Question ID

2024_7265

Legal act

Directive 2015/2366/EU (PSD2)

Topic

Other topics

Article

66,67

COM Delegated or Implementing Acts/RTS/ITS/GLs/Recommendations

Regulation (EU) 2018/389 - RTS on strong customer authentication and secure communication

Article/Paragraph

32.3

Type of submitter

Credit institution

Subject matter

Proxy matrices

Question

Are credit institutions (ASPSPs) allowed to facilitate proxy matrices implemented by their (corporate) clients that allocate proxy to only certain users to invoke the services of third party payment service providers (TPPs)?

Background on the question

For (international) corporates the management of their bank accounts (initiating payments and viewing account information) poses significantly more risk compared to private individuals and SME businesses. In a corporate client environment, such management entails risks that are exponentially higher due to:

- the high number (millions) of payment transactions and (sensitive)(personal) payment data records;
- the high numbers of users/employees with payment initiation and/or viewing rights;
- corporates using multiple (electronic) channels and payment instruments;

- corporates having many bank accounts in many currencies in multiple countries, often with multiple (Pan-) European ASPSPs; and
- the setup of their account and liquidity management may be subject to overarching cash management facilities and/or payment factories (centralisation of operations).

This results in risk being substantially higher for corporates (e.g. utility or telco companies, government/public agencies, tax authorities, media companies) compared to the context of a private individual or smaller business clients. To manage such risks corporates have comprehensive risk policies to identify, assess, and mitigate potential risks associated with payment processing. These risks include, but are not limited to, fraud, data breaches and business continuity. The factual day-to-day management of accounts is performed by users/employees appointed by the corporate or, in case of centralisation of account management, by group companies. Detailed proxy matrices are implemented by corporates with their ASPSPs to manage risk, particularly fraud and unauthorised access to sensitive company information and personal data included in transaction information. Authority/proxy to users is granted in accordance with the local (civil and corporate) law requirements of the country of incorporation of the corporate/accountholder.

Proxy matrices generally are very detailed, they cater for users to have access to one/more/all accounts and generally include limitations/conditions: joint or several (levels of) authorisation, authorisation up to certain amounts, access through one or more electronic channels/payment instruments, local/regional/global authority and use of certain payment products. A user can have access to one or more electronic channels/payment instruments with different transaction/daily limits applying to each of them. The corporate's governance framework/policy sets the internal rules, however, the relevant controls effectuating such governance framework/policy are (also) implemented through authorisation instruments issued by the corporate's ASPSPs. For ASPSPs it is paramount to abide by the proxy matrices to prevent the risk of unauthorised payment transactions and/or (personal) data leakage.

With the introduction of Open Banking a new 'PSD2 channel' has become available to corporates to manage accounts. Consequently, to manage and control above risks, they may further diversify their proxy matrices and specify if and to what extent a user has authority to manage accounts through third part payment service providers (TPPs). As Open Banking services can be invoked by users through mobile apps, corporates implement further conditions to control which sensitive and personal data may be shared with whom, e.g. by detailing in their proxy matrices which users may have access to (certain) accounts through TPPs without necessarily duplicating the proxy matrix existing for the ASPSP's proprietary channels.

It is a general principle of law that a corporate has sole discretion how to manage its assets (including bank accounts) and to which users/employees it so grants authority and subject to what conditions. Paragraph 46 of the EBA's Opinion on obstacles (EBA/OP/2020/10) acknowledges that only certain users may have authority to operate accounts. So, a user may have authority to manage one or more accounts through one or more channels subject to applicable conditions, e.g. different limits may apply for one user: a limit of 1500,- for a card, a limit of 100.000,- for electronic banking and no limit for host-to-host channel.

Submission date

03/12/2024

Final publishing date

29/08/2025

Final answer

Articles 66(1) and 67(1) of Directive (EU) 2015/2366 (PSD2) require Member States to ensure that payment service users (PSUs) have the right to use payment initiation and account information services provided by third-party providers (TPPs).

Article 66(4)(c) and 67(3)(b) of PSD2 further require Account Servicing Payment Service Providers (ASPSPs) to: "treat payment orders transmitted through the services of a payment initiation service provider without any discrimination other than for objective reasons, in particular in terms of timing, priority or charges vis-à-vis payment orders transmitted directly by the payer" and, respectively, to "treat data requests transmitted through the services of an account information service provider without any discrimination for other than objective reasons".

Article 32(2) of the Commission Delegated Regulation (EU) 2018/389 (the Delegated Regulation) provides that ASPSPs that have put in place a dedicated interface must "ensure that this interface does not create obstacles to the provision of payment initiation and account information services". This Article explicitly mentions, as an example of prohibited obstacles, "requiring additional checks of the consent given by payment service users to providers of payment initiation and account information services".

As regards access to payment accounts held by a legal entity, paragraph 46 of the EBA Opinion on obstacles under Article 32(3) of the Delegated Regulation (EBA/OP/2020/10) clarified that the terms and conditions concluded by ASPSPs with the PSU holding the respective accounts (i.e., the legal entity) may specify which authorised users are permitted to operate the corporate accounts.

The Opinion further clarified that ASPSPs should not impose additional checks when an authorised user accesses the corporate accounts via a TPP, compared to when the same user accesses the accounts directly through the ASPSP's interface. This clarification refers specifically to checks imposed unilaterally by the ASPSP and not to access controls defined by the PSU.

Neither PSD2 nor the Delegated Regulation preclude the legal entity holding the account from instructing the ASPSP to enforce differentiated access rights for its authorised users, in line with the entity's discretion to define user access to its payment accounts, including specifying which users may access the corporate accounts via TPPs. Such differentiated access rights, when applied by the ASPSP in accordance with the PSU's instructions and forming part of the agreed contractual framework, do not constitute in themselves obstacles under Article 32(3) of the Delegated Regulation.

Status

Final Q&A

Answer prepared by

Answer prepared by the EBA.