Non-paper of the Netherlands delegation
Regarding fraud-related clauses in the PSR
11-12-2023

The EU Serious and Organised Crime Threat Assessment (SOCTA) 2021 has identified online fraud as a main threat for the EU in the upcoming years. Every year, millions of EU citizens become victim of online fraud.[1] Governments and law enforcement cannot effectively act on this threat alone and private actors such as payment service providers, online marketplaces and electronic communication service providers have a responsibility to prevent, deter and detect crimes committed through their platforms and to protect their customers. The Netherlands welcomes the Commission's proposal as it underlines this responsibility on the side of payment service providers and acknowledges that they are in the unique position to respond to fraudulent payment transactions, while having direct contact with their customers.

The fight against fraudulent payment transactions should be addressed in all steps of the fraud chain, both at the front and end of the chain. This means prevention through customer awareness, raising barriers by real-time transaction monitoring and other preventive measures and taking care of victims once fraud has occurred. Reimbursement of unauthorized fraud and of bank impersonation fraud is an important part of this to make sure consumers keep faith in our online payment system and something that the Netherlands already has experience with.

With this in mind, the Netherlands sees room for improvement in the current text of the Regulation. In this non-paper we bring forward proposals where the Regulation can be more effective in achieving the desired goals, namely to reduce fraudulent transactions, reduce the number of victims of fraud and to consequently strengthen confidence in payments. Concomitantly, we propose to clarify the text in some aspects by looking at it through the lens of GDPR obligations when dealing with personal data relating to criminal convictions and offences. Our proposals focus on four elements of the PSR:

1. Transaction monitoring
2. Data sharing
3. Position of the alleged fraudster and proportionality of measures
4. Liability regime and gross negligence

1. Transaction monitoring

Transaction monitoring is central to PSPs ability to detect and stop fraud. It protects consumers against fraudulent transactions and helps to maintain confidence in our financial system.[2] In recital 102 it is explained that transaction monitoring is aimed at detection and prevention and data retention periods are linked to these goals. Moreover, the Regulation stresses that in order for transaction monitoring to be effective, it should be constantly improved and should benefit from as much relevant information as possible to be able to assess risks. Therefore, the Netherlands proposes the following:

1. To clarify the purpose of transaction monitoring and storing of the information that stems from it. When fraud is detected by PSPs, they can take real-time preventive action. For example by freezing suspected fraudulent transactions or contacting and informing the customer. However, the information that stems from monitoring can also be very valuable for other preventive or reconstruction purposes. For example, for accountability of the PSP towards supervisors, reconstruction in criminal investigation by the police and in the assessment of liability towards the customer to refund financial losses. These purposes should be added under article 83 (1C). This also means that in case of a proven fraudulent transaction, PSPs should be able to extend the retention period until after the customer relationship has ended. Otherwise this can be an incentive for fraudsters to swiftly change from PSP.
2. To add other information sources to transaction monitoring. Monitoring criteria should not only be based on information of the PSP (for example previous payment transactions) but could also be based on information - for example on modus operandi - from the customer, police and electronic communication service providers.[3] This information should therefore be added under article 83 (2).

Furthermore, the Netherlands requests:

[1] Consumer fraud affects 1 in 4 Europeans | European Union Agency for Fundamental Rights (europa.eu)
[2] Delegated regulation (EU) 2018/389
[3] For example, a police report that has been filed, new modus operandi, session data from electronic communication service providers.

3. The Presidency to discuss options to clarify of the use of AI in the Regulation. The Netherlands endorses the importance of the use of technology for transaction monitoring as described in recital 103. Where the use of AI in transaction monitoring results in automated processing of data and automated decision-making, guarantees for data subjects are required under the GDPR.[4] An important guarantee, for example, is the right not to be subject to decisions solely based on automated processing.

2. Data-sharing

The Netherlands endorses an important objective of the Commission's proposal, namely detecting fraud and the necessary comparison of data from multiple registrations, as laid down in recital 103. In the current text, sharing of unique identifiers of a payee, manipulation techniques and other circumstances associated with fraudulent credit transfers identified individually by each PSP happens amongst PSPs on a voluntary basis when there is sufficient evidence that stems from transaction monitoring that there was a fraudulent payment transaction. The Netherlands has a number of proposals, as well as questions for clarification. The Netherlands proposes:

1. To include an option to share a limited set of data broader than the unique identifier, in conformity with GDPR, and for the purposes as laid down in 83 1 (c). Recital 103 mentions the importance of sharing of ¨all relevant information amongst PSPs¨ and mentions a few examples of data that can be shared, while article 83 (3) only describes sharing of the unique identifier. From practice in the Netherlands we know that a unique identifier is not enough data to properly detect fraud networks as they operate with multiple unique identifiers. As was highlighted in the Swedish non-paper, more data is needed for this purpose. According to the Netherlands this could include IP addresses of devices, stolen authentication elements and user agents. Sharing this data should be subject to GDPR safeguards and the use of privacy enhanced technology. The Netherlands proposes to request the EBA to establish which technical data/traces of fraud are needed for this purpose and to add this data in article 83 (3).
2. To clarify the link with the GDPR in transaction monitoring and data sharing. Because processing and sharing of data in the context of fraud detection and prevention can concern personal data of a criminal nature the Netherlands proposes to include a reference in Article 80 to Article 10 GDPR/2016, and/or article 11 2018/1275.

The Netherlands requests:

3. The Commission to elaborate on whether sharing of data on a voluntary basis by PSPs provides consumers with a sufficient level of protection against fraud in our payment system. Should this be more obligatory under certain circumstances?
4. The Commission to elaborate on why sharing of information with law enforcement or filing a police report in case of fraudulent transactions is not mentioned in the PSR. The Netherlands finds it important that criminal investigations take place into fraud and that PSPs report to the police when they detect fraud. This point was also brought forward in the Swedish non-paper.
5. The Commission to elaborate if the cooperation that is required from electronic service providers in case of bank impersonation fraud in article 59 also encompasses the sharing of relevant (personal) data, subject to GDPR requirements.

3. The position of the alleged fraudster

Transaction monitoring and sharing of fraud data can have direct consequences for the alleged fraudster, for example when the PSP pauses or blocks a transaction, shares data of the alleged fraudster or withdraws banking services.The Payment Accounts Directive[5] already stipulates the right of any customer to a basic payment account. We recognise the importance of 'de-risking' while at the same time we wish to protect the financial system and the consumers for fraudulent activities.
The Netherlands has one question about the position of the alleged fraudster and one proposal. The Netherlands proposes:

1. To include the requirement of conducting detailed investigation in Article. 83 In line with recital 105, we propose to include in Article 83 the responsibility that a PSP conducts a detailed investigation before taking measures that affect the alleged fraudster. A distinction should be made between measures that are aimed at stopping fraud at an instant, such as blocking a payment transaction and contacting the customer, and more far reaching consequences, such as sharing of data with other PSP's, for which sufficient evidence of a fraudulent payment transaction is needed, and withdrawal of services. For these more far reaching consequences, the term detailed investigation from recital 105 should be included in

[4] Article 22 GDPR
[5] Directive 2014/92/EU

article 83. Moreover, we suggest to include in the recitals that in the detailed investigation personal circumstances such as the possible vulnerability of the alleged fraudster must be taken into account. The alleged fraudster can be a money mule, for example under financial guardianship, and measures taken by the PSP should be carefully weighed.

The Netherlands requests the Commission and the Presidency:

2. To discuss options to clarify the legal position of the alleged fraudster in the PSR proposal. This could entail specifying legal remedies that the alleged fraudster has, access to complaints procedures, and transparency in decision making by the PSP. The Netherlands suggests to add, for example, measures to prevent de-risking and disproportionate measures against the alleged fraudster in Article 80.

3. Liability regime and gross negligence

Bank impersonation fraud undermines consumer trust in their PSP, and ultimately affects the trust that society has in electronic payments. The Netherlands shares the Commission's view that PSPs are well equipped to prevent and combat fraud. Therefore, it is crucial to implement a liability regime that ensures that victims receive compensation and that simultaneously incentivises banks to prevent fraud within their capabilities. Consumers also bear the responsibility to engage in electronic payments safely and consciously because banks do not have the means and capabilities to prevent all forms of fraud, and, as a result, cannot be held accountable for all incurred damages by fraud. The Netherlands already has good experience with liability for banks in case of bank impersonation fraud. In principle, victims will be compensated 100% of their loss. However, a bank may decide not to pay compensation, or to adjust the amount of the compensation, for example when the victim was complicit in the scam or the victim fails to adequately assist the bank in the investigation of the scam. Furthermore, in this system it is important that banks thoroughly assess the unique circumstances surrounding each case of fraud. This framework works effectively, has a generous approach and does not lead to reduced vigilance from consumers. Based on the experience that we have, the Netherlands proposes the following:

1. To let the determination of gross negligence be contingent on the specific attributes of each fraud case and to refrain from formulating a definition or mandatory list of circumstances. Establishing a prescribed list of conditions or a strict definition of gross negligence could result in a minimal rate of reimbursement by PSPs. Moreover, we should avoid confusion by including conditions that are, in fact, only relevant to unauthorized payments, such as ensuring that cards and security credentials are safely kept by consumers. Instead, the Netherlands proposes to include broad examples of circumstances in the recitals that can constitute gross negligence and has text proposals for this.

Text proposals:

Recital 105

… Additional safeguards should be put in place by payment services providers, such as contacting the customer if he or she is the payer of a credit transfer which can be assumed to be fraudulent, and further monitoring of an account, where the unique identifier shared as potentially fraudulent designates a customer of that payment service provider. Payment fraud data shared amongst payment services providers in the context of such arrangements should not constitute grounds for withdrawal of banking services without detailed investigation**, including on the personal situation of the alleged fraudster.**

Recital 82

To assess possible negligence or gross negligence on the part of the payment service user, account should be taken of all circumstances. The evidence and degree of alleged negligence should generally be evaluated according to national law. However, while the concept of negligence implies a breach of a duty of care, 'gross negligence' should mean more than mere negligence, involving conduct exhibiting a significant degree of carelessness **that should be assessed depending on the circumstances of the case**; for example, 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. The fact that a consumer has already received a refund from a payment service provider after having fallen victim of bank employee impersonation fraud and is introducing another refund claim to the same payment service provider after having been again victim of the same type of fraud could, **depending on the circumstances of the case,** 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. **Moreover if the victim was complicit in**

the scam or the victim fails to adequately assist the bank in the investigation of the scam could be considered as gross negligence.

Article 80 Dataprotection
Payment systems and payment service providers shall be allowed to process special categories of personal data as referred to in in Article 9(1) of Regulation (EU) 2016/679 and Article 10(1) of Regulation (EU) 2018/1725) and when it concerns fraud prevention and detection payment systems and payment service providers shall be allowed to process data as referred to in **article 10 GDPR (Regulation (EU) 2016/679) and article 11 (Regulation (EU) 2018/1275)** to the extent necessary for the provision of payment services and for compliance with obligations under this Regulation, in the public interest of the well functioning of the internal market for payment services, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons, **and subject to the rights for the data subject enshrined in the GDPR,** including the following:

The addition to 'subject to appropriate safeguards for the fundamental rights and freedoms of natural persons, including:
c. measures to prevent de-risking and disproportionate measures as a result of transaction monitoring and fraud data exchange.

Article 83 Transaction monitoring mechanisms and fraud datasharing
1. Payment service providers shall have transaction monitoring mechanisms in place that:
(a) support the application of strong customer authentication in accordance with Article 85;
(b) exempt the application of strong customer authentication based on the criteria under Article 85(11), subject to specified and limited conditions based on the level of risk involved, the types and details of the data assessed by the payment service provider;
(c) enable payment service providers to prevent and detect potentially fraudulent payment transactions, including transactions involving payment initiation services.
(d) enable payment service providers to establish accountability towards supervisors, to inform decisions about liability towards the customer and to inform the police for purposes of criminal investigation.

2. Transaction monitoring mechanisms shall be based on the analysis of previous payment transactions and access to payment accounts online. Processing shall be limited to the following data required for the purposes referred to in paragraph 1:
(a) information on the payment service user, including the environmental and behavioural characteristics which are typical of the payment service user in the circumstances of a normal use of the personalised security credentials;
(b) information on the payment account, including the payment transaction history;
(c) transaction information, including the transaction amount and unique identifier of the payee;
(d) session data, including the device internet protocol address-range from which the payment account has been accessed.
(e) customer reports
(f) information from the police
(g) information from electronic communication service providers

Paragraph 3
To the extent necessary to comply with paragraph 1, point (c **and d**), payment service providers may exchange **a minimal set of data** ~~the~~ **, including the** unique identifier of a payee**,** with other payment service providers who are subject to information sharing arrangements as referred to in paragraph 5, when the payment service provider has sufficient evidence to assume that there was a fraudulent payment transaction. Sufficient evidence for **on the basis of which** sharing ~~unique identifiers~~ **a minimal set of data** ~~shall be~~ **can take place** ~~assumed when at least two different payment services users who are customers of the same payment service provider have informed that a unique identifier of a payee was used to make a fraudulent credit transfer~~ **shall be derived from investigation of facts and circumstances of the case.** Payment service providers shall not keep unique identifiers

obtained following the information exchange referred to in this paragraph and paragraph 5 for longer than it is necessary for the purposes laid down in paragraph 1, point (c **and d**).

Paragraph 4
The information sharing arrangements shall define details for participation and shall set out the details on operational elements, including the use of dedicated IT platforms **that are based on privacy enhanced technology. Moreover, it should be specified within which timeframe information shall be shared to timely detect and respond to fraud**. **In the information sharing arrangement it should be included how data subjects are protected against disproportionate measures as a result of data sharing.** Before concluding such arrangements, payment service providers shall conduct jointly a data protection impact assessment as referred to in Article 35 of the Regulation (EU) 2016/679 and, where applicable, carry out prior consultation of the supervisory authority as referred to in Article 36 of that Regulation.

Paragraph 6
- The processing of personal data in accordance with paragraph 4 shall not lead to termination of the contractual relationship with the customer by the payment service provider or affect their future on-boarding by another payment service provider**, in accordance with Payment Accounts Directive, Directive 2014/92/EU.**