DIGITALEUROPE

12 August 2024

PSR: Reaction to Council discussions on authorisation and gross negligence

Authorisation

The Risk of a Subjective Approach to Authorisation

The proposed Payment Services Regulation (PSR) replaces 'authentication' with 'authorisation' in Art.55 *(Evidence on authorisation and execution of payment transactions).* The European Parliament has subsequently **linked authorisation with the intent/willingness of the consumer to carry out/authorise a payment transaction** by noting in its position (Recital 79a) that *"with regards to the authorisation of payment transactions, permission should entail the intention of the payer on the basis of full knowledge of relevant facts including amount, recipient and purpose of the transaction".* Again, this is relevant because Art.55 refers to **payment services providers (PSPs) having to prove a payment transaction was authorised,** in the case that a payment service user (PSU) denies having authorised or executed a transaction.

DIGITALEUROPE is concerned about the inclusion of such a subjective component into the definition of authorisation. By defining authorisation through the PSU's permission and will (subjective element), **the PSP would have no objective standard to verify the authorisation.** It is worth noting here that we laud the Belgian Presidency for having attempted to define the "subjective component" as narrowly as possible via their proposed amendment to Art.49(2): *"A payment transaction shall not be deemed as authorised where the payer was manipulated through social engineering into initiating the payment transaction in favour of a third party which was not the intended payee, or where the transaction was initiated by a third party using the personal security credentials of the payment service user fraudulently obtained".* That being said, it should be noted as these discussions continue, that narrowing the subjective component whilst still keeping the "intention" element in the definition in any respect, remains highly concerning.

Practically, this means that payment orders could become reversible and conditional in nature because **PSUs could challenge all transactions based on a lack of intent, obliging the payer's PSP to refund said transactions.** In a worst-case scenario, we may find ourselves in a situation whereby PSPs will be obliged to refund customers the amounts of **all**

DIGITALEUROPE
Rue de la Science, 37, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

transactions reported as unauthorised. This could lead to significant losses for PSPs operating in the EU, a surge in legal proceedings in the EU and could ultimately endanger the stability and confidence of our financial system as a whole.

Second, this subjective approach may also induce fraudsters to **take advantage of the PSR and recover money from the PSP that is not theirs to recover,** by claiming they did not "intend" to authorise the payment – with no need to "prove" this lack of intent.

Importantly, proving the "inner will/intent" of a customer would be excessively burdensome **if not impossible for the PSP.** Overall, it could also lead to payers paying less attention to how they use their Strong Customer Authentication (SCA) credentials and engaging in potentially risky behaviours (sharing credentials, declaring them lost or stolen…) **therefore reducing the overall performance and trust of the SCA solution.**

Finally, the subjective approach **may also risk disincentivising PSPs from investing in new forms of SCA.** When held liable regardless of whether SCA was used in a particular transaction, **the PSP has no financial incentive to continue to invest in such technology.**

Authorisation vs Authentication

Authentication and authorisation are two fundamental security processes that serve different purposes. As outlined in the Polish non-paper that clearly describes this issue:

- Authentication refers to a technical procedure which allows the PSP to verify the identity of a PSU or the validity of the use of a specific payment instrument. For example: Strong Customer Authentication (SCA).

- Authorisation – as per the Polish non-paper - refers to the consent (please see below our comments that 'permission', not consent, should be used in the definition of authorisation) given by a user, to execute a given payment transaction. The manner of this consent is dependent on the individual contract. Necessary components of authorisation are 1) the will and 2) its expression (externalisation).

It is key to understand that **the will (authorisation) is usually expressed through the authentication procedure.** The PSP, by necessity, must rely on the externalisation of will (i.e. the authentication procedure) as evidence that the PSU intends to authorise the transaction. **Without this externalisation, the PSP has no objective way of measuring or discerning the PSU's will, given that an individual's will is inherently internal and subjective**.

DIGITALEUROPE's Recommendation

For the aforementioned reasons, we strongly urge co-legislators to refrain from adding subjective elements to the concept of authorisation. **We propose that first, a clear objective definition of authorisation be included in PSR. Second, that this definition be combined with an approach to manage customer losses.** Such an approach could build on the Dutch approach, whereby banks/PSPs refund losses, for both bank impersonation fraud and phishing, but importantly, subject to certain criteria (namely, no gross negligence).

We believe that the definition of authorisation proposed by the Polish, is logical and should be used in the PSR Regulation. However, it should replace the word 'consent' with 'permission':

'Authorisation' means a payment service user's ~~consent~~ permission to execute a payment transaction or to perform other activity carried out by the payment service provider which is considered to be given if correct authentication has been made. Permission ~~Consent~~ to execute a payment transaction may also be given via the payee or the payment initiation service provider.

The notion of consent when describing 'authorisation'

As mentioned above, a further example of where **the effectiveness of the legislation could be undermined if inaccurate terminology is used is in relation to the use of the term 'consent' instead of 'permission' when describing 'authorisation'.**

The term 'consent' should only be used in the context of the GDPR. Reintroducing the term 'consent' to replace 'permission' would only add legal uncertainty. It is essential we learn from previous drafting experience, which illustrate the challenges caused by using the same terminology

Gross Negligence

First, we note and welcome the set of criteria to assess gross negligence laid out by the Council and agree that this is useful. We propose to add a point to its list, that: *"the customer has followed procedures and recommendations by the PSP to prevent fraud and has not ignored explicit warnings issued by the PSP on possible fraud that were issued during the payment process".* This addition **mirrors the liability regime introduced for payers authorising payment transactions despite the warning of the payer's PSP** that the payment may not land with the intended beneficiary.

Second, **a non-cumulative list of examples to help determine when consumers have been grossly negligent could be useful to help harmonise the application of the PSR across the bloc.** It should be made clear that only one of the below examples need occur to determine gross negligence has occurred. Recital 82 of the PSR contains two examples[1] of situations that shall be deemed gross negligence. We believe this list would benefit from the addition of further examples, such as:

- Ignoring messages from the bank or other payment service providers that specifically warn the client of the risk of scams.
- Not carefully reading the operation authorisation messages before accepting their execution. I.e. carrying out payments where the amount, transaction type (e.g. tokenisation of card, recurring payment or subscription) and merchant displayed (e.g. during checkout or in the authentication message sent to the cardholder) do not reflect the intended payment.
- Persuading the payment service provider to lift the block placed after a fraud alert with instructions from the fraudster.
- Transferring money to foreign accounts under suspicious circumstances and opening one or more crypto wallets at the instruction of the fraudster to keep their money 'safe there'.
- Sharing payment card or online banking credentials including OTP, CVV and card online banking pin with third parties, even if they present themselves as bank employees, a payment service provider or third-

[1] keeping the credentials used to authorise a payment transaction beside the payment instrument in a format that is open and easily detectable by third parties; and the fact that a consumer has already received a refund from a PSP after having fallen victim of bank employee impersonation fraud and is introducing another refund claim to the same PSP after having been again victim of the same type of fraud could be considered as 'gross negligence' as that might indicate a high level of carelessness from the user who should have been more vigilant after having already be victim of the same fraudulent modus operandi.

party service provider such as tax authorities, postal couriers, telecommunication provider or otherwise.

- Allowing others to use one's device with their biometrics enabled and stored in the device, either physically or through a remote-control application.

FOR MORE INFORMATION, PLEASE CONTACT:

Laura Chaney

Manager for Digital Finance Policy

laura.chaney@digitaleurope.org / +32 493 09 87 42

Ray Pinto

Senior Director for Digital Transformation Policy

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

DIGITALEUROPE

About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies. We wish Europe to grow, attract, and sustain the world's best digital talents and technology companies. Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies. Our membership represents over 45,000 businesses that operate and invest in Europe. It includes 108 corporations that are global leaders in their field of activity, as well as 41 national trade associations from across Europe.

DIGITALEUROPE
Rue de la Science, 37, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20