Recommendations of the President of UOKiK for payment service suppliers

* **The working group appointed by the President of UOKiK has been working on solutions aimed at mitigating the risk of fraudulent transactions.**
* **The group was composed of representatives of the Office of the Polish Financial Supervision Authority and banking experts, among others.**
* **As a result, a set of recommendations for payment service suppliers has been developed.**

**[Warsaw, 23 October 2024]** Electronic payments is one the fastest-growing segment in the financial services market. Technological development has changed the financial habits of consumers. The issues which entailed a visit to a bank outlet and a discussion with an advisor a few years ago may now be sorted out online. Saving time, convenience and easiness in using online financial services are accompanied, though, by a range of risks related to the security of transactions and funds deposited on bank accounts.

- The role of payment service suppliers is not coming to an end as the capacities of quick and convenient payments have been provided. Each new solution requires educated customers, not only for its functionality. It is also important to inform customers reliably of the risks and teach them how to avoid such risks. A key issue, however, is the work of payment service suppliers on minimizing the risk at the systemic level - says Tomasz Chróstny, the President of UOKiK.

**Security as a market standard**

For a while, a number of payment service providers have been implementing various types of solutions aimed at mitigating the risk of fraudulent transactions, treating it as an element of competitive advantage. This is a positive tendency, but it will not solve the increasing phenomenon of using online payment mechanisms to rob consumers.

- We appreciate the efforts of payment service suppliers aimed at increasing online transaction security which have been expended in the course of our proceedings. At the same time, we would like to draw the attention to the fact that consumer protection on this market requires that some coherent systemic and organisational solutions be developed which will allow us to reforge the best practices into the market standard - says Tomasz Chróstny, the President of UOKiK.

Ensuring security for consumers using online payments requires engagement of as many participants to the financial market as possible. This was the belief of the President of UOKiK when he appointed the working group focused on developing the solutions for mitigating risk of using payment services for robbing customers. The group was composed of representatives of the Office of the Polish Financial Supervision Authority and banking experts. The deliverable of its works is the document titled: [“Actions Aimed at Mitigating the Risk of Fraudulent Transactions. Recommendations of the President of UOKiK for Payment Service Suppliers”](https://uokik.gov.pl/Download/937).

- We are aware that providing customers with modern and convenient solutions is the basis for competitiveness of financial market entities. The competition among payment service suppliers, though, should not be limited exclusively to offering solutions enhancing customers’ convenience. First and foremost, it must take account of the security of transactions and funds deposited by consumers - say the President of UOKiK.

**The best answers to key problems**

The document developed by UOKiK includes a list of risk factors or functions offered by payment service suppliers which are used by fraudsters most frequently. The said list was developed on the basis of an analysis of complaints delivered by consumers to UOKiK and was additionally supplemented with the risks specified by sector representatives in the course of the work of the working group. A vital aspect of the work was to develop a coherent standard for transaction security while staying flexible in reacting to threats on the part of the suppliers at the same time.

The main part of the document is formed by a set of 16 recommendations aimed at mitigating the risk of performing some fraudulent online transactions. These include, among other things, the recommendations on monitoring atypical transactions, applying transaction limits, using authorisation channels or a capacity to promptly report an unauthorised or fraudulent payment transaction by a customer.

**New responses to new risks**

The dynamics of e-commerce and IT development and the ensuing services related to processing online transactions make that the guidelines contained in the document developed by UOKIK may not be treated as an exhaustive list. In order to perform their role, not only should the recommendations be duly applied but they should also be developed by all the market participants in line with the evolving consumer habits, solutions and threats.

- Restricting the scale of fraudulent transactions is in the interest of both the consumers as well as any and all commercial market participants. I expect that not only will the financial sector fail to delay in observing the recommendations, but it will also be actively involved in creating the best practices and development of solutions increasing the security of online payment transactions - says the President of UOKiK.

**Consumer Support:**

Consumer helpline: 801 440 220 or 222 66 76 76   
contact form: [poradydlakonsumentow.pl](https://poradydlakonsumentow.pl/)  
[Consumer Ombudsmen](https://uokik.gov.pl/pomoc.php) – in your town or district

[Trade Inspection Authority](https://uokik.gov.pl/kontakt-inspekcja-handlowa) – in your province