KPMG

Financial Risk&Regulation

The new MNB recommendation regarding payment services and open banking

Newsletter – August 2021

The MNB is committed to promoting the spread of open banking in Hungary, therefore in 2020 it addressed an executive circular to the relevant market participants on certain issues in the context of secure communication related to payment order and account information services. Subsequently, in 2021, it launched an inspection to technically assess the open API solutions of the 10 largest Hungarian banks, and issued a recommendation on the prevention of open banking in July in order to facilitate the uniform application of the legislation. Our August newsletter presents a number of topics from this recommendation, which are particularly important for consumer protection, in order to illustrate what practices the MNB considers to be an obstruction and a market solution to follow.

Following the entry into force of the PSD2, since 14 September 2019 account servicing payment service provider (hereinafter: account managers or banks) must provide access to their application programming interfaces to account information and payment order payment service providers, in other words, third-party service providers. Nevertheless, in both the domestic and EU markets, "the great innovation of PSD2, open banking, has so far been limited in its spread, as international regulation is not specific enough about the access interfaces to be implemented, and banks can obstruct new participants in many ways." – writes the Payment System Report published by the MNB recently. "Obstruction" is not necessarily intentional from banks, as it may also stem from misinterpretation of regulations or the aim of minimum compliance. However, in the light of the recommendation, it is worthwhile for banks to review their existing access interfaces, because in the future, designs or solutions that qualify as obstructive may result in supervisory fines.

Open banking allows emerging fintech firms to come up with new services satisfying customer needs by controlled access to robust banking data. Furthermore, the changed environment caused by the coronavirus has created a receptive environment for forward-looking online services. Banks can also take advantage in this progress, if they see fintechs as partners rather than rivals, and the benefits of working with smaller, agile organizations are recognized. While it can open up new opportunities for banks, open banking can also be accompanied by countless uncertainties. How should a customer complaint about a third-party transaction be handled? How can the openness of the systems be ensured without compromising IT security? Our PSD2 services can help with these and similar issues.

KPMG

What is an API?

Application Programming Interface and its documentation gives a program access to the instruction set of another system - in our case internet bank - without the programmer having to know its internal operation. In our everyday life, we most often come across APIs when we install a new application on our phone and it asks for permissions e.g. to use the device camera. In this case, the newly installed app communicates with the camera's management software via the camera's API.

Obstruction of the payment services of third party service providers

Referring to the SCAr[1]. article 31, the MNB reminds payment service providers that they can provide API access in two ways. They either allow the use of their interfaces that are used to authenticate their payment service users or create a dedicated interface for this purpose. Banks that have opted for the latter solution are obliged to ensure that this interface does not obstruct the use of third-party services.

Multiple strong customer authentication

The payment service provider is required to use strong customer authentication when the payer performs a remote/online transaction (even through a fraudulent channel). The account servicing payment service provider is therefore also obliged to provide the third party service provider with the authentication procedures that it applies to its own customers. Therefore, during the usage the payment services of third-party payment service providers, the account servicing payment service provider performs strong customer authentication. The MNB expects the authentication

– do not consist of more steps than necessary,

– do not request unnecessary information or data, and

– do not cause any other undue inconvenience

for a customer using the payment services of a third party service provider compared to when accessing their payment account directly (hereinafter referred to as multiple strong customer authentication)

According to the recommendation, the following cases qualify as multiple strong customer authentications:

a. the strong customer authentication performed by the account manager during the use of the account information service consists of several steps or causes other inconvenience to the user than compared to when directly requesting their account information,

b. the account manager does not use a single strong customer authentication when using the payment order service, even though the third party service provider has provided all the necessary payment data,

c. the account manager requires multiple strong customer authentications for payment transactions initiated through a payment service provider providing the payment order service, with the justification that the solution it provides uses two separate strong customer authentications.

It does not constitute as obstruction if, for an appropriate reason, the account manager requests multiple strong customer authentication (e.g. suspected fraud), but at the same time they must provide proper support to their suspicion. It does not exhaust the concept of obstruction either, if the account manager requests the user to be authenticated multiple times by referring to incomplete information. In such a case, the retrieval of the incomplete information and then the execution of the payment order are subject to authentication. It also does not constitute as obstruction if the use of the account information service and the payment order service together requires two separate strong customer authentications to access the account data and then to initiate the payment transaction.

Re-authentication within 90 days

The payment service provider may, in its sole discretion, waive the use of strong customer authentication if it complies with the conditions set out in SCAr. Articles 2 and 10 (2) paragraphs, and without the client disclosing sensitive payment data:

a. to the balance of one or more designated payment accounts;

b. to payment transactions made through one or more designated payment accounts in the last 90 days.

The MNB considers it a good practice if the payment service provider uses the exception, but does not consider it as obstruction if it does not use this option. However, if the payment service provider makes the above information available to its own customers without authentication, it must apply it to all third-party service providers without discrimination. The account manager may only deviate from this procedure if there is a reasonable suspicion of fraud.

1 Commission Regulation (EU) 2018/389 (27 November 2017) supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open communication standards

Forcing the customer to disclose their payment account

The MNB considers it good practice for account servicing payment service providers who created a dedicated interface if, in the case of the onboarding process of the third party service, only personal credentials (e.g. internet banking identification number) need to be entered manually for customer identification. Furthermore, the MNB expects that third party customers are not required to manually entering the identification number of their payment account, because it constitutes as obstruction in the interpretation of the Supervisor. On the part of the account manager, the MNB considers it a good practice to allow service providers providing account information services to retrieve a list of all the customer's payment accounts via the interface, given the customer's consent. In the case of the payment order service, the customer should be able to use a drop-down list to select the payment account to be debited.

Requirement of additional customer approval

The provision of a payment order and account information service is subject to the explicit consent of the customer, which they give directly to the third party. Requiring additional customer consent from the account manager is considered as obstruction.

Although the account-holding bank has no insight into the consent given to the third party, it cannot make this a condition for using the interface.

The MNB considers it a good practice to provide the user with the ability to block the access of third-party service providers of their choice to their account data on the Internet or mobile banking interface of the account manager. At the same time, it calls on the account manager to avoid the kind of solution where third party services are prohibited by default and must be pre-authorized by the customer before using a third party service.

Other procedures counting as obstruction

The recommendation states that the use of an account information and payment initiation service should not be conditional on the existence of a contractual relationship between the third party service provider and the account manager. Nor may banks charge a fee for the use of a dedicated interface unless the parties wish to enter into an agreement for services other than the usage of the interface.

Banks should ensure that the customer is able to use the same strong authentication procedures (e.g. biometric identification) when using a third-party service provider as when the customer has direct access to his payment account.

Technically, this requires that banks' interfaces allow third-party service providers to rely on the strong customer authentication they perform. During authentication, the MNB expects account servicing payment service provider not to use unnecessary steps and obscure or discouraging language (e.g. during telephone authentication), and may not charge a higher fee for an SMS sent to a customer.

The application of the recommendation is expected from the relevant financial institutions from 1 August 2021 and at the same time the executive circular issued in 2020 expires.

*****

In accordance with the international regulatory environment and domestic practices, the MNB is continuously expanding and clarifying its expectations, which significantly affects the participants of the financial markets and their compliance with legal requirements. KPMG experts are available to interpret and implement supervisory expectations and provide relevant professional advice to develop appropriate practices.

The newsletter was prepared by Kitti Szvetlik and Wieder Gergő.

Contacts:

Ágnes Rakó
Partner
M: +36 70 370 1792
E: agnes.rako@kpmg.hu

Péter Szalai
Director
M: +36 70 370 1739
E: peter.szalai@kpmg.hu

Gergő Wieder
Senior Manager
M: +36 70 333 1471
E: gergo.wieder@kpmg.hu

József Soltész
Manager
M: +36 70 370 1766
E: jozsef.soltesz@kpmg.hu

KPMG.hu