KNF | KOMISJA NADZORU FINANSOWEGO

BOARD OF THE POLISH FINANCIAL SUPERVISION AUTHORITY

19 August 2019

Communication on strong customer authentication in the case of certain means of payment using payment instruments

As of 14 September 2019, there arises an obligation to apply Article 32i of the Act of 19 August 2011 on payment services and Commission Delegated Regulation (EU) 2018/389 of 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 standards of communication (Regulation). Under Article 32i of the Act on payment services, payment service providers must use strong customer authentication where a customer (payer):

- accesses its payment account online,
- initiates an electronic payment transaction,
- carries out any action through a remote channel which may imply a risk of payment fraud or other abuse.

In particular, strong customer authentication should be used where a customer logs on to online banking, to initiate payments using a payment card or any other payment instrument, and for online payments.

According to Article 2 point 26aa) of the Act on payment services, strong authentication ensures protection of confidentiality of data through the application of at least two elements categorised as:

- knowledge of something only the user knows (e.g. PIN code, reusable password),
- possessing something only the user possesses (e.g. a payment card, a smartphone application),
- inherence (e.g. client's biometric features)

– that are an integral part of such authentication and independent in that the breach of one of such elements does not compromise the reliability of the others. According to the European Banking Authority (EBA), at least two of the elements of strong authentication should fall under different categories. The detailed rules for using strong customer authentication (SCA) and the exceptions from the requirement to use it have been laid down in the Regulation.

The data on the European market of payment services collected by the EBA show that the participants of that market are not sufficiently prepared for the implementation of the SCA rules for payments made through online channels, especially in the e-commerce area. That applies not only to payment service providers but also to unsupervised stakeholders in the payment services market, especially payees (sellers, merchants). Such conclusions are also confirmed by the data collected and analyses carried out by the Polish Financial Supervision Authority (UKNF) with regard to the Polish market.

Considering the complexity of solutions used in payment services markets in the European Union and the necessary changes required to implement the SCA solutions fully and without disrupting the markets, in its opinion of 21 June 2019, EBA concluded that on an exceptional basis and in order to avoid unintended negative consequences for payment service users after 14 September 2019, supervisory authorities in Member States may provide limited additional time to allow migration of the current authentication approaches to the solutions that are fully compliant with the SCA requirements. Such supervisory flexibility requires, however, that each payment service provider submit an appropriate 'migration plan', agree the plan with their supervisory authority and cooperate closely with the supervisory authority to execute the plan.

In view of the arrangements made in respect of the preparedness of participants of the Polish payment services market to fully implement the SCA solutions, and considering the need to ensure that the implementation will not disrupt the functioning of that market or cause any inconvenience for payment service users, the KNF Board considers the application of the solution proposed by the EBA in relation to online payments based on payment cards and to contactless payments executed at payment terminals to be acceptable. This means that no other supervisory measure relating to the failure to use strong customer authentication will be applied towards the payment service providers who will notify the KNF Board, before 14 September 2019, of the need to apply the solution in question and then submit an appropriate realistic 'migration plan', as agreed with the KNF Board, during the period of proper execution of the plan. At the same time it should be emphasised that even in that case, the risk associated with the failure to use, after 13 September 2019, strong customer authentication that is compliant with the Regulation, is fully borne by payment service providers, who are required to use it.

The framework conditions, including maximum time limits for the implementation of the SCA solutions within the 'migration plan', will be indicated after the conclusion of the arrangements at EBA, which will take place most likely after 14 September 2019.