Minister
Finansów i Gospodarki

Warszawa, 29 maja 2026 roku

Sprawa: Interpelacja nr 17149
Znak sprawy: FN1.054.5.2026
Kontakt: Kancelaria MF
tel.: +48 22 694 55 55
e-mail: kancelaria@mf.gov.pl

Pan Włodzimierz Czarzasty
Marszałek Sejmu
Rzeczypospolitej Polskiej

Szanowny Panie Marszałku,

w odpowiedzi na interpelację numer 17149 Posła na Sejm RP, Pana Jana Michała Dziedziczaka, uprzejmie przedstawiam poniższe wyjaśnienia.

Ad. 1

W odpowiedzi na pytanie pierwsze, warto zauważyć, że Ministerstwo Finansów dokonało analizy przepisów prawnych dotyczących uwierzytelniania użytkownika i przepisów ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2025 r. poz. 644, dalej jako: „ustawa") zawartej w niniejszej odpowiedzi na interpelację, a także skonsultowało kwestie poruszone w interpelacji z Komisją Nadzoru Finansowego (dalej jako: „UKNF") oraz Związkiem Banków Polskich (dalej jako: „ZBP").

Ministerstwo Finansów zwraca uwagę, że banki udostępniają klientom również alternatywne metody uwierzytelniania i autoryzacji, w zależności od stosowanych rozwiązań oraz rodzaju usługi. Mogą to być metody oparte na aplikacji mobilnej banku, bankowości internetowej, autoryzacji w aplikacji, powiadomieniach push lub innych rozwiązaniach przewidzianych w danym banku.

W przypadku wystąpienia indywidualnych trudności, opisanych w interpelacji, rekomendowane jest, aby klient skontaktował się bezpośrednio ze swoim bankiem oraz operatorem telekomunikacyjnym w celu weryfikacji dostępnych metod autoryzacji oraz ewentualnych ograniczeń technicznych.

Ad. 2

W zakresie odpowiedzi na pytanie drugie, można wskazać, że Ministerstwo Finansów nie odnotowało sygnałów, które wskazywałyby na potencjalne występowanie problemu autoryzacji transakcji płatniczych bądź niedostarczania kodów autoryzacyjnych za pomocą wiadomości SMS klientom dostawców usług płatniczych (w tym banków), przebywających za granicą.

UKNF nie otrzymał zgłoszeń klientów polskich banków dotyczących problemów opisywanych w interpelacji.

Z informacji pozyskanych przez ZBP od przedstawicieli banków współpracujących w ramach grup roboczych przy ZBP nie wynika, aby banki otrzymywały negatywne sygnały wskazujące na systemowy problem z dostępnością tej formy uwierzytelniania dla klientów przebywających w USA. ZBP wskazuje także, że w szczególności nie odnotowano informacji, które wskazywałyby na powszechną niedostępność usług bankowych z tego powodu.

Ad. 3

W odniesieniu do odpowiedzi na pytanie trzecie, warto wskazać, że istnieją już rozwiązania dotyczące alternatywnych metod uwierzytelniania klientów zagranicznych innych niż SMS-ów. Wybór możliwości autoryzacji transakcji dla klientów polskiego sektora bankowego nie jest ograniczony wyłącznie do metody autoryzacji poprzez wiadomości SMS, a obejmuje również autoryzację poprzez mobilną aplikację bankową czy autoryzację biometryczną. Obecnie polski sektor bankowy oferuje swoim klientom kilka sposobów autoryzacji przelewu, wobec których klient ma prawo wyboru, bez ograniczenia wyłącznie do jednego sposobu.

Ponadto, można zwrócić uwagę, na regulacje prawne odnośnie do przedstawionej powyżej kwestii uwierzytelniania użytkownika. Silne uwierzytelnienie użytkownika (ang. SCA – Strong customer authentication) zostało wprowadzone do polskiego porządku prawnego poprzez implementację dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego (dalej jako: „dyrektywa PSD2") do ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz. U. 2026 poz. 623, dalej jako: „ustawa o usługach płatniczych" lub „UUP"). Zgodnie z art. 2 pkt 26aa ustawy o usługach płatniczych, silne uwierzytelnienie użytkownika jest uwierzytelnieniem zapewniającym ochronę poufności danych w oparciu o 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

- będących integralną częścią tego uwierzytelniania oraz niezależnych w taki sposób, że naruszenie jednego z tych elementów nie osłabia wiarygodności pozostałych. Natomiast zgodnie z art. 2 pkt 33b UUP, uwierzytelnienie jest to procedura umożliwiająca dostawcy usług płatniczych weryfikację tożsamości użytkownika lub ważności stosowania konkretnego instrumentu płatniczego, łącznie ze stosowaniem indywidualnych danych uwierzytelniających. Ustawa o usługach płatniczych w art. 32i zobowiązuje dostawców usług płatniczych, którymi są m.in. banki, do stosowania silnego uwierzytelniania użytkownika, w przypadku, gdy płatnik:

- uzyskuje dostęp do swojego rachunku w trybie on-line;
- inicjuje elektroniczną transakcję płatniczą;

- przeprowadza za pomocą kanału zdalnego czynność, która może wiązać się z ryzykiem oszustwa związanego z wykonywanymi usługami płatniczymi lub innych nadużyć.

Ponadto zgodnie z art. 43 UUP dostawca (w tym bank) ponosi ryzyko związane z wysłaniem płatnikowi instrumentu płatniczego lub indywidualnych danych uwierzytelniających. Wysyłanie kodów poprzez wiadomości SMS jest popularną metodą autoryzacji przelewu w polskim sektorze bankowym. Z reguły konsumenci podają swoim bankom numery telefonów, które są zarejestrowane u polskich operatorów sieci komórkowej. Niemniej podanie numeru telefonu zarejestrowanego u polskiego operatora telefonicznego nie jest wymogiem prawnym, lecz indywidualną decyzją banku, opartą na wybranym przez siebie modelu biznesowym oraz polityce wewnętrznej. W związku z czym nie we wszystkich bankach zdaje się istnieć wymóg posiadania polskiego numeru telefonu, na który dostarczany będzie kod autoryzacyjny poprzez wiadomość SMS. Niezależnie od powyższego istnieje również możliwość przeprowadzenia autoryzacji poprzez m.in. mobilną aplikację bankową, która to metoda nie wymaga polskiego numeru telefonu, lecz wyłącznie posiadania aktywnej aplikacji danego banku wraz z połączeniem internetowym. Wskazana mobilna autoryzacja jest odporna na typowy błąd ludzki przy przepisywaniu kodu wysłanego przez SMS bądź na niechciane przejęcie takiego SMS. W przeciwieństwie do autoryzacji metodą wiadomości SMS, w mobilnej aplikacji bankowej widoczny jest pełny kontekst operacji (kwota, odbiorca, rodzaj dyspozycji) przed jej zatwierdzeniem, co pozwala natychmiastowo rozpoznać próbę oszustwa.

Wskazać również należy na procedowany na forum europejskim pakiet PSD3/PSR, tj. projekt rozporządzenia w sprawie usług płatniczych w ramach rynku wewnętrznego (dalej jako: „PSR") oraz projekt dyrektywy w sprawie usług płatniczych i usług związanych z pieniądzem elektronicznym. Oba akty są łącznie następcami drugiej, obecnie obowiązującej dyrektywy o usługach płatniczych (tzw. dyrektywy PSD2). Pakiet przewiduje wprowadzenie szerokich obowiązków przy aktywacji aplikacji mobilnej: wymóg silnego uwierzytelnienia z użyciem różnych kanałów komunikacji, niezwłoczne powiadomienie użytkownika o aktywacji oraz obowiązek natychmiastowego zablokowania dostępu, gdy użytkownik zgłosi, że sam aktywacji nie dokonał. Ponadto w ramach rozporządzenia PSR dostawcy usług płatniczych będą zobowiązani do wprowadzenia mechanizmów monitorowania transakcji i stosowania silnego uwierzytelniania klienta.

Ad. 4

W zakresie odpowiedzi na pytanie czwarte, Ministerstwo Finansów zwróciło się o opinię UKNF. Instytucja ta wskazuje, że w odniesieniu do podniesionej w interpelacji kwestii „dostępu obywateli polskich mieszkających w USA do usług polskiego sektora bankowego", należy przede wszystkim zwrócić uwagę, że w świetle przepisów prawa polskiego (ustawy - Prawo bankowe), jak i zapewne przepisów obowiązujących w USA, polskie banki krajowe nie są uprawnione do świadczenia usług bankowych na terytorium USA i na rzecz rezydentów tego państwa.

Według UKNF podstawowy zakres terytorialny działalności banków krajowych ograniczony jest do terytorium Rzeczypospolitej Polskiej, a na zasadach jednego paszportu europejskiego – do terytorium Europejskiego Obszaru Gospodarczego. Zgodnie z opinią UKNF prawdopodobnie z tych względów wynikają zgłaszane w interpelacji trudności z otrzymywaniem SMS-ów autoryzacyjnych na numery

telefonów spoza EOG, nawet w przypadku osób, które korzystały z usług polskich banków na terytorium RP. UKNF zauważa, że nie odnotowuje działalności banków krajowych poza terytorium EOG oraz nie otrzymuje też zgłoszeń klientowskich czy sygnałów od zagranicznych organów nadzoru dotyczących zagranicznej działalności banków, w tym praktyk wobec klientów mieszkających poza Polską, w szczególności w Stanach Zjednoczonych. W opinii UKNF z tych względów UKNF nie prowadzi szczególnego monitoringu takiej działalności lub praktyk.

W ocenie UKNF dostęp obywateli polskich, będących rezydentami państw spoza EOG, do usług bankowych świadczonych przez polskie banki krajowe, może być zapewniony wyłącznie w drodze rozwiązań na poziomie ustaw i umów międzynarodowych.

Ad. 5

Wobec braku zgłoszeń dotyczących problemu wskazanego w przedmiotowej interpelacji skierowanych do Ministerstwa Finansów takie działania systemowe nie są planowane.

Dodatkowo, w zakresie poruszonej w interpelacji kwestii wymogów AML (Anti-Money Laundering, czyli przeciwdziałanie praniu pieniędzy), można zauważyć, że przepisy ustawy wdrażają do polskiego systemu prawa przepisy dyrektywy UE nr 2015/849[1]. Przepisy ustawy określają wymogi prawne odnośnie obowiązku przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu i nie regulują kwestii technicznych systemów informatycznych służących w poszczególnych instytucjach obowiązanych do realizacji tych obowiązków.

Wyjaśniając kwestie prawne dotyczące obowiązków dla instytucji obowiązanych (np. banki) należy zaznaczyć, że przepisy ustawy przewidują możliwość do działania w imieniu klienta instytucji obowiązanej. Zgodnie z art. 34 ust. 2 ustawy instytucje obowiązane, stosując środki bezpieczeństwa finansowego, o których mowa w ust. 1 pkt 1 i 2, identyfikują osobę upoważnioną do działania w imieniu klienta oraz weryfikują jej tożsamość i umocowanie do działania w imieniu klienta.

Zgodnie z art. 33 ust. 1 ustawy instytucje obowiązane stosują wobec swoich klientów środki bezpieczeństwa finansowego. Instytucja obowiązana, w przypadku nawiązywania stosunków gospodarczych lub przeprowadzania transakcji okazjonalnej ma obowiązek, wynikający z art. 33 ust. 2 ustawy, rozpoznania ryzyka prania pieniędzy oraz finansowania terroryzmu związanego z nawiązywanym stosunkiem gospodarczym lub transakcją okazjonalną oraz dokonania jego oceny. Kolejnym obowiązkiem instytucji obowiązanych jest zastosowanie określonych w art. 34 ust. 1 ustawy środków bezpieczeństwa finansowego. Instytucje obowiązane stosują określone w ustawie środki bezpieczeństwa finansowego w przypadkach określonych w art. 35 ustawy.

Zgodnie z art. 41 ust. 1 ustawy, w sytuacji, gdy instytucja obowiązana nie może zastosować jednego ze środków bezpieczeństwa finansowego, nie nawiązuje stosunków gospodarczych, nie przeprowadza transakcji okazjonalnej, nie

[1] Dyrektywa Parlamentu Europejskiego i Rady (UE) nr 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE.

przeprowadza transakcji za pośrednictwem rachunku bankowego, rozwiązuje stosunki gospodarcze. Rezygnacja z nawiązania stosunku gospodarczego lub decyzja o rozwiązaniu stosunku gospodarczego nie może być jednak podyktowana jedynie faktem, że podmiot należy do grupy klientów o podwyższonym ryzyku prania pieniędzy i finansowania terroryzmu (zgodnie z wytycznymi Europejskiego Urzędu Nadzoru Bankowego). Każda decyzja dotycząca takiego klienta powinna zostać oparta na indywidualnej analizie. Instytucje obowiązane mogą rozważyć w powyższych sytuacjach podwyższonego ryzyka podjęcie czynności mających na celu:

- dostosowanie poziomu i intensywności monitoringu w sposób współmierny do ryzyka prania pieniędzy i finansowania terroryzmu związanego z klientem,
- oferowanie wyłącznie podstawowych produktów i usług finansowych, które ograniczają możliwość nadużywania tych produktów i usług przez użytkowników do celów związanych z przestępstwami finansowymi. Takie podstawowe produkty i usługi mogą również ułatwić instytucjom identyfikację nietypowych transakcji lub schematów transakcji, w tym niezamierzonego wykorzystania produktu. Ważne jest jednak, aby wszelkie ograniczenia były proporcjonalne i nie ograniczały w sposób nieuzasadniony lub niepotrzebny dostępu klientów do produktów i usług finansowych;
- dokonanie skutecznej weryfikacji i dokumentacji tożsamości, w przypadku klienta, będącego osobą fizyczną, o statusie podwyższonego ryzyka.

Ustawa daje instytucjom obowiązanym możliwość wyboru metod i sposobów realizacji nałożonych przez ustawę obowiązków. Ważne jest, aby przez ich realizację osiągnięty został cel ustawy, jakim jest przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu.

Za prawidłową realizację powyższych obowiązków w tym za prawidłowe zarządzanie ryzykiem prania pieniędzy oraz finansowania terroryzmu oraz za podejmowanie decyzji o poziomie przypisanego ryzyka, a w konsekwencji decyzji o nawiązaniu lub odmowie nawiązania relacji z klientem odpowiadają instytucje obowiązane.

Generalny Inspektor Informacji Finansowej nie ma ustawowej legitymacji do ingerencji w powyższe decyzje instytucji obowiązanych. Generalny Inspektor Informacji Finansowej nie ma również wpływu na politykę biznesową instytucji obowiązanych i ich relacje z poszczególnymi klientami.

Należy dodać, że klientom instytucji obowiązanych przysługuje w sprawie naruszenia zbiorowych interesów konsumentów skarga do Urzędu Ochrony Konkurencji i Konsumentów.
Klient banku ma również prawo skierować wniosek o rozpatrzenie sprawy przez Rzecznika Finansowego lub wystąpić z powództwem do sądu powszechnego.

W zakresie wykluczania niektórych kategorii klientów z nawiązywania stosunków gospodarczych (derisking) Generalny Inspektor Informacji Finansowej wydał komunikat nr 73[2].

[2] https://www.gov.pl/web/finanse/komunikat-nr-73-w-sprawiewykluczania-niektorych-kategorii-klientow-z-nawiazywania-stosunkowgospodarczych-derisking-oraz-skarg-wnoszonych-do-generalnego-inspektorainformacji-finansowej-przez-klientow-instytucji-obowiazanych

Podsumowując, w przypadku trudności opisanych w interpelacji warto, aby klient banku skontaktował się bezpośrednio ze swoim bankiem oraz operatorem telekomunikacyjnym w celu weryfikacji dostępnych metod autoryzacji. Banki udostępniają klientom oprócz potwierdzania kodem SMS, także alternatywne metody uwierzytelniania i autoryzacji, w zależności od stosowanych rozwiązań oraz rodzaju usługi. Mogą to być w szczególności metody oparte na aplikacji mobilnej banku, bankowości internetowej, autoryzacji w aplikacji, powiadomieniach push lub innych rozwiązaniach przewidzianych w danym banku.

Z wyrazami szacunku

Z upoważnienia Ministra Finansów i Gospodarki

Jurand Drop
podsekretarz stanu

w Ministerstwie Finansów