



Minister Finansów

Warszawa, 13 czerwca 2025 roku

Sprawa: Petycja Fundacji Dobre Państwo ws. oszustw z użyciem kodu BLIK
Znak sprawy: FN7.056.1.2025
Kontakt: Kancelaria MF
tel.: +48 22 694 55 55
e-mail: kancelaria@mf.gov.pl

Fundacja Dobre Państwo

reprezentowana przez:
Witolda Solskiego
Katarzynę Kosakowską
Kancelaria Doradcza
Solski i Partnerzy sp. z o.o.
ul. Żbikowa 14
61-065 Poznań

Szanowni Państwo,

w odpowiedzi na Państwa petycję, wnoszącą o podjęcie systemowych działań mających na celu uniemożliwienie okradania klientów w Polsce tzw. metodą BLIK, niniejszym proszę o przyjęcie poniższych wyjaśnień.

Na wstępie należy wskazać, że opisana przez Państwa sprawa dotyczy bezpieczeństwa transakcji płatniczych, którego zapewnienie przez dostawców usług płatniczych jest uregulowane w polskim prawie na gruncie ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz.U. 2024 poz. 30; dalej UUP).

Polskie przepisy dotyczące bezpieczeństwa transakcji płatniczych i obowiązków jakie w tym zakresie spoczywają na bankach i innych dostawcach uczestniczących w przeprowadzaniu transakcji płatniczych, wynikają z przepisów unijnych (przede wszystkim z tak zwanej Dyrektywy PSD2). Zmiana polskich przepisów w tym zakresie, musi wynikać ze zmiany prawa unijnego, ponieważ są to obszary prawa UE, o wysokim stopniu harmonizacji i we wszystkich państwach członkowskich z uwagi na interes konsumentów muszą być jednolite.

W związku z powyższym Ministerstwo Finansów w aktualnym stanie prawnym nie widzi możliwości zmiany obowiązujących w tym zakresie przepisów jedynie na poziomie krajowym. Jednak, należy wskazać, że obecnie, na poziomie Rady UE trwa rewizja wskazanej wyżej Dyrektywy PSD2, tj. negocjowane są przepisy Dyrektywy Parlamentu Europejskiego i Rady w sprawie usług płatniczych i usług związanych z pieniądzem elektronicznym w ramach rynku wewnętrznego, zmieniająca dyrektywę 98/26/WE i uchylająca dyrektywy (UE) 2015/2366 i 2009/110/WE – dyrektywy

PSD3 oraz Rozporządzenia Parlamentu Europejskiego i Rady w sprawie usług płatniczych w ramach rynku wewnętrznego i zmieniające rozporządzenie (UE) nr 1093/2010 – rozporządzenia **PSR**.

Zaproponowane w powyższych projektach aktów prawnych zasady dotyczące bezpieczeństwa transakcji płatniczych w tym przede wszystkim zwalczanie i zapobieganie oszukańczej transakcjom płatniczym stanowi jeden z najistotniejszych obszarów ww. regulacji i zostanie on istotnie rozwinięty w porównaniu z dyrektywą PSD2. Projektowana unijna regulacja ma zdecydowanie wydźwięk prokonsumencki, nakładając na dostawców usług płatniczych dodatkowe obowiązki i odpowiedzialność za transakcje oszukańcze, jak również po raz pierwszy proponuje się pewne rozwiązania skutkujące większym zaangażowaniem tzw. platform internetowych w zapobieganiu utracie środków pieniężnych konsumentów.

Jedną z najistotniejszych kwestii proponowanych w rozporządzeniu PSR, jest propozycja wprowadzenia art. 59, zgodnie z którym jeśli dochodzi do manipulacji stosowanej przez osobę trzecią na konsumentcie, która doprowadziła do nielegalnych transakcji płatniczych, to dostawca usług płatniczych będzie zobowiązany zwrócić konsumentowi pełną kwotę tejże nielegalnej transakcji, pod warunkiem niezwłocznego zgłoszenia przez konsumenta policji informacji o zaistniałym przestępstwie oraz powiadomienia przez niego dostawcę usług płatniczych. Jednocześnie jak wspomniano wyżej w ramach ww. prac nad PSD3 i PSR prowadzona jest dyskusja odnośnie wprowadzenia pewnych obowiązków po stronie dostawców usług łączności elektronicznych (którzy dostarczają m.in. danych podczas procesu uwierzytelnienia – na przykład przez SMS, czy też odpowiadają za realizowanie połączeń telefonicznych podczas rozmów z pracownikami banków), tak, aby zarówno banki, jak i dostawcy usług łączności elektronicznych byli zobligowani do wdrażanie odpowiednich środków zwiększających bezpieczeństwo transakcji płatniczych oraz współpracowali między sobą w tym zakresie.

Poza powyższą kwestią proponowane rozporządzenie PSR przewiduje również, w mechanizmy monitorowania transakcji przez dostawców usług płatniczych, obejmujące, min. cechy środowiskowe i behawioralne użytkownika, historię transakcji płatniczych, dane dotyczące sesji logowania się użytkownika. Aby ułatwić dostawcom ww. monitorowanie, zaproponowano dodanie art. 83a, dotyczącego dzielenia się danymi w zakresie oszustw, w ramach którego dostawcy będą mogli wymieniać się informacjami m.in. o danych transakcji, sesjach logowania czy danych urządzenia związanych z potencjalnie oszukańczą transakcją. Tekst ten zakłada również, że dostawca odbiorcy płatności, będzie mógł, na podstawie danych z monitoringu transakcji, czasowo blokować środki podejrzaną transakcji, tak aby móc zweryfikować czy transakcja nie jest oszukańcza. Środki byłyby więc udostępniane odbiorcy płatności dopiero po uprzedniej weryfikacji takiej transakcji.

Polska jako państwo sprawujące od początku tego roku do końca czerwca Prezydencję w Radzie UE proceduje wszelkie propozycje zapewniające jak największą skuteczność regulacji odnoszących się do kwestii bezpieczeństwa transakcji płatniczych, tak, aby zapewnić jak największą ochronę konsumentów, przy jednoczesnym zapewnieniu odpowiednich warunków rozwoju dla branży usług płatniczych.

W odniesieniu do przedstawionych w petycji postulatów dotyczących wniosku o wzmocnienie regulacji nadzorczych, w tym wydania wytycznych lub rekomendacji dla banków, zobowiązujących je do aktywniejszej ochrony klientów przez oszustami oraz zmiany procedur reklamacyjnych (str. 8 akapit 2 i 3 ww. petycji), niniejszym załączam przekazaną do Ministerstwa Finansów odpowiedź Narodowego Banku Polskiego.

Z wyrazami szacunku

Z upoważnienia Ministra Finansów

Jurand Drop
podsekretarz stanu

Załącznik: NBP do MF – odpowiedź na petycję