UKNF | URZĄD KOMISJI NADZORU FINANSOWEGO

5 czerwca 2019 r.

Stanowisko UKNF dotyczące identyfikacji klienta i weryfikacji jego tożsamości w bankach oraz oddziałach instytucji kredytowych w oparciu o metodę wideoweryfikacji

Na przestrzeni ostatnich lat obserwowany jest przede wszystkim na rynku bankowym narastający trend obejmowania stosunkami gospodarczymi lub transakcjami nowych produktów i usług oraz oferowania produktów lub usług przy wykorzystaniu nowych kanałów dystrybucji. Jednocześnie, jak potwierdzają doświadczenia z inspekcji przeprowadzonych przez UKNF, w sektorze bankowym występują wątpliwości w zakresie właściwego doboru oraz zastosowania środków bezpieczeństwa finansowego, w szczególności w sytuacji gdy klient nie jest fizycznie obecny w celu nawiązania stosunków gospodarczych lub przeprowadzenia transakcji okazjonalnej.

Niniejszy dokument przedstawia dobre praktyki w zakresie wypełniania obowiązków wynikających z ustawy z dnia 1 marca 2018 r. *o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2018 r. poz. 723 z późn. zm.*; zwanej dalej: *ustawą*), dotyczących identyfikacji klienta i weryfikacji jego tożsamości w bankach oraz oddziałach instytucji kredytowych w oparciu o metodę wideoweryfikacji[1], które powinny znaleźć zastosowanie w bieżącej działalności banków i oddziałów instytucji kredytowych oferujących usługę wideoweryfikacji. Wdrożenie i funkcjonowanie schematu identyfikacji i weryfikacji tożsamości klientów w oparciu o rozwiązania technologiczne (tj. wideoweryfikację przeprowadzaną ewentualnie przy jednoczesnym wykorzystaniu metod biometrycznych) powinno być zgodne ze standardami Rekomendacji D Komisji Nadzoru Finansowego dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach.

Niezależnie od powyższego, zgodnie z dyspozycją art. 33 ust. 4 *ustawy* – „instytucje obowiązane stosują środki bezpieczeństwa finansowego w zakresie i z intensywnością uwzględniającymi rozpoznane ryzyko prania pieniędzy oraz finansowania terroryzmu związane ze stosunkami gospodarczymi lub z transakcją okazjonalną oraz jego ocenę". Powyższe unormowanie wskazuje, że na instytucjach obowiązanych ciąży wymóg ustalenia poziomu i profilu ryzyka klienta i stanowi, że to od zidentyfikowanego przez instytucję obowiązaną poziomu i profilu ryzyka klienta oraz przeprowadzonej przez nią oceny tego ryzyka zależy, w jakim zakresie i jak szczegółowo instytucja obowiązana (w tym przypadku bank lub oddział instytucji kredytowej) zastosuje środki

[1] Treść niniejszego pisma uwzględnia zapisy *Wytycznych Generalnego Inspektora Informacji Finansowej w sprawie identyfikacji klienta instytucji obowiązanej i weryfikacji jego tożsamości w sytuacji braku jego fizycznej obecności* - opublikowanych dnia 22 sierpnia 2018 r. oraz *Komunikatu nr 4 w sprawie korekty komunikatu Generalnego Inspektora Informacji Finansowej z dnia 22 sierpnia 2018 r. w sprawie identyfikacji klienta instytucji obowiązanej i weryfikacji jego tożsamości.*

bezpieczeństwa finansowego wobec swojego klienta, w tym identyfikację klienta oraz weryfikację jego tożsamości, w przypadku, gdy klient nie jest fizycznie obecny w banku w celu nawiązania stosunków gospodarczych lub przeprowadzenia transakcji okazjonalnej.
Proces identyfikacji klienta polega na podaniu bankowi przez klienta swoich danych osobowych (art. 36 ust. 1 *ustawy*). Bank powinien również przeprowadzić weryfikację tożsamości klienta, do której niezbędny jest (zgodnie z art. 37 *ustawy*) dokument stwierdzający tożsamość osoby fizycznej oraz inne dokumenty, dane lub informacje, pochodzące z wiarygodnego i niezależnego źródła.

W zakresie weryfikowania tożsamości klienta bez jego fizycznej obecności – instrumentami najbardziej pewnymi w zastosowaniu są środki identyfikacji elektronicznej, o których mowa w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. *w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającym dyrektywę 1999/93/WE (Dz. Urz. L 257 z 28.08.2014 r., str. 84)*, w tym kwalifikowany podpis elektroniczny.
W przypadku braku możliwości wykorzystania powyższych środków identyfikacji elektronicznej, bank powinien rozważyć zastosowanie – zgodnie z art. 43 ust. 2 pkt 7 *ustawy* – wzmożonych środków bezpieczeństwa finansowego. Należy również uwzględnić dyspozycję art. 43 ust. 2 pkt 9 *ustawy* dotyczącą objęcia stosunkami gospodarczymi lub transakcjami nowych produktów lub usług przy wykorzystaniu nowych kanałów dystrybucji. Tak ogólnie określone normy, przenoszą na bank konieczność ustalenia, jakimi dokumentami, danymi oraz informacjami (tj. materiałami weryfikacyjnymi) będzie się posługiwać w celu weryfikacji tożsamości klienta, a także jakie sposoby uzyskiwania dostępu do materiałów weryfikacyjnych będzie stosować.
Do weryfikacji tożsamości klienta nieobecnego dla celu identyfikacji, bank powinien rozważyć posłużenie się różnymi materiałami weryfikacyjnymi pochodzącymi z wiarygodnych i niezależnych źródeł.
W zakresie weryfikacji tożsamości osoby fizycznej przynajmniej jeden z materiałów weryfikacyjnych powinien być dokumentem stwierdzającym tożsamość w rozumieniu powszechnie obowiązujących przepisów prawa (dowód osobisty, paszport, karta pobytu). Jako przykład kolejnego materiału weryfikacyjnego można wskazać dokument ze zdjęciem, np. prawo jazdy. Jako uzupełniające dokumenty potwierdzające tożsamość klienta i adres jego pobytu można uznać np. rachunki za media. Dodatkowym środkiem bezpieczeństwa, którego stosowanie oczekiwane jest przez KNF, będzie przeprowadzenie pierwszej transakcji za pomocą przelewu bankowego z rachunku klienta (prowadzonego w innej instytucji obowiązanej) na rzecz banku weryfikującego jego tożsamość. Należy jednak pamiętać, że z uwagi na minimalny zakres danych osobowych zawartych w informacji o przelewie, dane te będą służyć jedynie pomocniczo do weryfikacji tożsamości klienta.

Bank może posłużyć się metodą wideoweryfikacji. W tym przypadku powinien przeprowadzić analizę ryzyka w odniesieniu do wprowadzanej usługi wideoweryfikacji, biorąc pod uwagę m.in. model funkcjonowania usługi, możliwe do zastosowania technologie i dostosowane do nich

mechanizmy kontrolne zapewniające odpowiedni poziom bezpieczeństwa usługi, w szczególności mitygowanie rodzajów ryzyka związanych z prawidłową identyfikacją i weryfikacją klienta (np. ryzyka kradzieży tożsamości), w tym odnoszących się do wiarygodności materiałów weryfikacyjnych.

Bank może uzyskiwać dostęp do materiałów weryfikacyjnych za pomocą wideorozmowy, podczas której pracownik banku uzyskuje możliwość bliższej obserwacji klienta i oryginałów dokumentów przedstawionych przez klienta, a także upewnienia się, że materiały weryfikacyjne nie zostały sfałszowane, porównania fotografii w dokumencie tożsamości z osobą, z którą rozmawia oraz sprawdzenia klienta w wiarygodnych bazach danych. Niezależnie od powyższego bank powinien wziąć pod uwagę czynniki behawioralne które mogą wskazywać, że klient np.:

– jest pod wpływem środków odurzających,
– nie działa samodzielnie (obecność osób trzecich),
– nie jest świadomy, że nawiązuje relacje z bankiem (nie ma świadomości, że podjęte działania oznaczają zawarcie umowy, np. na prowadzenie rachunku).

W przypadku zastosowania usługi wideoweryfikacji bank powinien rozważyć zastosowanie wzmożonych środków bezpieczeństwa finansowego - minimalizujących ryzyko błędnej weryfikacji klienta.

Poniżej przedstawiono mechanizmy kontrolne mające na celu mitygowanie ryzyka związanego z prawidłową identyfikacją i weryfikacją tożsamości klienta, które mogą być zastosowane zarówno na etapie wdrażania, jak i na etapie funkcjonowania usługi wideoweryfikacji.

- Wprowadzenie rozwiązań w zakresie wideoweryfikacji w banku powinno być poprzedzone przeprowadzeniem analizy ryzyka oraz opiniowaniem i konsultacjami w aspekcie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu (*AML/CFT*), np. przez komórki ds.: biznesowych, bezpieczeństwa, compliance, audytu, *AML/CFT*.
- Posiadanie przez bank formalnie wprowadzonej procedury dotyczącej procesu wideoweryfikacji, zawierającej, m.in.:
  – określenie ograniczeń (mitygantów ryzyka) w odniesieniu do możliwości nawiązania relacji z klientem przy pomocy wideoweryfikacji, np. wyłącznie do obywateli polskich, rezydentów w Polsce, rezydentów w UE, do wybranych produktów depozytowych, wykluczenie osób zajmujących eksponowane stanowisko polityczne – *PEP*, wykluczenie udzielenia kredytu, limity kwotowe operacji (dzienne i/lub miesięczne), itd.,
  – określenie wymogów sprzętowych po stronie klienta (określenie minimalnych wymogów jakościowych sprzętu, np. rozdzielczości kamery, itp.) oraz wymagane narzędzia (stacja robocza, smartfon, tablet),
  – określenie rozwiązań, które zmniejszają ryzyko założenia rachunku w drodze wideoweryfikacji na osobę trzecią, tj. „na słupa" bądź osobę nieświadomą celu wykonywanych czynności, poprzez ustalenie wymogów zewnętrznych dotyczących miejsca i czasu (np. wykluczenie możliwości przeprowadzenia wideoweryfikacji w miejscach

publicznych gdzie panuje duży hałas i obecność w zasięgu kamery osób trzecich, ograniczenie możliwości wstrzymywania/zawieszania procesu – wyjścia osoby spoza obiektywu kamery, wprowadzenie ograniczeń czasowych na wykonanie poszczególnych działań),
  - wymóg monitorowania portfela klientów pozyskanych za pomocą wideoweryfikacji w aspekcie wykorzystania rachunków do prania pieniędzy lub innych działań niezgodnych z prawem,
  - wymóg dokonania przeglądu i ewentualnie modyfikacji procedury (z odpowiednią częstotliwością), w tym pod kątem skuteczności przyjętych kryteriów oceny ryzyka i stosowanych środków bezpieczeństwa finansowego,
  - wymóg archiwizowania zapisów wideo (zarówno dźwięku jak i obrazu) z rozmowy z klientami. W procedurach banku powinny być odpowiednie przepisy dotyczące nagrywania i przechowywania zapisów wideo. Okres przechowywania powinien spełniać wymogi *ustawy*.
- Dokonywanie analizy przypadków odmowy nawiązania relacji z klientem przy pomocy wideoweryfikacji.
- Prowadzenie szkoleń dla pracowników operacyjnych banku, w szczególności w zakresie identyfikacji i weryfikacji tożsamości klienta oraz szkoleń z weryfikacji dokumentów tożsamości.
- Objęcie rozwiązań w zakresie wideoweryfikacji systemem kontroli wewnętrznej oraz systemem informacji zarządczej.
- Jako wzmożone środki bezpieczeństwa w przypadku wideoweryfikacji, należy uznać:
  - sprawdzenie klienta i informacji zawartych w jego dowodzie osobistym - w bazach danych, jak np.:
    - Baza dokumentów zastrzeżonych,
    - Rejestr Dowodów Osobistych,
    - Baza numerów PESEL,
    - Lista Osób Poszukiwanych,
    - System Wymiany Ostrzeżeń o Zagrożeniach,
    - Listy sankcyjne,
    - Wewnętrzne bazy danych banku (tzw. „czarne listy”),
  - upewnienie się o nie przebywaniu osób trzecich w towarzystwie klienta podczas dokonywania wideoweryfikacji oraz o braku jakiejkolwiek ingerencji osób trzecich (np. podpowiedzi kierowane do klienta przez takie osoby), niedopuszczalne jest także opuszczenie pomieszczenia przez klienta, czy inny rodzaj przerwy w toku wideoweryfikacji, co może sugerować konsultacje klienta z osobami trzecimi,
  - przeprowadzanie wideoweryfikacji przynajmniej z częściowym udziałem pracownika banku. W sytuacji gdy bank dopuszcza automatyczną wideoweryfikację, niezbędne jest ścisłe określenie warunków/kryteriów takiego procesu oraz w jakim zakresie i w jakich przypadkach weryfikacja musi zostać potwierdzona bądź uzupełniona przez pracownika

banku. W przypadku całkowicie zautomatyzowanej wideoweryfikacji – zapewnienie sprawdzenia w sposób manualny przez pracownika co najmniej części wniosków klientów (zarejestrowanych automatycznie zapisów), również pod kątem poprawności i jakości zapisu,
- okazanie dowodu osobistego do kamery pod wieloma kątami z obu stron oraz okazanie krawędzi dokumentu w celu weryfikacji jego autentyczności,
- zweryfikowanie autentyczności dokumentu tożsamości oraz integralności danych,
- porównanie zdjęć z dowodu tożsamości bezpośrednio z wizerunkiem klienta oraz ze zdjęciem twarzy (wskazane bez okularów), przy zagwarantowaniu odpowiednio wysokiego poziomu jakości wykonywanych fotografii,
- przesłanie przez konsultanta w trakcie wideoweryfikacji kodu SMS na numer telefonu komórkowego klienta, który musi być podany konsultantowi podczas wideorozmowy,
- pozostawienie w archiwach banku (jako materiału dowodowego) zapisu całej wideorozmowy.

Jednocześnie, jako uzupełniające techniki, które potwierdzają należytą staranność, uznaje się:
- uczestnictwo pracownika banku w całym procesie wideoweryfikacji,
- techniki biometryczne, np. porównanie twarzy klienta ze zdjęciem w dowodzie osobistym (ze wskazaniem procentowego poziomu zgodności),
- wykonywanie OCR dowodu osobistego (oprogramowanie służące do rozpoznawania znaków i całych tekstów - odczyt maszynowy danych zawartych w dokumencie), tak aby wniosek wypełniany był automatycznie danymi z dowodu osobistego, którego zdjęcia wykonano. Jeśli tak, bank powinien weryfikować jakość danych pochodzących z OCR,
- sprawdzanie dodatkowych elementów dowodu osobistego, np. kodu MRZ (obszar, na którym zapisano czcionką dane zawarte w dokumencie - do odczytu maszynowego),
- uwzględnianie przez bank przy wideoweryfikacji czynników behawioralnych i środowiskowych (sposób zachowania klienta przed kamerą, przesłanki wskazujące na możliwość występowania osoby towarzyszącej, rodzaj pomieszczenia, wystarczające oświetlenie, itp.),
- w przypadku wykorzystywania metody biometrycznej, należy określić odpowiednio wysokie progi/poziomy zgodności. W przypadku braku uzyskania ustalonego stopnia poziomu zgodności, weryfikacja biometryczna powinna być potwierdzona w dalszym procedowaniu, np:
  - przez pracownika *back office* (bez połączenia z klientem),
  - przejściem na kanał wideoweryfikacji przy połączeniu *on-line* z klientem,
  - w czasie bezpośredniej wizyty klienta w oddziale banku,
- wykonywanie zdjęcia twarzy klienta z poziomu aplikacji banku (w czasie wykonywania zdjęcia wyzwalana jest kamera, aby zweryfikować czy klient robiący zdjęcie faktycznie jest obecny w procesie weryfikacji, czy np. nie jest wykonywane zdjęcie fotografii).

Ponadto, jako dodatkowy środek bezpieczeństwa finansowego przyjmuje się wprowadzenie wymogu odczytania przez klienta - wskazanego przez bank dłuższego fragmentu tekstu, celem

oceny czy klient nie znajduje się pod wpływem środków odurzających, a w przypadku gdy otwarcie relacji poprzez kanał wideoweryfikacji udostępniono jedynie obywatelom polskim, wspierałoby to ocenę czy klient nie jest obcokrajowcem.

Bank może również zastosować zapytanie klienta o szczegółowe informacje znane jedynie klientowi, które zostały uprzednio uzyskane przez bank od klienta, np. mailowo lub poprzez wypełnienie formularza na stronie internetowej banku. Pytania te powinny być zmienne, tak aby ograniczały możliwość wypracowania schematu umożliwiającego przygotowanie gotowego zestawu odpowiedzi.

Mając na względzie istotny poziom ryzyka związanego z weryfikacją tożsamości klienta nieobecnego dla celów identyfikacji oczekuję, że banki oraz oddziały instytucji kredytowych będą stosowały dobre praktyki związane z oferowaniem usługi wideoweryfikacji.

Powyższe zasady powinny być stosowane odpowiednio przy oferowaniu usługi wideoweryfikacji przez pozostałe instytucje nadzorowane.

Stosowanie przedstawionych wyżej dobrych praktyk będzie podlegało ocenie w toku inspekcji prowadzonych przez UKNF.