure. To our understanding, the dynamic linking requirement was created to prevent man-in-the-middle attacks in a credit transfer environment. Man-in-the-middle attacks are virtually impossible in a card environment. The EMV 3DS cryptogram (authentication code) cannot be intercepted, forged or re-used for a different fraudulent transaction. EMV 3DS ensures confidentiality, authenticity and integrity of the cryptogram for the entire transaction flow, ensuring cardholder protection against man-in-the-middle attacks. A second authentication by the cardholder is therefore redundant from a security perspective.

DIGITALEUROPE believes that the issue is therefore not about security under Article 97 PSD2, but about consent to the incremental amount under the consumer rights of PSD2. Article 76(1) PSD2 envisages that for transactions for which the final amount is unknown the final amount may vary, and the payer is entitled to a refund if the final amount exceeds what s/he could reasonably have expected. Therefore, if the consumer has already authenticated and consented to the final amount increasing after authentication, and this increase is within the consumer's reasonable expectations, a second authentication by the consumer is redundant from a consumer rights perspective.

For these reasons, we believe that a sensible approach for transactions for which the final transaction amount is unknown is that the final amount may be higher than the amount authenticated, without a separate authentication for the incremental amount being required, if both of the two following conditions are met:

(1) The consumer has consented to the final amount increasing after authentication.

(2) The increase does not exceed the consumer's reasonable expectations within the meaning of Article 76(1) PSD2.

If either condition is not met, a separate authentication for the incremental amount will be required.

Finally, please note that the pre-authorization model envisaged by Article 75 PSD2 does not provide a convenient solution. With pre-authorization, the consumer is generally required to authenticate the expected transaction amount plus a certain margin. The funds are blocked on the consumer's account until the issuer is informed of the exact final amount (and at the latest immediately after receipt of the payment order). This may result in the consumer's funds being blocked for several days. During this period, the availability of funds on the card may be significantly reduced or even zeroed. This may result in serious inconveniences for the consumer.

DIGITALEUROPE appreciates this topic and the above comments being considered, and we are open to further discussions in order to find a sensible solution for European digital commerce.

FOR MORE INFORMATION, PLEASE CONTACT:

Ray Pinto

Digital Transformation Policy Director

ray.pinto@digitaleurope.org / +32 472 55 84 02

Vincenzo Renda

Senior Policy Manager for Digital Industrial Transformation

vincenzo.renda@digitaleurope.org / +32 490 11 42 15

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Airbus, Amazon, AMD, Apple, Arçelik, Bayer, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Epson, Ericsson, Facebook, Fujitsu, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, MasterCard, METRO, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Qualcomm, Red Hat, Ricoh Europe PLC, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, UnitedHealth Group, Visa, VMware, Xerox.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Teknikföretagen, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK