Minister
Finansów

Warszawa, 17 stycznia 2025 roku

Sprawa: Prośba o zapoznanie się i zajęcie stanowiska w sprawie tekstu oświadczenia złożonego przez senator P. Ewę Kaliszuk podczas 25. posiedzenia Senatu RP, 19.12.2024 r.
Znak sprawy: FN7.701.1.2025
Kontakt: Kancelaria MF
tel.: +48 22 694 55 55
e-mail: kancelaria@mf.gov.pl

Pani Małgorzata Kidawa-Błońska
Marszałek Senatu
Rzeczypospolitej Polskiej

Szanowna Pani Marszałek,

w odpowiedzi na Oświadczenie Pani Senatorki Ewy Kaliszuk złożone podczas 25. posiedzenia Senatu RP w dniu 19 grudnia 2024 r., dotyczące prośby o podjęcie przez Ministra Finansów działań w zakresie zmian legislacyjnych dotyczących wprowadzenia nowych czy też dodatkowych stopni weryfikacji transakcji płatniczej, proszę o przyjęcie poniższych wyjaśnień.

Na wstępie należy wskazać, że opisana przez Panią Senator sprawa dotycząca bezpieczeństwa transakcji płatniczych, jest uregulowana w polskim prawie na gruncie ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz.U. 2024 poz. 30; dalej UUP).

Na gruncie UUP, banki mają obowiązek stosować uwierzytelnienie (a więc procedurę umożliwiającą bankowi weryfikację tożsamości użytkownika lub ważności stosowania konkretnego instrumentu płatniczego, łącznie ze stosowaniem indywidualnych danych uwierzytelniających – art. 2 pkt 33b UUP), w ściśle określonych przypadkach.

Mianowicie, zgodnie z art. 32i UUP, dostawca ma obowiązek stosować silne uwierzytelnienie użytkownika, w przypadku gdy użytkownik: uzyskuje dostęp do swojego rachunku w trybie on-line, inicjuje elektroniczną transakcje płatniczą, czy też przeprowadza za pomocą kanału zdalnego czynność, która może wiązać się z ryzykiem oszustwa związanego z wykonywanymi usługami płatniczymi lub innych nadużyć. Ponadto, zgodnie z ust. 2 ww. art. 32i UUP, w przypadku gdy płatnik inicjuje transakcję płatniczą z użyciem sieci Internet, lub stosuje środki które mogą być wykorzystywane do porozumienia się na odległość, silne uwierzytelnienie takiej

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

transakcji obejmuje elementy, które dynamicznie łączą transakcję płatniczą z określoną kwotą transakcji oraz określonym odbiorcą. Samo silne uwierzytelnienie (art. 2 pkt 26aa UUP) zakłada zastosowanie co najmniej dwóch elementów należących do kategorii: wiedza o czymś, o czym wie wyłącznie użytkownik; posiadanie czegoś, co posiada wyłącznie użytkownik; cechy charakterystyczne użytkownika. Przy czym elementy te mają być na tyle niezależne, że naruszenie jednego z nich nie osłabia wiarygodności pozostałych.

Konsekwencje niestosowania silnego uwierzytelnienia klienta są dla banków dotkliwe, ponieważ to one ponoszą winę za nieautoryzowaną transakcję płatniczą. Mianowicie, zgodnie z art. 46 ust. 4a UUP, w przypadku gdy dostawca płatnika nie wymaga silnego uwierzytelniania użytkownika, płatnik nie ponosi odpowiedzialności za nieautoryzowane transakcje płatnicze, chyba że działał umyślnie.

W przypadku nieautoryzowanej transakcji płatniczej, gdy doszło do wadliwego uwierzytelnienia klienta (lub nie doszło do niego wcale), bank ma obowiązek niezwłocznego zwrotu środków na rzecz klienta. Mianowicie, zgodnie z art. art. 46 UUP, w przypadku wystąpienia nieautoryzowanej transakcji płatniczej dostawca płatnika niezwłocznie, nie później jednak niż do końca dnia roboczego następującego po dniu stwierdzenia wystąpienia nieautoryzowanej transakcji, którą został obciążony rachunek płatnika, lub po dniu otrzymania stosownego zgłoszenia, zwraca płatnikowi kwotę nieautoryzowanej transakcji płatniczej, z wyjątkiem przypadku gdy dostawca płatnika ma uzasadnione i należycie udokumentowane podstawy, aby podejrzewać oszustwo, i poinformuje o tym w formie pisemnej organy powołane do ścigania przestępstw. W przypadku gdy płatnik korzysta z rachunku płatniczego, dostawca płatnika przywraca obciążony rachunek płatniczy do stanu, jaki istniałby, gdyby nie miała miejsca nieautoryzowana transakcja płatnicza.

Niezależnie od powyższego, należy dodać, że od czasów wprowadzenia ww. regulacji odnośnie do silnego uwierzytelnienia klienta, nastąpił znaczny rozwój oszustw polegających na kradzieży danych uwierzytelniających, czy też na manipulowaniu wolą płatnika, wskutek której dochodzi do prawidłowego uwierzytelnienia transakcji, ale przez osobę, która dokonuje transakcji na rzecz oszusta (tak jak w przypadku opisanego przez Panią Senator, podszywania się pod pracownika banku czy też innych przestępstw w których płatnik nieświadomie udziela oszustom dostępu do swoich środków).

W tym miejscu należy wskazać, że 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.

W związku z powyższym Ministerstwo Finansów w aktualnym stanie prawnym nie widzi możliwości zmiany obowiązujących w tym zakresie przepisów jedynie na poziomie krajowym. W tym miejscu należy nadmienić o toczącym się obecnie na

poziomie Rady UE procesie uzgodnieniowym, dotyczącym: 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.

Analizując zaproponowane w powyższych aktach prawnych zasady dotyczące bezpieczeństwa transakcji płatniczych, należy zauważyć, że temat oszukańczych transakcji płatniczych stanowi jeden z istotnych obszarów ww. regulacji i zostanie on istotnie rozwinięty w porównaniu z obowiązująca obecnie dyrektywą PSD2.

Jedną z najistotniejszych kwestii proponowanych w rozporządzeniu PSR, jest propozycja wprowadzenia art. 59, zgodnie z którym jeśli dochodzi do manipulacji stosowanej przez osobę trzecią wobec konsumenta, która doprowadziła do nielegalnych autoryzowanych 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 w ramach ww. prac nad PSD i PSR prowadzona jest dyskusja odnośnie do 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.

W trakcie prac grupy Rady UE, dotyczącej ww. przepisów, Polska jako Państwo sprawujące obecnie Prezydencję w Radzie będzie procedowała wszelkie propozycje zapewniające jak największa 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.

Z wyrazami szacunku

Z upoważnienia Ministra Finansów/W zastępstwie Ministra Finansów

Jurand Drop
podsekretarz stanu