Minister
Finansów i Gospodarki

Warszawa, 8 października 2025 roku

Sprawa: Petycja zawierający żądanie wprowadzenia pilnych działań legislacyjnych oraz nadzorczych, dotyczących transakcji BLIK, w związku z narastającą falą oszustw phishingowych.
Znak sprawy: FN7.056.3.2025
Kontakt: Kancelaria MF
tel.: +48 22 694 55 55
e-mail: kancelaria@mf.gov.pl

[redacted]
E-mail: [redacted]@o2.pl

Szanowna Pani,

w odpowiedzi na Pani petycję, wnoszącą o wprowadzenia pilnych działań legislacyjnych oraz nadzorczych, dotyczących transakcji BLIK, w związku z narastającą falą oszustw phishingowych, niniejszym proszę o przyjęcie poniższych wyjaśnień.

Na wstępie należy wskazać, że opisana przez Panią 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 podmiotach 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

tel.: +48 22 694 55 55
fax: +48 22 694 36 84
gov.pl/finanse
e-mail: kancelaria@mf.gov.pl

ul. Świętokrzyska 12
00-916 Warszawa

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 oszukańczym 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.

Jednocześnie, odnośnie do postulatu dotyczącego wyświetlania nazwy odbiorcy przy transakcjach BLIK, należy wskazać, że od 8 kwietnia 2024 r. obowiązują w całej Unii Europejskiej przepisy Rozporządzenia Parlamentu Europejskiego i Rady w sprawie zmiany rozporządzeń (UE) nr 260/2012 i (UE) 2021/1230 oraz dyrektyw 98/26/WE i (UE) 2015/2366 w odniesieniu do poleceń przelewu natychmiastowego w euro (dalej: IPR). Rozporządzenie to wprowadza na dostawców usług płatniczych i agentów rozliczeniowych szereg obowiązków dotyczących wymogów technicznych, które zwiększą m.in. bezpieczeństwo transakcji płatniczych.

IPR wprowadza m.in. obowiązek świadczenia usługi weryfikacji dopasowania, polegającej na sprawdzaniu, czy numer IBAN i nazwa odbiorcy podane przez płatnika są zgodne z danymi przekazanymi przez dostawcę odbiorcy. Podobne przepisy znalazły się we wspominanym już Rozporządzeniu PSR, i będą one dotyczyły wszystkich transakcji, nie tylko takich, których walutą jest euro.

Odnośnie do postulatu wprowadzenia limitów transakcji BLIK do nieznanych odbiorców bez dodatkowej autoryzacji czy 15-sekundowej pauzy przy akceptacji kodów BLIK dla niezweryfikowanych odbiorców, należy ponownie odwołać się do wspomnianego wyżej IPR, który zobowiązuje dostawców usług płatniczych oferujących polecenia przelewu natychmiastowego do sprawdzania co najmniej raz dziennie, czy którykolwiek z ich użytkowników jest osobą lub podmiotem umieszczonym w wykazie podmiotów, do których stosuje się ukierunkowane finansowe środki ograniczające. Jednocześnie należy wskazać, że szybkość transakcji BLIK czy innych transakcji natychmiastowych, stanowi o ich konkurencyjności. IPR wprowadza jednolitą w całej UE, definicję transakcji natychmiastowej. Zgodnie z tą definicją, transakcja natychmiastowa to polecenie przelewu wykonywane natychmiast. Natychmiast, czyli rachunek płatniczy odbiorcy jest uznawany przekazywaną kwotą w ciągu 10 sekund od momentu odebrania zlecenia płatniczego. Równocześnie, należy mieć na uwadze, że na rynku istnieją inne, bezpieczniejsze, ale też wolniejsze rozwiązania, jak przelewy tradycyjne, które to dają klientowi dłuższy czas na weryfikację danych transakcji i to konsument zawsze będzie miał prawo wyboru, z których metod płatności korzysta.

Odnośnie do postulatu dotyczącego utworzenia tzw. „Safe Zones" BLIK dla zaufanych instytucji takich jak np. Allegro, OLX czy InPost, należy wskazać, że

wprowadzenie takiego rozwiązania w powszechnie obowiązujących przepisach stanowiłoby nieuzasadnioną ingerencję w zasady wolnej konkurencji i wolnego rynku. Stwarzałoby bowiem uprzywilejowaną pozycję rynkową wybranym, prywatnym przedsiębiorstwom.

Jeśli chodzi o rozwiązania komercyjne, funkcjonujące już w tym momencie, to należy wskazać, że są już w Polsce dostawcy, oferujący płatność BLIK, którzy umożliwiają dodanie konkretnej witryny internetowej na listę witryn zaufanych. Płatność BLIK w takich przypadkach możliwa jest bez kodu.

Odnośnie do mechanizmów natychmiastowego blokowania transakcji zgłoszonych jako oszustwo, należy wskazać, na wspomniane już wyżej rozporządzenie PSR. Przewiduje ono 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 podejrzanej transakcji, tak aby móc zweryfikować czy transakcja nie jest oszukańca. Środki byłyby więc udostępniane odbiorcy płatności dopiero po uprzedniej weryfikacji takiej transakcji.

Odnośnie do dodatkowej weryfikacji tożsamości przy wypłatach BLIK w bankomatach powyżej ustalonego limitu, należy wskazać, że na rynku istnieją wolniejsze, ale dające więcej możliwości weryfikacji, metody wypłat z bankomatów. Funkcjonalności bankowości mobilnej większości polskich dostawców prowadzących rachunki płatnicze, umożliwiają klientowi samodzielne ustalenie limitu takich wypłat.

Z wyrazami szacunku

Bartosz Drej
Zastępca dyrektora
Departamentu Rozwoju Rynku Finansowego
w Ministerstwie Finansów