UKNF | URZĄD KOMISJI NADZORU FINANSOWEGO

Stanowisko
Urzędu Komisji Nadzoru Finansowego dotyczące identyfikacji klienta instytucjonalnego i weryfikacji jego tożsamości w sektorze finansowym podlegającym nadzorowi Komisji Nadzoru Finansowego w oparciu o metodę wideoweryfikacji

Stanowisko Urzędu Komisji Nadzoru Finansowego dotyczące identyfikacji klienta instytucjonalnego[1] i weryfikacji jego tożsamości w sektorze finansowym podlegającym nadzorowi Komisji Nadzoru Finansowego w oparciu o metodę wideoweryfikacji

Prezentujemy 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 2021 r. poz. 1132, ze zm.*), zwanej dalej: *ustawą*, dotyczących zapewnienia środków bezpieczeństwa finansowego, w szczególności identyfikacji klienta instytucjonalnego (zwanego dalej także: *klientem*) i weryfikacji jego tożsamości w instytucjach obowiązanych, podlegających nadzorowi KNF (zwanych dalej: *podmiotami nadzorowanymi*), w oparciu o metodę wideoweryfikacji[2].

Praktyki te powinny znaleźć zastosowanie w bieżącej działalności *podmiotów nadzorowanych*, wykorzystujących metodę wideoweryfikacji (dotyczy nawiązania stosunków gospodarczych lub przeprowadzenia transakcji okazjonalnych bez fizycznej obecności klienta).

W zakresie zarówno wdrożenia, jak i funkcjonowania modelu identyfikacji i weryfikacji tożsamości klientów w oparciu o rozwiązania technologiczne, mają zastosowanie standardy zawarte w przeznaczonych dla *podmiotów nadzorowanych* rekomendacjach KNF i wytycznych w zakresie IT, np. w *Rekomendacji D dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach*, *Rekomendacji D-SKOK dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w spółdzielczych kasach oszczędnościowo-kredytowych*.

Zgodnie z 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 oznacza, że to na *podmiotach nadzorowanych* ciąży wymóg ustalenia poziomu ryzyka (w tym profilu ryzyka klienta wynikającego m.in. z branży prowadzonej działalności gospodarczej, ryzyka kraju, itd.). W przypadku, gdy nawiązywanie albo utrzymywanie stosunków gospodarczych lub przeprowadzanie transakcji okazjonalnej następuje bez fizycznej obecności klienta, to od zidentyfikowanego przez *podmiot nadzorowany* poziomu i profilu ryzyka klienta oraz przeprowadzonej przez niego oceny tego ryzyka zależy, w jakim zakresie i jak szczegółowo

[1] Klient instytucjonalny - rozumiany jako osoba fizyczna prowadząca działalność gospodarczą, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej.

[2] Stanowisko uwzględnia postanowienia *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* z dnia 18 kwietnia 2019 r.

podmiot nadzorowany zastosuje konieczne środki bezpieczeństwa finansowego wobec swojego klienta, w tym identyfikację klienta oraz weryfikację jego tożsamości.

Proces identyfikacji klienta instytucjonalnego, osób upoważnionych do działania w jego imieniu oraz beneficjenta rzeczywistego klienta instytucjonalnego polega na ustaleniu przez *podmiot nadzorowany*:

- w przypadku osoby fizycznej prowadzącej działalność gospodarczą - nazwy (firmy), numeru identyfikacji podatkowej (NIP) oraz adresu głównego miejsca wykonywania działalności gospodarczej (art. 36 ust. 1 pkt 1 lit. f *ustawy*),
- w przypadku osoby prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej - nazwy (firmy), formy organizacyjnej, adresu siedziby lub adresu prowadzenia działalności, NIP, a w przypadku braku takiego numeru - państwa rejestracji, nazwy właściwego rejestru oraz numeru i daty rejestracji (art. 36 ust. 1 pkt 2 lit. a-d *ustawy*), a także
- danych identyfikacyjnych, tj. imienia i nazwiska oraz numeru PESEL lub daty urodzenia - w przypadku gdy nie nadano numeru PESEL oraz państwa urodzenia osoby reprezentującej/ osób reprezentujących osobę prawną lub jednostkę organizacyjną nieposiadającą osobowości prawnej (art. 36 ust. 1 pkt 2 lit. e *ustawy*),
- danych identyfikacyjnych beneficjenta rzeczywistego obejmujących imię i nazwisko, w przypadku posiadania informacji przez instytucję obowiązaną - również danych, o których mowa w art. 36 ust. 1 pkt 1 lit. b-e *ustawy*[3], (art. 36 ust. 2 *ustawy*),
- danych identyfikacyjnych, tj. imienia i nazwiska, obywatelstwa, oraz numeru PESEL lub daty urodzenia - w przypadku gdy nie nadano numeru PESEL oraz państwa urodzenia, a także serii i numeru dokumentu stwierdzającego tożsamość osoby upoważnionej/ osób upoważnionych do działania w imieniu klienta (art. 36 ust. 3 *ustawy*),
- danych osoby osób upoważnionych do działania w imieniu klienta oraz ich umocowania (art. 34 ust. 2 *ustawy*).

Zgodnie z art. 34 ust. 4 *ustawy*, *podmioty nadzorowane* na potrzeby stosowania środków bezpieczeństwa finansowego mogą przetwarzać informacje zawarte w dokumentach tożsamości klienta i osoby upoważnionej do działania w jego imieniu oraz sporządzać ich kopie.

Podmiot nadzorowany ma obowiązek również przeprowadzić weryfikację tożsamości (tj. dokonać potwierdzenia ustalonych danych identyfikacyjnych):

- klienta,
- osoby upoważnionej/ osób upoważnionych do działania w imieniu klienta oraz
- beneficjenta rzeczywistego/ beneficjentów rzeczywistych (która nie może polegać jedynie na informacjach z Centralnego Rejestru Beneficjentów Rzeczywistych lub rejestru, o którym

[3] To jest danych dotyczących: obywatelstwa, numeru Powszechnego Elektronicznego Systemu Ewidencji Ludności (PESEL) lub daty urodzenia - w przypadku gdy nie nadano numeru PESEL, oraz państwa urodzenia, serii i numeru dokumentu stwierdzającego tożsamość osoby, adresu zamieszkania.

mowa w art. 30 lub art. 31 dyrektywy 2015/849, prowadzonego we właściwym państwie członkowskim),

do której zgodnie z art. 37 ust. 1 *ustawy* niezbędne są: dokument stwierdzający tożsamość osoby fizycznej, dokument zawierający aktualne dane z wyciągu z właściwego rejestru lub inne dokumenty, dane lub informacje pochodzące z wiarygodnego i niezależnego źródła, w tym, o ile są dostępne, ze środków identyfikacji elektronicznej lub z odpowiednich usług zaufania określonych w rozporządzeniu 910/2014 Parlamentu Europejskiego i Rady (UE) 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.* (zwanego dalej: *rozporządzeniem 910/2014*).

W zakresie weryfikowania tożsamości klienta lub osoby upoważnionej/ osób upoważnionych do działania w imieniu klienta, bez fizycznej obecności – instrumentami najbardziej pewnymi w zastosowaniu są środki identyfikacji elektronicznej oraz usługi zaufania umożliwiające identyfikację elektroniczną w rozumieniu *rozporządzenia nr 910/2014*.

W przypadku braku możliwości wykorzystania środków identyfikacji elektronicznej oraz usług zaufania, *podmiot nadzorowany* powinien rozważyć zastosowanie – zgodnie z art. 43 ust. 1 w związku z ust. 2 pkt 7 *ustawy* – wzmożonych środków bezpieczeństwa finansowego. Należy przy tym uwzględnić dyspozycję art. 43 ust. 1 w związku z ust. 2 pkt 9 *ustawy* dotyczącą objęcia (albo oferowania) stosunkami gospodarczymi lub transakcjami nowych produktów lub usług przy wykorzystaniu nowych kanałów dystrybucji lub nowych rozwiązań technologicznych. Tak określone normy przenoszą na *podmiot nadzorowany* konieczność ustalenia jakimi dokumentami, danymi oraz informacjami (tj. materiałami weryfikacyjnymi) będzie się posługiwać w celu weryfikacji (w rozumieniu *ustawy*) tożsamości klienta instytucjonalnego lub osoby upoważnionej/ osób upoważnionych do reprezentowania klienta, a także jakie sposoby uzyskiwania dostępu do materiałów weryfikacyjnych będzie stosować.

W zakresie weryfikacji tożsamości osoby fizycznej prowadzącej działalność gospodarczą, osoby prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej (pamiętając, że w imieniu klienta instytucjonalnego zawsze występuje osoba fizyczna/ osoby fizyczne), *podmiot nadzorowany* powinien posłużyć się dokumentem zawierającym aktualne dane z właściwego rejestru - w Polsce: KRS, CEIDG oraz m.in. zaświadczeniem o numerze identyfikacyjnym REGON, decyzją w sprawie nadania numeru identyfikacji podatkowej NIP, umową spółki, zaświadczeniami ZUS i US oraz innymi dokumentami. W przypadku obcej jurysdykcji, niezbędne są odpisy z innych właściwych rejestrów dotyczących klienta (kopie poświadczenia rejestracji uwierzytelnione przez instytucję do tego powołaną, taką jak np. notariusz).

Niezbędna jest również weryfikacja tożsamości osoby fizycznej upoważnionej/ osób fizycznych upoważnionych do działania w imieniu klienta oraz ich umocowania. W przypadku wątpliwości, w tym dotyczących prawidłowego umocowania takiej osoby, konieczne jest odesłanie jej

do placówki instytucji obowiązanej celem osobistego nawiązania stosunków gospodarczych lub przeprowadzenia transakcji okazjonalnej.

Do weryfikacji tożsamości klienta instytucjonalnego lub osoby upoważnionej/ osób upoważnionych do działania w imieniu klienta, dokonywanej bez fizycznej obecności tych osób, *podmiot nadzorowany* powinien rozważyć posłużenie się różnymi materiałami weryfikacyjnymi pochodzącymi z wiarygodnych i niezależnych źródeł[4].

Jako dodatkowy środek bezpieczeństwa, można uznać przeprowadzenie pierwszej transakcji za pomocą przelewu bankowego z rachunku klienta (prowadzonego w innej instytucji) na rzecz *podmiotu nadzorowanego* weryfikującego jego tożsamość. Nie należy jednak traktować ww. środka jako podstawowego sposobu weryfikowania tożsamości klienta, pamiętając, że z uwagi na minimalny zakres danych dotyczących zleceniodawcy przelewu (zawartych w informacji przekazywanej
wraz z przelewem), dane te mogą służyć jedynie pomocniczo do weryfikacji tożsamości klienta, przeprowadzonej na podstawie innych materiałów weryfikacyjnych.

Należy również zwrócić uwagę na obowiązek przechowywania przez instytucje obowiązane, przez okres 5 lat od dnia zakończenia stosunków gospodarczych z klientem lub od dnia przeprowadzenia transakcji okazjonalnej, uzyskanych w wyniku stosowania środków bezpieczeństwa finansowego kopii dokumentów i informacji, w tym informacji uzyskanych za pomocą środków identyfikacji elektronicznej oraz usług zaufania umożliwiających identyfikację elektroniczną w rozumieniu *rozporządzenia 910/2014* (art. 49 ust. 1 pkt 1 *ustawy*).

Przy rozważaniu sposobów uzyskiwania dostępu do materiałów weryfikacyjnych *podmiot nadzorowany* powinien dokładnie przeanalizować rodzaje ryzyka z tym związane, zwłaszcza odnoszące się do możliwości wprowadzenia w błąd co do prawdziwości materiałów weryfikacyjnych.

Wymogi dotyczące stosowania wideoweryfikacji

Podmiot nadzorowany powinien przeprowadzić analizę ryzyka w odniesieniu do wprowadzanej metody wideoweryfikacji, biorąc pod uwagę m.in. model jej funkcjonowania, możliwe do zastosowania technologie i dostosowane do nich mechanizmy kontrolne zapewniające odpowiedni poziom bezpieczeństwa. Dotyczy to w szczególności mitygowania ryzyk związanych z nieprawidłową identyfikacją i weryfikacją tożsamości klienta lub osoby upoważnionej/ osób

[4] Rodzaje materiałów weryfikacyjnych pochodzących z wiarygodnych i niezależnych źródeł zostały szczegółowo określone w *Stanowisku UKNF dotyczącym identyfikacji klienta i weryfikacji jego tożsamości w bankach oraz oddziałach instytucji kredytowych w oparciu o metodę wideoweryfikacji* (z dnia 5 czerwca 2019 r.).

upoważnionych do działania w imieniu klienta (np. ryzyka kradzieży tożsamości), w tym odnoszących się do wiarygodności materiałów weryfikacyjnych.

Podmiot nadzorowany może uzyskiwać dostęp do materiałów weryfikacyjnych za pomocą wideorozmowy, w sposób uwzględniający również kwestie reprezentacji łącznej klienta.

Podczas wideorozmowy *podmiot nadzorowany* uzyskuje możliwość bliższej obserwacji klienta lub osoby upoważnionej/ osób upoważnionych do działania w imieniu klienta i oryginałów dokumentów przedstawionych przez osobę/ osoby uczestniczące w wideoweryfikacji, a także możliwość upewnienia się, że materiały weryfikacyjne nie zostały sfałszowane, poprzez w szczególności porównanie fotografii w dokumencie tożsamości klienta lub osoby upoważnionej/ osób upoważnionych do działania w imieniu klienta z wyglądem osoby, z którą nawiązano wideorozmowę oraz sprawdzenia, czy klient lub osoba upoważniona/ osoby upoważnione do działania w imieniu klienta występują w wiarygodnych bazach danych. W przypadku reprezentacji łącznej klienta instytucjonalnego wideoweryfikacja następuje w trakcie odrębnych sesji dla każdej z osób upoważnionych. Niezależnie od powyższego *podmiot nadzorowany* powinien wziąć pod uwagę czynniki behawioralne, które mogą wskazywać, że klient lub osoba upoważniona do działania w imieniu klienta, np.:

- znajduje się pod wpływem środków odurzających,
- nie działa samodzielnie (obecność osób trzecich),
- nie jest świadoma, że nawiązuje relacje z *podmiotem nadzorowanym* (tzn. nie ma świadomości, że podjęte działania oznaczają zawarcie umowy, np. o prowadzenie rachunku).

W przypadku wdrożenia metody wideoweryfikacji, *podmiot nadzorowany* powinien rozważyć zastosowanie wzmożonych środków bezpieczeństwa finansowego minimalizujących ryzyko błędnej weryfikacji tożsamości klienta lub osoby upoważnionej/ osób upoważnionych do działania w imieniu klienta.

Poniżej przedstawiono przykładowe mechanizmy kontrolne, mające na celu mitygowanie ryzyk związanych z nieprawidłową identyfikacją i weryfikacją tożsamości klienta oraz osoby upoważnionej/ osób upoważnionych do działania w imieniu klienta, które mogą być zastosowane zarówno na etapie wdrażania, jak i na etapie funkcjonowania metody wideoweryfikacji:

- wprowadzenie rozwiązań w zakresie wideoweryfikacji powinno być poprzedzone przeprowadzeniem wszechstronnej analizy ryzyka oraz opiniowaniem i konsultacjami w aspekcie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu (*AML/CFT*), przez stosowne osoby, zespoły lub jednostki organizacyjne *podmiotu nadzorowanego*;
- posiadanie przez *podmiot nadzorowany* formalnie wprowadzonej procedury dotyczącej procesu wideoweryfikacji, zawierającej, m.in.:
  - określenie podmiotowych ograniczeń ryzyka (tzw. mitygantów ryzyka) – w tym związanych z ryzykiem geograficznym w odniesieniu do możliwości nawiązania relacji z klientem przy

pomocy wideoweryfikacji, np. ograniczenie takiej możliwości wyłącznie do obywateli i podmiotów polskich, rezydentów w Polsce, rezydentów w UE i/lub EOG. Wymóg lub możliwość wyłączenia podmiotów zarejestrowanych w krajach wysokiego ryzyka oraz ewentualnie powiązanych z osobami zajmującymi eksponowane stanowiska polityczne – *PEP*. Odesłanie do osobistego nawiązania relacji z *podmiotem nadzorowanym* (oraz ewentualne nadawanie dodatkowych punktów ryzyka w ramach systemu oceniania/ kryteriów punktacji/ matrycy ryzyka *ML/FT* dotyczącej klienta) w przypadku nietypowej formy prawnej, nietypowej lub nadmiernie złożonej struktury własnościowej klienta, biorąc pod uwagę rodzaj i zakres prowadzonej przez niego działalności gospodarczej, podmiotów w fazie organizacji albo rozpoczynających działalność, powiązanych z *PEP*, cech klienta, które wskazują na korzystanie z określonych usług niezgodnie z jego profilem, jeżeli zarejestrowanie podmiotu nastąpiło w innej jurysdykcji niż dopuszczalna proceduralnie dla metody wideoweryfikacji,

- określenie przedmiotowych mitygantów ryzyka – m.in. okresowego (np. w ciągu 6 miesięcy od nawiązania relacji) ograniczenia oferty do wybranych produktów, wykluczenia udzielenia kredytu, limitów kwotowych operacji (dziennych i/lub miesięcznych), posiadania tylko 1 kanału dystrybucji (dostarczania usług), korzystania wyłącznie z elektronicznej metody transferu środków, wyłączenia transakcji gotówkowych, itd.,
- określenie sposobu weryfikacji tożsamości klientów oraz osoby upoważnionej/ osób upoważnionych do działania w imieniu klienta, polegającego na zebraniu i potwierdzeniu dokumentów służących do identyfikacji i weryfikacji tożsamości klienta oraz osoby upoważnionej/ osób upoważnionych do działania w imieniu klienta (w zależności od formy prawnej i typu działalności wnioskodawcy). Sprawdzenie klienta i osób upoważnionych do działania w imieniu klienta oraz osób reprezentujących klienta na określonych przez *podmiot nadzorowany* listach (w tym sankcyjnych) i w bazach danych (w tym dotyczących *PEP*). W odniesieniu do beneficjenta rzeczywistego, ocena czy jego dane są zgodne z zebranymi informacjami, czy beneficjent posiada status *PEP*, lub czy znajduje się na listach sankcyjnych. Dokonywanie innych działań weryfikacyjnych, np. dostępnych w ramach serwisów informacyjnych (np. *PAP, Reuters, Bloomberg*), na stronach internetowych klientów, w komercyjnych bazach danych (dotyczących informacji gospodarczych),
- określenie precyzyjnych warunków odmowy nawiązania relacji z klientem przy pomocy wideoweryfikacji lub wezwania go do bezpośredniego spotkania w siedzibie albo placówce *podmiotu nadzorowanego*,
- określenie wymogów sprzętowych po stronie klienta (określenie minimalnych wymogów jakościowych sprzętu, np. rozdzielczości kamery, itp.) oraz wymaganych narzędzi (np. stacja robocza, notebook, smartfon, tablet),

- określenie rozwiązań, które zmniejszają ryzyko założenia rachunku w drodze wideoweryfikacji w sposób pozorny, z wykorzystaniem tożsamości osoby trzeciej, która nie ma faktycznego związku z danym klientem instytucjonalnym[5],
- zapewnienie, aby otwarcie rachunku było poprzedzone otrzymaniem i sprawdzeniem pełnej dokumentacji na temat klienta według listy kontrolnej *podmiotu nadzorowanego* (*checklist*) i zatwierdzone przez zwierzchnika zespołu procesującego bądź inne wyznaczone zespoły lub osoby,
- wymóg bieżącego monitorowania portfela klientów pozyskanych za pomocą wideoweryfikacji w aspekcie wykorzystania rachunków do prania pieniędzy lub innych działań niezgodnych z prawem, w tym również w zakresie:
  - obserwacji przepływów środków przez rachunek klienta (m.in. czy wpływy pochodzą z wiarygodnych instytucji sektora finansowego i czy są przekazywane z rachunku klienta jedynie do wiarygodnych instytucji sektora finansowego) oraz kierunków geograficznych transferów pieniężnych (zwłaszcza pod kątem krajów wysokiego ryzyka, krajów podlegających sankcjom), wykorzystywanych walut transakcji, itd.,
  - celu, regularności transakcji i przeznaczenia rachunku – m.in. czy przeprowadzane transakcje odpowiadają ustalonemu profilowi klienta odnośnie celu przeprowadzanych operacji,
  - rodzaju produktów, usług i sposobów ich dystrybucji – np. realizacja jednorazowych transakcji, odbiegających sposobem realizacji i wartością od typowej dla danej operacji,
  - źródeł i poziomu wartości majątkowych deponowanych przez klienta oraz wartości przeprowadzanych transakcji – np. występowanie transakcji przewyższających wartość oczekiwaną ze względu na ustalony profil klienta i charakter danej usługi,
  - stwierdzonych utrudnień w kontakcie osobistym z osobą upoważnioną/ osobami upoważnionymi do działania w imieniu klienta - np. nieudane próby kontaktu w celu potwierdzenia danych, zwłaszcza dotyczących transakcji,
- precyzyjne określenie procesu eskalacji i decyzji w przypadku konieczności modyfikacji poziomu ryzyka klienta lub zgłoszenia podejrzenia do Generalnego Inspektora Informacji Finansowej – GIIF, względnie innych organów lub służb w przypadku podejrzenia innych przestępstw niż pranie pieniędzy lub finansowanie terroryzmu,
- wymóg dokonania przeglądu i ewentualnie modyfikacji procedury (z odpowiednią częstotliwością), w tym pod kątem skuteczności przyjętych kryteriów oceny ryzyka i stosowanych środków bezpieczeństwa finansowego,

[5] Szczegółowo opisano w *Stanowisku UKNF dotyczącym identyfikacji klienta i weryfikacji jego tożsamości w bankach oraz oddziałach instytucji kredytowych w oparciu o metodę wideoweryfikacji* (z dnia 5 czerwca 2019 r.).

- wymóg archiwizowania zapisów wideo (zarówno dźwięku jak i obrazu) z rozmowy z klientem, osobą upoważnioną/ osobami upoważnionymi do działania w imieniu klienta. W procedurze *podmiotu nadzorowanego* powinny znajdować się odpowiednie przepisy dotyczące nagrywania i przechowywania zapisów wideo. Okres przechowywania powinien spełniać wymogi *ustawy*;

- dokonywanie przez właściwe komórki organizacyjne okresowych analiz/ regularnych przeglądów poziomu ryzyka związanego z wykorzystaniem metody wideoweryfikacji oraz przekazywanie ich wyników do odpowiednich szczebli zarządczych i decyzyjnych, w tym m.in. dokonywanie analizy:
  - przypadków odmowy nawiązania relacji z klientem przy pomocy wideoweryfikacji dotyczącej głównych przyczyn tego rodzaju odmowy i sposobów zakończenia sprawy (nawiązanie relacji poprzez osobistą wizytę klienta lub osoby upoważnionej/osób upoważnionych do działania w imieniu klienta, w placówce *podmiotu nadzorowanego*, skierowanie informacji do GIIF, bądź zawiadomienia do prokuratury, itd.),
  - portfela klientów pozyskanych za pomocą wideoweryfikacji w aspekcie wykorzystania rachunków, np. do prania pieniędzy, nadużyć, lub innych działań niezgodnych z prawem oraz czy klienci pozyskani w drodze wideoweryfikacji byli przedmiotem zapytań organów ścigania, UKNF lub GIIF;

- prowadzenie szkoleń dla pracowników operacyjnych *podmiotu nadzorowanego*, w szczególności w zakresie identyfikacji i weryfikacji tożsamości klienta oraz osoby upoważnionej/ osób upoważnionych do działania w imieniu klienta, a także szkoleń dotyczących weryfikacji autentyczności dokumentów tożsamości osób fizycznych;

- objęcie rozwiązań w zakresie wideoweryfikacji systemem kontroli wewnętrznej oraz systemem informacji zarządczej;

- za wzmożone środki bezpieczeństwa, o których mowa w *ustawie*, w przypadku wideoweryfikacji, należy uznać w szczególności:
  - sprawdzenie klienta, w tym informacji zawartych w jego dowodzie osobistym (lub paszporcie) w przypadku osób fizycznych prowadzących działalność gospodarczą; sprawdzenie osoby upoważnionej do działania w imieniu klienta/ osób upoważnionych do działania w imieniu klienta będącego osobą prawną lub jednostką organizacyjną nieposiadającą osobowości prawnej oraz informacji zawartych w ich dowodach osobistych (lub paszportach) w bazach danych, jak np.:
    - Baza Dokumentów Zastrzeżonych,
    - Rejestr Dowodów Osobistych,
    - PRADO (Publiczny rejestr *on-line* autentycznych dokumentów tożsamości i dokumentów podróży),
    - Rejestr Dłużników Biura Informacji Gospodarczej,

- Biuro Informacji Kredytowej,
- Baza Numerów PESEL,
- Lista Osób Poszukiwanych,
- Ognivo,
- System Wymiany Ostrzeżeń o Zagrożeniach,
- wewnętrzne bazy danych *podmiotu nadzorowanego* i/lub grupy kapitałowej, zrzeszeń Banków Spółdzielczych, itd. (tzw. „czarne listy")[6].

Jednocześnie, jako uzupełniające techniki, które potwierdzają należytą staranność, uznaje się np.:

- wykorzystanie za zgodą klienta, osoby upoważnionej/ osób upoważnionych do działania w imieniu klienta - geolokalizacji,
- ocenę zgodności rodzaju stosowanej na urządzeniu mobilnym aplikacji, z aplikacjami używanymi w kraju zamieszkania klienta, osoby upoważnionej/ osób upoważnionych do działania w imieniu klienta lub kraju zarejestrowania,
- ocenę szybkości/ sprawności obsługi aplikacji klienta oraz aplikacji *podmiotu nadzorowanego*[7].

Mając na względzie istotny poziom ryzyka związanego z identyfikacją i weryfikacją tożsamości klienta i osób upoważnionych do jego reprezentowania, w przypadku nawiązania albo utrzymywania stosunków gospodarczych lub przeprowadzenia transakcji okazjonalnych bez ich fizycznej obecności, oczekuje się, że *podmioty nadzorowane* będą stosowały dobre praktyki związane
z oferowaniem usługi wideoweryfikacji.

Jednocześnie informujemy, że zaprezentowane Stanowisko nie uchyla oraz nie zmienia *Stanowiska UKNF dotyczącego identyfikacji klienta i weryfikacji jego tożsamości w bankach oraz oddziałach instytucji kredytowych w oparciu o metodę wideoweryfikacji* opublikowanego 5 czerwca 2019 r.

[6] Pozostałe wzmożone środki bezpieczeństwa w przypadku wideoweryfikacji opisano w *Stanowisku UKNF dotyczącym identyfikacji klienta i weryfikacji jego tożsamości w bankach oraz oddziałach instytucji kredytowych w oparciu o metodę wideoweryfikacji* (z dnia 5 czerwca 2019 r.).

[7] Pozostałe uzupełniające techniki, które potwierdzają należytą staranność, opisano w *Stanowisku UKNF dotyczącym identyfikacji klienta i weryfikacji jego tożsamości w bankach oraz oddziałach instytucji kredytowych w oparciu o metodę wideoweryfikacji* (z dnia 5 czerwca 2019 r.).

Urząd Komisji Nadzoru Finansowego

ul. Piękna 20

00-549 Warszawa