Single Rulebook Q&A

Question ID	2021_6245
Status	Final Q&A
Legal act	Directive 2015/2366/EU (PSD2)
Topic	Strong customer authentication and common and secure communication (incl. access)
Article	68
Paragraph	5
Subparagraph	-
COM Delegated or Implementing Acts/RTS/ITS/GLs/Recommendations	Not applicable
Article/Paragraph	Not applicable
Date of submission	19/10/2021
Published as Final Q&A	13/04/2022
Disclose name of institution / entity	No
Type of submitter	Other
Subject matter	ASPSP restricting access for TPPs who embeds the redirect
Question	Do Account Servicing Payment Service Providers (ASPSPs) have the right to block access to payment accounts for a Third Party Provider (TPP) who embeds the ASPSP-provided redirection website in order to provide the Payment Service User (PSU) with a TPP-provided user interface?
Background on the question	According to Article 68(5) PSD2, an ASPSP may only deny TPPs access for objectively and duly evidenced reasons related to unauthorised or fraudulent access, including fraudulent initiation of payment transactions. It has however happened that ASPSPs have contacted TPPs to say that they will restrict access to the PSD2 Application Programming Interface (API) because the TPP embeds the redirection domain provided by the ASPSP for PSUs to enter their credentials when using the services of a TPP. The stated reason is that the PSU in this instance does not enter its credentials into the ASPSP-hosted redirection domain but into an interface provided by the TPP. If the ASPSP offers a redirection-only API, the TPP can improve the user journey by embedding the redirection domain and provide the user with a TPP-provided user interface (instead of requiring the user to enter the credentials into the redirection domain). This allows the TPP to e.g. provide a user

	interface in different languages, different font sizes and/or adapted to different devices/technology environments. As an example, a web-based redirection domain would not work in environments that are not web-browser based, such as e.g. gas stations, smart watches, Point of Sale terminals, internet of things, AI and voice assistants, etc. whereas the TPP would be able to provide user interfaces adapted for such environments by means of embedding the redirection domain. Articles 45 and 46 PSD2 specify which information the TPP needs to provide to the PSU when providing such user interfaces and the transmission of security credentials needs to be done in a secure manner with encryption applied using RTS compliant techniques. To be clear, embedding the redirection domain is not "screen scraping" as the TPP identifies itself vis-a-vis the ASPSP (and leverages the PSD2 API); it only means the TPP can adapt and improve the user interface and as such convenience for the PSU. The ASPSP does not need to do anything to enable embedded redirection; the work is solely at the side of the TPP. Alternatively, the ASPSP can of course as a part of its PSD2 API actively enable an embedded flow, which would mean the TPP would not have to embed the redirection domain itself. But the ASPSP must not block or otherwise make it difficult for the TPP if the TPP elects to build its own PSU-facing interface and transmit the credentials to the redirection domain of the ASPSP as TPPs may transmit credentials pursuant to Article 66(3)(b) PSD2.
Final answer	Article 68(5) PSD2 provides that an account servicing payment service provider (ASPSP) may deny an account information service provider (AISP) or a payment initiation service provider (PISP) access to a payment account for objectively justified and duly evidenced reasons relating to unauthorised or fraudulent access to the payment account. Q&A 6044 clarified that: • In accordance with Article 30(3) of the Commission Delegated Regulation (EU) 2018/389, PISPs and AISPs should follow the technical specifications set out by the ASPSP when accessing the ASPSP's interface. • Where the ASPSP has opted for a redirection or a decoupled approach and does not allow in its documentation the possibility for the PISP/AISP to transmit the payment service user (PSU)'s credentials to the ASPSP, the PISP/AISP should redirect the PSU to the ASPSP's domain to authenticate and should not introduce an approach for sending the PSU's personalised security credentials to the ASPSP that is different to the approach envisaged by the ASPSP in the technical specifications of the interface. Such latter approach would not be in line with the requirements of Article 30(3) of the Delegated Regulation.

	It follows from the above that the approach described by the submitter, where the PISP/AISP “embeds” the ASPSP’s redirection domain, would not be in line with Article 30(3) of the Delegated Regulation. In addition, such an approach may lead to a situation where the ASPSP identifies, based on its transaction monitoring mechanisms under Article 2 of the Delegated Regulation, that it is not the PSU who is trying to access the account and subsequently denies access to the payment account. In such case, the denial of access to the account would be in line with Article 68(5) PSD2.
Link	https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2021_6245

European Banking Authority, 03/07/2022
www.eba.europa.eu