CERTFin

Il Salone dei Pagamenti 2024

Pagamenti digitali e frodi: nuove sfide e la proposta di PSR

Mario Trinchera

Technical Coordinator

TLP:GREEN

Refunding and IBAN check

TIMING OF CUSTOMER REFUND → **Art. 56** PSR *"Payment service provider's liability for unauthorised payment transactions"*: the possibility for the PSP to undertake an "investigation" before reimbursing the customer is introduced in paragraph 2.

(*"Where the payer's payment service provider had reasonable grounds for suspecting fraud committed by the payer it shall,* ***within 10 business days after noting or being notified of the transaction, either refund the payer the amount of the unauthorised payment transaction if it has concluded, after further investigation, that no fraud has been committed by the payer, or provide a justification for refusing the refund*** *and indicate the bodies to which the payer may refer the matter in accordance with Articles 90 to 94 if the payer does not accept the reasons provided."*).

IBAN CHECK → **Art. 50** PSR *"Discrepancies between the name and unique identifier of a payee in case of credit transfers"*.

In line with the proposed regulation on Instant Payments, a requirement has been included for the payer's PSP to verify the correspondence between IBAN and payee's name.

Transaction Monitoring and Infosharing

INFOSHARING → **Art. 83** PSR "*Transaction monitoring mechanisms and fraud data sharing*".

*(a) the **unique identifier of a payee**;*

*(b) the **name of the payee**;*

*(c) the **personal identification number** or organisation number of the payee, where applicable;*

A payment service provider may exchange data with other payment service providers who are subject to an information sharing arrangement as referred to in paragraph 3 where the payment service provider has reasonable and objective grounds to suspect a fraudulent behaviour by a payment service user.

Consumer Education

CONSUMER EDUCATION → **Whereas (106)** *Payment service providers can play an important role in reinforcing fraud prevention by regularly taking every necessary initiative to increase their payment service users' understanding and awareness about the risks and trends of payment fraud. In particular,* ***PSPs should run proper awareness raising programmes and campaigns on fraud trends*** (…)

The payment service provider shall seek to: educate the payment service user and help (…)

Concept also reiterated when the objective n.1 (*Strengthen user protection and confidence in payments*) of the new regulation is described, such that charged to PSPs there is the "***obligation to educate customers about fraud***".

Spoofing Liability

SPOOFING → **art. 59:** *"Payment service provider's liability for impersonation fraud".*

Where a payment services user who is a consumer was manipulated by a third party pretending to be an employee of the consumer's payment service provider ***using the name or email address or telephone number of that payment service provider*** *unlawfully and that manipulation gave rise to subsequent fraudulent authorised payment transactions, the payment service provider shall refund the consumer the* ***full amount of the fraudulent authorised payment transaction****.*

In our opinion, the issue should be promoted to telecommunications authorities at the European level and in each member state. Only telephone operators can act to reduce the phenomenon, while, apart from informing and raising awareness, **nothing can PSPs do** about something that is completely outside their perimeter and over which **they have no control**.

Article 59 may be not effective in the part "*Mobile network operators shall cooperate closely*" since it is obvious that no one else will do anything where PSPs are always responsible for reimbursing customers.

Distinction between fraud and scam

DISTINCTION BETWEEN FRAUD AND SCAM → ***missing article***

Based on our experience, it would have been very useful to introduce a distinction between fraud and scam, so that it would clearer what is included in the Regulations and what is not.

A summary of the content of our last proposal follows:

Scam: A scam definitely involves the sale of goods and/or services that once purchased are either not delivered/provided or turn out to be significantly different from what the scammer advertised. However, in these cases, payment is voluntarily and consciously completed by the victim (consciously means that the money actually goes to whom the customer wants it to go), without any compromise or technical manipulation.

Fraud: The attacker's goal is not to sell something but to access the victim's money through the direct or indirect use of banking channels. Fraud is characterized by unauthorized transactions or authorized transactions without the perception that the money is directed to someone other than the will of the account holder. In fraud there is always compromise or manipulation or both.

Blocking Funds

BLOCKING FUNDS → ***missing article***

Complete lack of an article clarifying what powers the PSP has when it identifies a fraudster among its clients.

Article 51 (“*Limits and blocking of the use of the payment instrument* ”) appears insufficient for this purpose while it would be proper to give the PSP the power to block those funds that are the result of transactions that are not legitimately authorized, especially when the victims' PSPs provide adequate evidences.

Even better if the PSP at which the fraudster is a customer **could be allowed to return those funds to the victims' PSPs**.

MISP Architecture