[redacted]

Betreff: Amex Written Comments on PSD3-PSR1 BE Presidency Progress Report
Datum: Dienstag, 18. Juni 2024 um 14:52:14 Mitteleuropäische Sommerzeit

[redacted]

[redacted]

Anlagen: image001.png

[redacted]

[redacted]

Spending limits: Ideally, whether spending limits want to be set should be up for the contracting parties (i.e. PSP and PSU) to agree on, without mandating PSPs to provide such feature by default.

Cool off periods and other reactive measures: the cool period (after the increase of the spending limit) and other measures can be applied as a consequence of the detection of possible fraudulent activity and the result of the transaction monitoring. Considering that PSPs will be obliged to enhance the detection of possible fraudulent activity, they should have discretion on the type of measures that can be applied to prevent fraud (e.g. block payment instruments, accounts, cool off periods, request additional SCA or other verifications, and similar), but it shouldn't be imposed by level 1 regulations, since it may be detrimental to both the PSP and the PSU (who, ultimately, might not be able to execute a payment at the time it has requested to increase the limit but has to wait for the cooling off period to elapse).

Transaction monitoring measures by the PSP of the beneficiary: We agree that the PSP of the beneficiary should be obliged to monitor the transaction and the activity and implement possible measure to prevent fraud (e.g. freeze received funds if the transaction is unusual, and similar).

GDPR elements: The processing of data for fraud prevention may imply the processing of sensitive data for the analysis of information and for the possible implementation of measures (biometric data, payment data, scorings, profiles and similar). The processing of such data is regulated under Art. 9 of the GDPR (special categories of data). Hence, the PSR must enable the processing of special categories of data, for fraud prevention purposes in the context of the PSR framework. GDPR must not be an obstacle for fraud prevention. Hence it is necessary to find the appropriate interplay between both regulations.
[External] Data sharing with the authorities: PSPs already have obligations related to the report of fraud information. The duplication and overlap of obligations should be avoided if those contribute to creating an excessive reporting burden to PSPs.

Authorization – Conditions for unauthorized transactions: It is positive that the Art. 49 includes a description of cases that can lead to the lack of authorization (e.g. social engineering applied to the PSU).

Duty to cooperate in fraud investigation: It is important to remember that in social engineering the fraudster exploits the "human factor" of the security process. Hence, it is necessary that the PSR framework also aims to reinforce the duty of care of the PSUs, since this will lead to reduce the number of fraud cases.

For such purpose, it is necessary that the users cooperate, providing the information deemed reasonable by the PSP for the prevention of fraud (e.g. modus, method and consequences of the fraud). Also, PSUs must be required to report to the police the crime (fraud) committed, since this is also a matter linked to law enforcement and crime prevention. The requirement of a police report will also improve the duty of care of the PSUs and mitigate unintended consequences such as the increase of friendly fraud (fraud from the PSU in the report of fraudulent transactions).

We also agree with the consequences related to the lack of cooperation from the PSU. For a PSU to be entitled for a reimbursement, the PSU must cooperate and provide reasonable information to the PSP. If not, the PSU must not be entitled for reimbursement.

ADR: We agree with the implementation of ADR procedures, if the PSP decides that the PSU is not entitled for a reimbursement, and the PSU wants to challenge that decision. However, considering that PSUs would have a right to challenge the decision, and that PSPs already need to report fraud data to the Supervisors, the obligation to report the refusal to reimburse an alleged unauthorized transaction should be removed from the PSR. Such obligation would only generate an unnecessary workload for PSPs and NCAs, in an already complicated task.

Limit liability caps: this provision does not seem feasible. If further context is provided, it would help having a clearer view around it.

IBAN discrepancy alert / Alerts to the PSU regarding the possibility of fraud: Any concrete effort from the PSP to alert the PSU of a possible fraud, should be considered as a relevant element to determine if there was gross negligence from the PSU. This can be included in L3 (please refer to the next comment).

Gross negligence: We agree that L1 can include a list of non-exhaustive elements that can be considered when analyzing whether the PSU committed Gross Negligence. Additionally, the EBA can be mandated to develop Guidelines on the concept of Gross Negligence for the purpose of the PSR (non-binding, hence not directly affecting the civil law framework of MS).

[redacted]

[redacted]

DON'T *live life* WITHOUT IT™