ANEKS NR 2 – ANALIZA RYZYKA PRANIA PIENIĘDZY ORAZ FINANSOWANIA TERRORYZMU WEDŁUG SEKTORÓW

OBSZARY

Obszar	Pranie pieniędzy			Finansowanie terroryzmu		
	Podatność uśredniona	**Zagrożenie uśrednione**	**Oszacowany poziom ryzyka**	**Podatność uśredniona**	**Zagrożenie uśrednione**	**Oszacowany poziom ryzyka[1]**
1. Obszar – bankowość	2,75	2,75	2,65	2,75	3,0	2,31
2. Obszar – usługi płatnicze (oferowane przez inne podmioty niż banki)	3,0	2,33	2,64	3,33	3,67	2,68
3. Obszar – ubezpieczenia	2,0	2,0	2,20	3,0	1,0	1,92
4. Obszar – inne instytucje finansowe	2,0	2,2	2,25	2,0	1,0	1,56
5. Obszar – wymiana walut	2,33	3,33	2,64	2,0	2,0	1,80
6. Obszar – waluty wirtualne	3,0	3,0	2,80	3,0	3,0	2,40
7. Obszar - usługi telekomunikacyjne powiązane z płatnościami mobilnymi	4,0	2,0	2,92	4,0	1,0	2,28
8. Obszar – fizyczny przewóz wartości majątkowych przez granicę	3,5	3,5	3,10	,0	3,5	2,88
9. Obszar – gry hazardowe	2,0	2,75	2,38	2,0	1,0	1,56
10. Obszar – organizacje typu non-profit	3,0	3,0	2,80	3,0	2,0	2,16

[1] Oszacowany poziom ryzyka dla każdego sektora został wyliczony zgodnie z zasadami przeprowadzania krajowej oceny ryzyka, sformułowanymi w Aneksie nr 1. Dla każdego obszaru oszacowano poziom uśredniony zagrożenia i podatności prania pieniędzy oraz oddzielnie finansowania terroryzmu. Następnie oszacowano poziom prawdopodobieństwa oddzielnie dla prania pieniędzy oraz finansowania terroryzmu w każdym sektorze (na podstawie wzoru: Pprs=40%*Zps+60%*Pps, gdzie Pprs – Poziom prawdopodobieństwa, Zps – poziom zagrożenia, Pps – poziom podatności). W kolejnym etapie wyliczono dla każdego sektora ryzyko prania pieniędzy oraz ryzyko finansowania terroryzmu dla kazdego oddzielnie (wg wzoru: Rps=60%*Pprs+40%*Krp, gdzie: Rps – Poziom ryzyka, Pprs – Poziom prawdopodobieństwa, Krp – poziom konsekwencji PP do oceny „ryzyka podstawowego"). Przyjęte założenia dotyczące poziomu konsekwencji w obszarze prania pieniędzy w zakresie ryzyka podstawowego oszacowano na poziomie 2,5, natomiast założenia dotyczące poziomu konsekwencji w obszarze finansowania terroryzmu w zakresie ryzyka podstawowego oszacowano na poziomie 1,5.

11. Obszar – finansowanie społecznościowe	4,0	2,0	2,92	4,0	2,0	2,52
12. Obszar - handel dobrami o wysokiej wartości	3,0	2,5	2,68	3,0	1,5	2,04
13. Obszar – działalność gospodarcza (ogólnie)	2,5	4,0	2,86	2,0	2,0	1,80
14. Obszar - nieruchomości	2,0	3,0	2,44	2,0	3,0	2,04

1. Obszar – bankowość

Opis sektora – zawarty jest w podrozdziale 2.1.2. KOR „Sektory rynku finansowego" oraz w podrozdziale 7.2.1 „*Podatność rynku finansowego*".

Scenariusze wystąpienia ryzyka (tj. możliwe przykłady wystąpienia ryzyka) zarówno w przypadku prania pieniędzy, jak i finansowania terroryzmu - dotyczyły wykorzystania do prania pieniędzy i finansowania terroryzmu produktów finansowych w postaci rachunku bankowego, kredytów i pożyczek, anonimowych kart przedpłaconych (nośników pieniądza elektronicznego wydawanych przez podmioty zagraniczne – instytucje pieniądza elektronicznego oferujące swoje produkty w Polsce na podstawie paszportu europejskiego) oraz transferów środków pieniężnych. Szczegółowy opis znajduje się w scenariuszach do konkretnego obszaru ryzyka poniżej.

Pranie pieniędzy

Tabela 1

Rodzaj wykorzystanych usług, produktów finansowych	Rachunek bankowy
Ogólny opis ryzyka	Wykorzystanie rachunku do gromadzenia i transferowania pieniędzy pochodzących z nielegalnych źródeł
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Gromadzenie na rachunku bankowym środków (poprzez wpłaty gotówkowe lub przelewy z innych rachunków), celem ich wypłaty w gotówce lub dalszego transferowania, najczęściej na rachunki w instytucjach kredytowych, ulokowanych w jurysdykcjach nieprzestrzegających międzynarodowych standardów i rekomendacji z zakresu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu (PPP/PFT). 2. Wykorzystywanie rachunków bankowych prowadzonych dla rzeczywiście istniejących firm. Transferowanie środków pochodzących z nielegalnych źródeł poprzez łańcuch rachunków bankowych należących do powiązanych podmiotów gospodarczych, pod fikcyjnymi tytułami (np. zapłaty za usługi lub pożyczek czy też ich spłaty), celem odseparowania ich od pierwotnego źródła pochodzenia. 3. Wykorzystanie rachunków bankowych założonych na podstawione osoby (słupy) lub na firmy nieprowadzące rzeczywistej działalności gospodarczej (przedsiębiorstwa symulujące) do realizowania transakcji z wykorzystaniem środków pochodzących z nielegalnych źródeł. 4. Otwieranie rachunków bankowych na rzecz zagranicznej osoby prawnej (w szczególności zarejestrowanej w raju podatkowym), a następnie wykorzystanie tych rachunków do wpłat i wypłat gotówkowych, a także przelewów z i na zagraniczne rachunki bankowe w celu ukrycia nielegalnego źródła pochodzenia środków użytych w tych transakcjach.

	5. Otwieranie rachunków bankowych przez osoby fizyczne na podstawie fałszywego dowodu tożsamości. Wykorzystanie rachunku do wprowadzania środków pochodzących z nielegalnych źródeł do systemu bankowego i dalszego ich transferowania. 6. Udostępnienie rachunków bankowych klientom przez banki z usługą tworzenia indywidualnych rachunków wirtualnych (rachunki typu *collect*), służących do identyfikacji płatności przychodzących. Usługa dedykowana jest dla klientów firmowych posiadających dużą liczbę kontrahentów i otrzymujących znaczną liczbę wpłat od np. licznych os. fizycznych. Usługa ta, może zostać wykorzystana do prowadzenia fikcyjnej działalności gospodarczej w zakresie udzielania rzekomych pożyczek. Indywidualne rachunki bankowe przypisane zostają do indywidualnych kredytobiorców, celem pobierania opłat rezerwacyjnych tj. prowizje przygotowawcze za rozpatrzenie wniosku kredytowego. Zgromadzone środki z rachunkach wirtualnych, zbiorczo i automatycznie transferowane są na rachunek bieżący klienta, a następnie na kolejne rachunki bankowe, bądź wypłacane w gotówce. 7. Wykorzystanie rachunku bankowego przez osoby podające się za uchodźców z Ukrainy, będących członkami organizacji przestępczej o zasięgu międzynarodowym. Komórki tej organizacji są rozlokowane m.in. na terenie Polski. Dokonywane przez te rachunki przepływy finansowe łączą się z przestępstwem prania pieniędzy.
Poziom podatności	3
Uzasadnienie dla poziomu podatności	Otwarcie rachunku bankowego, jak i dokonywanie transakcji - również o międzynarodowym charakterze - za jego pośrednictwem jest stosunkowo łatwe. Istotny jest dostęp do rachunku za pośrednictwem elektronicznych kanałów łączności (w szczególności przez Internet), który umożliwia ukrycie danych rzeczywistych zleceniodawców transakcji - przy wykorzystywaniu tzw. słupów czy przedsiębiorstw symulujących do otwarcia rachunku. Zgodnie z danymi pochodzącymi z Raportu[2] „PRNews.pl: Rynek kont osobistych – I kw. 2022 r." - wynika, że w segmencie bankowości uniwersalnej działa już 35,6 mln ROR-ów. Najwięcej jest obsługiwanych przez takie banki, jak: PKO BP, Pekao i Santander. W porównaniu do danych z końca 2021 r. rynek kont urósł o 394 tys., a w porównaniu do danych sprzed roku o blisko 1,7 mln. Najwięcej rachunków osobistych prowadzi niezmiennie PKO BP – 8,7 mln. Na drugim miejscu jest Bank Pekao – 4,6 mln, a na trzecim Santander – 4,2 mln. Te same trzy banki odnotowały w ciągu minionego roku największy wzrost liczby rachunków. Z opublikowanych przez NBP danych wynika, że na koniec 2021 r. na rynku polskim było 43,3 mln kart płatniczych. Oznacza to, że w ostatnim kwartale 2021r. przybyło 470 tys. kart. Wartość pojedynczej transakcji wynosiła średnio 123 zł. W samym czwartym kwartale 2021 r. dokonano 2,1 mld transakcji kartami płatniczymi o łącznej wartości 254,98 mld zł. Transakcje bezgotówkowe stanowiły już ponad 93 % wszystkich transakcji. W czwartym kwartale 2021 r. liczba wypłat z bankomatów spadła o 6,8 % Wypłata wynosiła średnio 738 zł. Z kolei wartość transakcji kartami w Internecie wzrosła o 1,15 mld zł, czyli o 19 % w porównaniu do poprzedzającego kwartału. Wszystkie podmioty oferujące ww. produkty/usługi są instytucjami obowiązanymi (IO). Podmioty te stosują środki bezpieczeństwa finansowego, choć wciąż ujawniane są podczas kontroli braki w tym obszarze. W związku z trwającym konfliktem wojennym na Ukrainie szczególnym wyzwaniem związanym z prawidłowym stosowaniem środków bezpieczeństwa stanowi prawidłowa identyfikacja i weryfikacja tożsamości uchodźców z Ukrainy, zainteresowanych skorzystaniem z funkcjonujących na rynku finansowym produktów. Z uwagi na trwający konflikt zbrojny utrudnione jest pozyskanie szerszego spektrum dokumentów potwierdzających tożsamość lub wiarygodność klienta. Występują poważne problemy z identyfikacją i weryfikacją osób, które albo w ogóle nie miały żadnych dokumentów, albo miały dokumenty w rodzaju paszportu wewnętrznego pisanego cyrylicą. Właściwa transkrypcja takich dokumentów na alfabet łaciński jest niezwykle utrudniona.

[2] https://prnews.pl/raport-prnews-pl-rynek-kont-osobistych-i-kw-2022-465248 dostęp 25.06.2022 r.

	Poza tym istniejąca bariera językowa i kulturowa pomiędzy pracownikami instytucji obowiązanych, a uchodźcami korzystającymi z rachunku bankowego utrudnia rozpoznanie nietypowych zachowań klienta, zarówno klienta pragnącego założyć np. rachunek bankowy, jak i klienta dokonującego transakcji. Bariera językowa i kulturowa w istotny sposób wpływa na prawidłowe rozpoznanie czynników zwiększonego ryzyka. Stanowi ona ten czynnik behawioralny, który utrudnia prawidłową ocenę odpowiedzi klientów-uchodźców w kwestiach problematycznych, które wymagają dodatkowych informacji czy dokumentów. Instytucje obowiązane posiadają świadomość swoich obowiązków z zakresu PPP/PFT. Efektywnie analizują transakcje, ale w instytucjach obowiązanych pracownicy realizujący zadania z zakresu PPP/PFT w dobie konfliktu zbrojnego na Ukrainie zostali z reguły obarczeni zadaniami z zakresu stosowania sankcji nałożonych na Rosję i Białoruś. Powoduje to sytuację, w której zadaniami z zakresu PPP/PFT zajmuje się faktycznie mniej osób w instytucjach obowiązanych niż przed konfliktem i do prawidłowej realizacji tych zadań PPP/PFT osób tych może być w niektórych przypadkach za mało. Występują też problemy z weryfikacją zagranicznych klientów w centralnych rejestrach beneficjentów rzeczywistych państw UE, zwłaszcza dotyczy to podmiotów o skomplikowanej strukturze kapitałowej. Organy administracji publicznej posiadają wiedzę nt. ryzyka prania pieniędzy oraz finansowania terroryzmu (PP/FT) w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek prania pieniędzy w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. W 2021 r. ogółem zarejestrowano w systemie GIIF 251 zawiadomień opisowych[3] (SAR) od jednostek współpracujących (JW), co stanowi wzrost w stosunku do 2020 r., w którym zarejestrowano ich 179. Od instytucji obowiązanych GIIF zarejestrował w 2021 r. wpływ 3574 SAR. Ich liczba utrzymuje się na wysokim poziomie i jest o ok. 20% wyższa niż średnia z lat 2014-2018. Istniejące przepisy prawne odpowiadają w dużej mierze zakresowi analizowanego ryzyka.
Poziom zagrożenia	4
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie transakcji poprzez założone rachunki bankowe, zarówno rachunki firmowe, jak i rachunki osób fizycznych, do prania pieniędzy wydaje się relatywnie częste. Sposób ten jest szeroko dostępny i jego zastosowanie relatywnie niewiele kosztuje. Dokonywanie transakcji na rachunkach bankowych nie wymaga specjalistycznej wiedzy ani umiejętności. Stosowane przez banki środki bezpieczeństwa finansowego stwarzają co prawda pewne ryzyko dla podmiotów lokujących bądź transferujących środki poprzez rachunek bankowy, ale jest ono przez sprawców łagodzone różnymi sposobami, np. wykorzystaniem „słupów" czy „przedsiębiorstw symulujących" czy poprzez fałszerstwa dokumentów, których weryfikacja dla banku jest utrudniona. GIIF odnotowuje wiele przypadków wykorzystywania rachunków bankowych do prania pieniędzy. WNIOSEK: Wykorzystanie rachunku bankowego do gromadzenia i transferowania pieniędzy pochodzących z nielegalnych źródeł stwarza bardzo wysokie zagrożenie praniem pieniędzy.

[3] SPRAWOZDANIE Generalnego Inspektora Informacji Finansowej z realizacji ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu w 2021 roku, str. 43, na: https://www.gov.pl/web/finanse/sprawozdania-roczne-z-dzialalnosci-generalnego-inspektora-informacji-finansowej. Liczba dotyczy wszystkich zawiadomień opisowych – ML i FT.

Tabela 2

Rodzaj wykorzystanych usług, produktów finansowych	Kredyty i pożyczki
Ogólny opis ryzyka	Pozyskiwanie kredytów i pożyczek i ich spłata środkami pochodzącymi z nielegalnych źródeł
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Zaciąganie kredytów konsumpcyjnych i pożyczek, które następnie relatywnie szybko (przed terminem spłaty kredytu/pożyczki) są spłacane środkami pochodzącymi z nielegalnych źródeł. 2. Zaciąganie kredytów na zakup nieruchomości/ruchomości, często po zawyżonych cenach, przez podstawione osoby (słupy). Środki z kredytów są przekazywane do sprzedawców nieruchomości / ruchomości współpracujących ze sprawcami. Kredyty są spłacane środkami pochodzącymi z nielegalnych źródeł.
Poziom podatności	3
Uzasadnienie dla poziomu podatności	Dostęp do kredytów i pożyczek udzielanych przez banki jest prosty. Jednakże w związku z trwającym konfliktem wojennym na Ukrainie utrudnione jest stosowanie środków bezpieczeństwa związane z prawidłową identyfikacją i weryfikacją tożsamości uchodźców z Ukrainy, zainteresowanych skorzystaniem z funkcjonujących na rynku finansowym produktów. Niekiedy problem stanowi pozyskanie szerszego spektrum dokumentów potwierdzających tożsamość lub wiarygodność takiego klienta. Tym niemniej w zawieraniu umowy pożyczki czy kredytu istnieją pewne ograniczenia związane przede wszystkim z posiadaniem przez klienta zdolności kredytowej i odpowiednich zabezpieczeń. Z tych powodów możliwość wykorzystania słupów lub przedsiębiorstw symulujących do zaciągania kredytów i pożyczek jest utrudniona. Spłaty kredytów i pożyczek można dokonywać również poprzez realizację transakcji o charakterze międzynarodowym, również przy wykorzystaniu osób lub podmiotów trzecich. Według danych Biura Informacji Kredytowej[4] - w maju 2022 r. w porównaniu do maja 2021 r. banki i SKOK-i przyznały więcej (+1,5%) tylko kredytów gotówkowych. W pozostałych rodzajach kredytów odnotowano spadki. Spadła liczba udzielonych kredytów mieszkaniowych (-43,3%), limitów na kartach kredytowych (-29,3%), a także kredytów ratalnych (-4,7%). W ujęciu wartościowym banki i SKOK-i przyznały niższą wartość we wszystkich produktach kredytowych. Najwyższy spadek wartości wystąpił w kredytach mieszkaniowych (-38,6%). Na niższą wartość przyznano limitów na kartach kredytowych (-16,3%), kredytów ratalnych (-3,9%) i gotówkowych (-0,8%). W pierwszych pięciu miesiącach 2022 r. w porównaniu do analogicznego okresu ubiegłego roku, ujemne dynamiki w obu ujęciach odnotowały karty kredytowe (-34,0% oraz -16,7%) oraz kredyty mieszkaniowe (-27,9% i -19,7%). Natomiast dodatnie dynamiki zanotowano w przypadku kredytów ratalnych (+17,4% i +2,7%), a także kredytów gotówkowych (+5,1% i +2,4%). Wszystkie podmioty oferujące ww. produkty/usługi są IO. Te podmioty stosują środki bezpieczeństwa finansowego, choć wciąż ujawniane są podczas kontroli braki w tym obszarze. Posiadają świadomość swoich obowiązków z zakresu PPP/PFT. Efektywnie analizują transakcje – najwięcej SAR, przekazywanych do GIIF, pochodzi od banków/oddziałów instytucji kredytowych/oddziałów banków zagranicznych. Instytucje obowiązane w odpowiedzi na pandemię COVID-19 musiały szybko dostosować swoje systemy sprzedażowe do wymogów w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, by utrzymać sprzedaż produktów. Wiązało się to przede wszystkim z wprowadzeniem rozwiązań technologicznych umożliwiających dystrybucję produktów w systemie sprzedaży na odległość. Występują też problemy z weryfikacją zagranicznych klientów w centralnych rejestrach beneficjentów rzeczywistych państw UE, zwłaszcza dotyczy to podmiotów o skomplikowanej

[4] https://media.bik.pl/informacje-prasowe?offset=0 dostęp 25.06.2022 r.

	strukturze kapitałowej. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje prawdopodobieństwo, że przypadek PP w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia / śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej mierze zakresowi analizowanego ryzyka.
Poziom zagrożenia	2
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie możliwości zawarcia umowy kredytowej bądź umowy pożyczki, a następnie ich spłata środkami pochodzącymi z nielegalnych źródeł nie jest postrzegana w Polsce jako atrakcyjna metoda prania pieniędzy. W przypadku kredytów hipotecznych zagrożenie wykorzystania ich do prania pieniędzy bazuje też na możliwości ustalania cen nieruchomości odbiegających od rynkowych, a także na możliwości składania deklaracji podatkowych w różnych urzędach skarbowych (w zależności od deklarowanego miejsca zamieszkania). Wykorzystujący tą metodę przestępcy są dobrze przygotowani do dostarczenia fałszywej dokumentacji, a ograniczone prawo rzeczowe, jakim jest hipoteka, pomaga w ukryciu rzeczywistego beneficjenta funduszy. Często również pożyczkodawcą są podmioty ulokowane w tzw. „rajach podatkowych". Ten *modus operandi* wymaga jednak planowania, pewnej wiedzy i umiejętności. GIIF otrzymywał informacje o wykorzystywaniu tego sposobu prania pieniędzy. WNIOSEK: Zawarcie umowy kredytowej bądź umowy pożyczki, a następnie ich spłata środkami pochodzącymi z nielegalnych źródeł stanowi wysokie zagrożenie prania pieniędzy.

Tabela 3

Rodzaj wykorzystanych usług, produktów finansowych	Anonimowe karty przedpłacone – nośniki pieniądza elektronicznego wydawane przez podmioty zagraniczne – instytucje pieniądza elektronicznego oferujące swoje produkty w Polsce na podstawie paszportu europejskiego
Ogólny opis ryzyka	Korzystanie z anonimowych kart przedpłaconych w celu utrudnienia identyfikacji sprawców prania pieniędzy
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Anonimowe karty przedpłacone są zasilane przez sprawców środkami pochodzącymi z nielegalnych źródeł. Za pomocą rachunku karty przedpłaconej są następnie dokonywane transfery na rachunki innych osób celem ich wypłaty w gotówce lub dalszych transferów. 2. Anonimowe karty przedpłacone są zasilane przez sprawców środkami pochodzącymi z nielegalnych źródeł. Za pomocą karty przedpłaconej są dokonywane zakupy różnych towarów, które są następnie odsprzedawane innym osobom. 3. Anonimowe wielowalutowe karty przedpłacone niebankowej instytucji płatniczej są zasilane przez sprawców środkami pochodzącymi z nielegalnych źródeł. Za pomocą rachunku wielowalutowej karty przedpłaconej są następnie dokonywane transfery na rachunki innych osób celem ich wypłaty w gotówce lub dalszych transferów. 4. Wykorzystywanie kart przedpłaconych przez osoby podające się za uchodźców z Ukrainy. W rzeczywistości osoby te są członkami zorganizowanej grupy przestępczej. Anonimowe karty przedpłacone są przewożone pomiędzy, np. obszarem UE, a krajami trzecimi gdzie w fazie końcowej ma miejsce wypłata środków pieniężnych zdeponowanych wcześniej na anonimowych kartach przedpłaconych.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Dostęp do kart przedpłaconych będących nośnikiem pieniądza elektronicznego jest stosunkowo łatwy (poprzez Internet). Głównym źródłem ryzyka prania pieniędzy są anonimowe karty przedpłacone oferowane w Polsce, ale wydawane przez emitentów z innych krajów UE. Istnieje możliwość wydawania zgodnie z prawem pieniądza elektronicznego (zapisanego na karcie przedpłaconej lub na

	serwerze), bez identyfikowania i weryfikowania klienta, jakkolwiek w tym zakresie istnieją limity kwot przechowywanych na instrumencie płatniczym, a także limity kwot transakcji określone w dyrektywie 2018/843[5]. Pieniądz elektroniczny i karty przedpłacone mogą być używane do realizacji transakcji o charakterze międzynarodowym. Z uwagi na sprawowanie nadzoru nad zagranicznymi instytucjami pieniądza elektronicznego oferującymi swoje produkty i usługi w Polsce przez władze kraju macierzystego należącego do UE należy zakładać, że posiadają one i stosują się do obowiązujących procedur w zakresie przeciwdziałania praniu pieniędzy oraz finansowania terroryzmu (warto jednak pamiętać, że nie są one instytucjami obowiązanymi w myśl polskich przepisów, o ile nie działają one poprzez oddział ustanowiony w Polsce). Wg informacji NBP[6] na koniec II kw. 2022r. liczba kart przedpłaconych w Polsce wynosiła 1,95 mln szt., wobec 2,25 mln w II kw. 2021r. (spadek o 13,33%). Udział kart przedpłaconych w rynku na koniec II kw. 2022r. wyniósł 4,5%., tj. o 0,6% mniej niż w analogicznym okresie ubr. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia[7] i analizowania informacji, jednak w dużej mierze jest w tym zakresie uzależniony od informacji uzyskanych od zagranicznych jednostek analityki finansowej. Istnieje prawdopodobieństwo, że przypadek prania pieniędzy w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	1
Uzasadnienie dla poziomu zagrożenia	Banki krajowe wydają jedynie karty przedpłacone będące rodzajem kart debetowych. Anonimowe karty przedpłacone - nośniki pieniądza elektronicznego są wydawane przez instytucje pieniądza elektronicznego z innych krajów UE i oferowane klientom w Polsce. Należy zakładać, że ryzyko prania pieniędzy może dotyczyć przede wszystkim tych kart, które są nabywane przez osoby fizyczne. Wymaga to od sprawców wiedzy na temat oferty zagranicznych instytucji pieniądza elektronicznego. Są informacje pochodzące głównie z zagranicy o wykorzystywaniu tego *modus operandi* do prania pieniędzy. WNIOSEK: Wykorzystanie anonimowych kart przedpłaconych w celu utrudnienia identyfikacji osób dokonujących transakcji związanych z praniem pieniędzy jest aktualnie w Polsce na niskim poziomie zagrożenia.

Tabela 4

Rodzaj wykorzystanych usług,	Transfery środków pieniężnych

[5] Tj., dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/843 z dnia 30 maja 2018 r. zmieniającą dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniającą dyrektywy 2009/138/WE i 2013/36/UE (Dz. Urz. UE L 156 z 19.06.2018 r., str. 43).

[6] https://webcache.googleusercontent.com/search?q=cache:WD2NBBEHU3gJ:https://www.nbp.pl/home.aspx%3Ff%3D/systemplatniczy/karty/informacje_kwartalne.html&cd=2&hl=pl&ct=clnk&gl=pl

[7] Zgodnie z artykułem 53 ust. 1 dyrektywy 2015/849, w przypadku gdy dana jednostka analityki finansowej otrzyma raport o transakcji podejrzanej, dotyczący innego państwa członkowskiego UE (np. Polski), niezwłocznie go przekazuje jednostce analityki finansowej tego państwa członkowskiego.

produktów finansowych	
Ogólny opis ryzyka	Wykorzystanie transferów do przekazywania środków do innych jurysdykcji
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Wykorzystanie transferów środków pieniężnych do przekazywania środków pod fikcyjnym tytułem (m.in. na rzecz pomocy rodzinie). Środki przekazywane są w szczególności do banków ulokowanych na obszarze Europy, a także w tzw. rajach podatkowych. 2. Pracownik banku, współpracujący z przestępcami, przyjmuje od nich środki pieniężne pochodzące z nielegalnych źródeł, które następnie za pośrednictwem bezgotówkowych transferów przekazuje na wskazane przez nich rachunki bankowe, ukrywając ich źródło oraz przeznaczenie. 3. Dokonywanie przez osoby podające się za uchodźców z Ukrainy, a faktycznie będące członkami zorganizowanej grupy przestępczej o zasięgu międzynarodowym, transferów finansowych do innych krajów. W końcowej fazie operacji finansowej ma miejsce gotówkowa wypłata środków pieniężnych lub ich dalszy transfer pomiędzy członkami grupy przestępczej. 4. Przyjmowanie i zlecanie nabycia lub zbycia instrumentów finansowych na rachunek dającego zlecenie i/lub wykonywanie doradztwa finansowego przez podmiot nie posiadający odpowiedniego zezwolenia.
Poziom podatności	3
Uzasadnienie dla poziomu podatności	Zlecanie transferów środków pieniężnych za pośrednictwem banków jest stosunkowo łatwe. Część banków świadczy również usługi przekazów pieniężnych w imieniu zagranicznych instytucji płatniczych. Istnieje ograniczona ilość produktów ułatwiających dokonywanie anonimowych transakcji (ewentualnie jest to możliwe w przypadku dokonywania sporadycznych transakcji poniżej progu równowartości 1 tys. EUR lub w przypadku posłużenia się słupem albo przedsiębiorstwem symulującym). Transfery środków pieniężnych mają często charakter międzynarodowy. Wszystkie podmioty oferujące ww. produkty/usługi są IO. Podmioty te stosują środki bezpieczeństwa finansowego, choć wciąż ujawniane są podczas kontroli braki w tym obszarze. W związku z trwającym konfliktem wojennym na Ukrainie szczególnym wyzwaniem związanym z prawidłowym stosowaniem środków bezpieczeństwa stanowi prawidłowa identyfikacja i weryfikacja tożsamości uchodźców z Ukrainy, zainteresowanych skorzystaniem z funkcjonujących na rynku finansowym produktów. Z uwagi na trwający konflikt zbrojny utrudnione jest pozyskanie szerszego spektrum dokumentów potwierdzających tożsamość lub wiarygodność klienta. Występują poważne problemy z identyfikacją i weryfikacją osób, które albo w ogóle nie miały żadnych dokumentów, albo miały dokumenty w rodzaju paszportu wewnętrznego pisanego cyrylicą. Właściwa transkrypcja takich dokumentów na alfabet łaciński jest niezwykle utrudniona. Poza tym istniejąca bariera językowa i kulturowa pomiędzy pracownikami instytucji obowiązanych a uchodźcami korzystającymi z rachunku bankowego utrudnia rozpoznanie nietypowych zachowań klienta, zwłaszcza klienta chcącego dokonać transferu środków pieniężnych. Bariera językowa i kulturowa w istotny sposób wpływa na prawidłowe rozpoznanie czynników zwiększonego ryzyka. Stanowi ona ten czynnik behawioralny, który utrudnia prawidłową ocenę odpowiedzi klientów-uchodźców w kwestiach problematycznych, które wymagają dodatkowych informacji czy dokumentów. Instytucje obowiązane posiadają świadomość swoich obowiązków z zakresu PPP/PFT. Efektywnie analizują transakcje – ale w większości instytucji obowiązanych pracownicy realizujący zadania z zakresu PPP/PFT w dobie konfliktu zbrojnego na Ukrainie zostali z reguły obarczeni zadaniami z zakresu stosowania sankcji nałożonych na Rosję i Białoruś. Powoduje to sytuację, w której zadaniami z zakresu PPP/PFT zajmuje się faktycznie mniej osób w instytucjach obowiązanych niż przed konfliktem i do prawidłowej realizacji zadań PPP/PFT osób tych może być w niektórych przypadkach za mało. Jednakże najwięcej SAR, przekazywanych do GIIF, pochodzi od banków/oddziałów instytucji kredytowych/oddziałów banków zagranicznych. IO mają też problemy z weryfikacją zagranicznych klientów w centralnych rejestrach beneficjentów rzeczywistych państw UE, zwłaszcza dotyczy to

	podmiotów o skomplikowanej strukturze kapitałowej. Zgodnie z opracowaniem NBP p.t. *Porównanie wybranych elementów polskiego systemu płatniczego z systemami innych krajów Unii Europejskiej za 2021 r.,* łączna liczba przelewów wyniosła w 2021 r. ok. 4,03 mld.[8], a w 2020 r. ok. 3,6 mld. (spadek o 0,64%). W 2021 r. Polska zajmowała 13 miejsce wśród państw UE pod względem liczby transakcji instrumentami płatniczymi na 1 mieszkańca. [9] W stosunku do danych za 2020 r., Polska nie zmieniła swojej pozycji w rankingu państw UE. Na jednego Polaka w 2021 r. przypadało 301 transakcji, co w porównaniu do średniej UE oraz średniej dla Strefy Euro (odpowiednio 318 oraz 330 transakcji) oznacza nadal stosunkowo niskie wykorzystywanie bezgotówkowych instrumentów płatniczych w naszym kraju. Na uwagę zasługuje jednak fakt, iż liczba transakcji bezgotówkowych instrumentami płatniczymi na mieszkańca wzrosła w 2021r. w Polsce aż o 19,0% w stosunku do roku 2020, podczas gdy w Strefie Euro wzrost ten wynosił 11,3%, a w Unii Europejskiej 11,9%. Wszystkie podmioty oferujące ww. produkty/usługi są IO. Podmioty te stosują środki bezpieczeństwa finansowego, choć wciąż ujawniane są podczas kontroli braki w tym obszarze. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek prania pieniędzy w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej mierze zakresowi analizowanego ryzyka.
Poziom zagrożenia	4
Uzasadnienie dla poziomu zagrożenia	Pranie pieniędzy poprzez wykorzystanie transferów do przekazywania środków finansowych do innych jurysdykcji jest jedną z najczęściej spotykanych metod. Sposób ten ze względu na dobrze rozwinięty światowy system bankowy jest szeroko dostępny i jego zastosowanie stosunkowo niewiele kosztuje. Zlecanie transferów nie wymaga wiedzy o systemie bankowym ani specjalistycznych umiejętności, jednakże realizacja tego *modus operandi* jest wtedy stosunkowo bezpieczna, gdy bank ze względu na charakter transakcji bądź miejsce transakcji nie jest zobowiązany do stosowania wzmożonych środków badania klienta. Ominięciem tego niebezpieczeństwa jest np. pozyskanie do współpracy pracownika banku. Jeśli zorganizowana grupa przestępcza stworzy system fikcyjnych podmiotów posiadających rachunki bankowe w kraju i za granicą, może dokonywać przelewów i płatności pomiędzy tymi podmiotami, które to transakcje z punktu widzenia uzasadnienia ekonomicznego nie będą podejrzane i bardzo trudne do zakwestionowania. Wykorzystanie transferów do przekazywania środków finansowych do innych jurysdykcji w systemie bankowym jest łatwe, nie wymaga skomplikowanego planowania ani specjalistycznej wiedzy ani umiejętności. WNIOSEK: Wykorzystanie transferów do przekazywania środków finansowych do innych jurysdykcji stwarza bardzo wysokie zagrożenie prania pieniędzy

Finansowanie terroryzmu

[8] Porównanie wybranych elementów polskiego systemu płatniczego z systemami innych krajów Unii Europejskiej za 2021 r., NBP, grudzień 2022 r, s. 33, na: https://www.nbp.pl/SystemPlatniczy/Obrot_bezgotowkowy/Obrot_bezgotowkowy.html

[9] Tamże, str. 34.

Tabela 5

Rodzaj wykorzystanych usług, produktów finansowych	Rachunek bankowy
Ogólny opis ryzyka	Wykorzystanie rachunku bankowego do gromadzenia i transferowania pieniędzy na cele działalności terrorystycznej
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Gromadzenie na rachunku bankowym środków pozyskiwanych w różny sposób (ze źródeł legalnych, jak i nielegalnych), celem dalszej ich wypłaty w gotówce (często w krajach graniczących z krajami, w których działają organizacje terrorystyczne) lub transferowania, najczęściej na rachunki w instytucjach kredytowych, ulokowanych w pobliżu stref konfliktu lub w jurysdykcjach nieprzestrzegających międzynarodowych standardów i rekomendacji z zakresu AML/CTF. 2. Wyprowadzanie aktywów z kontrolowanej przez sympatyków organizacji terrorystycznej spółki, która następnie ogłasza bankructwo. Aktywa, w tym przypadku środki pieniężne, są transferowane poprzez łańcuch rachunków bankowych należących do powiązanych podmiotów, celem ich wypłaty w gotówce. 3. Korzystanie z rachunków bankowych osób fizycznych powiązanych z terrorystami (rodzina oraz inne bliskie osoby) w celu dokonania wpłat gotówkowych, a następnie przelewów transgranicznych. 4. Otwieranie rachunków bankowych na potrzeby zagranicznej osoby prawnej (zarejestrowanej w szczególności w raju podatkowym), a następnie wykorzystanie tych rachunków do przekazywania środków na rzecz podmiotów gospodarczych znajdujących się na obszarze o dużej aktywności organizacji terrorystycznych (np. Libia, Irak). 5. Otwieranie rachunków bankowych w placówkach bankowych przez osoby fizyczne na podstawie fałszywego dowodu tożsamości. Otwieranie rachunków bankowych przez Internet, infolinię bądź nawet za pomocą aplikacji mobilnej z wykorzystaniem fałszywych danych. Wykorzystanie następnie rachunku do przekazywania środków osobom powiązanym z działalnością terrorystyczną. 6. Samofinansowanie się terrorystów (zwł. "samotnych wilków") z własnych środków, zgromadzonych na rachunku bankowym (często z legalnych źródeł - zarobki, zapomogi, kredyty/pożyczki, stypendia, datki od rodziny). 7. Transfer środków przeznaczonych na cele działalności terrorystycznej z banku umiejscowionego w Azji na rachunek w instytucji kredytowej w Europie. Rachunek należy do członka lub zwolennika organizacji terrorystycznej, lub też podmiotu przez niego kontrolowanego, a transfer środków odbywa się za pośrednictwem banków-korespondentów umiejscowionych w Ameryce Płd., co utrudnia identyfikację i weryfikację danych zleceniodawcy transferu. 8. Wykorzystywanie rachunku bankowego przez podmiot, którego beneficjentem rzeczywistym jest osoba znajdująca się na międzynarodowych listach sankcyjnych bądź powiązana z organizacją terrorystyczną lub też z nią sympatyzująca. 9. Wykorzystanie rachunku bankowego przez uchodźców z Ukrainy, będących członkami bądź sympatykami jednej z organizacji panislamistycznych i fundamentalistycznych o zasięgu międzynarodowym. Organizacja ta głosi w swoim programie odbudowę kalifatu, który by objął cały świat muzułmański. Komórki tej organizacji pojawiają się w Polsce. Organizacja ta działała na Ukrainie legalnie, ale jej odłamy są zdelegalizowane w niektórych krajach europejskich. Dokonywane przez te rachunki przepływy finansowe mogą być związane z finansowaniem terroryzmu.
Poziom podatności	3

Uzasadnienie dla poziomu podatności	Otwarcie rachunku bankowego, jak i dokonywanie transakcji - również o międzynarodowym charakterze - za jego pośrednictwem jest stosunkowo łatwe. Istotny jest dostęp do rachunku za pośrednictwem elektronicznych kanałów łączności (w szczególności przez Internet), który umożliwia ukrycie danych rzeczywistych zleceniodawców transakcji - przy wykorzystywaniu tzw. słupów czy przedsiębiorstw symulujących do otwarcia rachunku. Zgodnie z danymi pochodzącymi z Raportu[10] „PRNews.pl: Rynek kont osobistych – I kw. 2022 r." - wynika, że w segmencie bankowości uniwersalnej działa już 35,6 mln ROR-ów. Najwięcej jest obsługiwanych przez takie banki, jak: PKO BP, Pekao i Santander. W porównaniu do danych z końca 2021 r. rynek kont urósł o 394 tys., a w porównaniu do danych sprzed roku o blisko 1,7 mln. Najwięcej rachunków osobistych prowadzi niezmiennie PKO BP – 8,7 mln. Na drugim miejscu jest Bank Pekao – 4,6 mln, a na trzecim Santander – 4,2 mln. Te same trzy banki odnotowały w ciągu minionego roku największy wzrost liczby rachunków. Z opublikowanych przez NBP danych wynika, że na koniec 2021 r. na rynku polskim było 43,3 mln kart płatniczych. Oznacza to, że w ostatnim kwartale 2021r. przybyło 470 tys. kart. Wartość pojedynczej transakcji wynosiła średnio 123 zł. W samym czwartym kwartale 2021 r. dokonano 2,1 mld transakcji kartami płatniczymi o łącznej wartości 254,98 mld zł. Transakcje bezgotówkowe stanowiły już ponad 93 % wszystkich transakcji. W czwartym kwartale 2021 r. liczba wypłat z bankomatów spadła o 6,8 % Wypłata wynosiła średnio 738 zł. Z kolei wartość transakcji kartami w Internecie wzrosła o 1,15 mld zł, czyli o 19 % w porównaniu do poprzedzającego kwartału. Wszystkie podmioty oferujące ww. produkty/usługi są instytucjami obowiązanymi (IO). Te podmioty stosują środki bezpieczeństwa finansowego, choć wciąż ujawniane są podczas kontroli braki w tym obszarze. W związku z trwającym konfliktem wojennym na Ukrainie szczególnym wyzwaniem związanym z prawidłowym stosowaniem środków bezpieczeństwa stanowi prawidłowa identyfikacja i weryfikacja tożsamości uchodźców z Ukrainy, zainteresowanych skorzystaniem z funkcjonujących na rynku finansowym produktów. Z uwagi na trwający konflikt zbrojny utrudnione jest pozyskanie szerszego spektrum dokumentów potwierdzających tożsamość lub wiarygodność klienta. Występują poważne problemy z identyfikacją i weryfikacją osób, które albo w ogóle nie miały żadnych dokumentów, albo miały dokumenty w rodzaju paszportu wewnętrznego pisanego cyrylicą. Właściwa transkrypcja takich dokumentów na alfabet łaciński jest niezwykle utrudniona. Poza tym istniejąca bariera językowa i kulturowa pomiędzy pracownikami instytucji obowiązanych a uchodźcami korzystającymi z rachunku bankowego utrudnia rozpoznanie nietypowych zachowań klienta, zarówno klienta pragnącego założyć np. rachunek bankowy, jak i klienta dokonującego transakcji. Bariera językowa i kulturowa w istotny sposób wpływa na prawidłowe rozpoznanie czynników zwiększonego ryzyka. Stanowi ona ten czynnik behawioralny, który utrudnia prawidłową ocenę odpowiedzi klientów-uchodźców w kwestiach problematycznych, które wymagają dodatkowych informacji czy dokumentów. Instytucje obowiązane posiadają świadomość swoich obowiązków z zakresu PPP/PFT. Efektywnie analizują transakcje, ale w instytucjach obowiązanych pracownicy realizujący zadania z zakresu PPP/PFT w dobie konfliktu zbrojnego na Ukrainie zostali z reguły obarczeni zadaniami z zakresu stosowania sankcji nałożonych na Rosję i Białoruś. Powoduje to sytuację, w której zadaniami z zakresu PPP/PFT zajmuje się faktycznie mniej osób w instytucjach obowiązanych niż przed konfliktem i do prawidłowej realizacji tych zadań PPP/PFT osób tych może być w niektórych przypadkach za mało. Występują też problemy z weryfikacją zagranicznych klientów w centralnych rejestrach beneficjentów rzeczywistych państw UE, zwłaszcza dotyczy to podmiotów o skomplikowanej strukturze kapitałowej. Organy administracji publicznej posiadają wiedzę nt. ryzyka prania pieniędzy oraz finansowania terroryzmu (PP/FT) w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że

[10] https://prnews.pl/raport-prnews-pl-rynek-kont-osobistych-i-kw-2022-465248 dostęp 25.06.2022 r.

	przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. W 2021 r. ogółem zarejestrowano w systemie GIIF 251 zawiadomień opisowych[11] (SAR) od jednostek współpracujących (JW), co stanowi wzrost w stosunku do 2020 r., w którym zarejestrowano ich 179. Od instytucji obowiązanych GIIF zarejestrował w 2021 r. wpływ 3574 SAR. Ich liczba utrzymuje się na wysokim poziomie i jest o ok. 20% wyższa niż średnia z lat 2014-2018. Istniejące przepisy prawne odpowiadają w dużej mierze zakresowi analizowanego ryzyka.
Poziom zagrożenia	4
Uzasadnienie dla poziomu zagrożenia	Finansowanie terroryzmu poprzez założone rachunki bankowe, zarówno rachunki firmowe, jak i rachunki osób fizycznych, jest jedną z najprostszych w wykorzystaniu metod. Rachunki mogą być zasilane zarówno legalnymi środkami, jak i pochodzącymi ze źródeł nielegalnych. Sposób ten ze względu na dobrze rozwinięty system bankowy jest szeroko dostępny i jego zastosowanie niewiele kosztuje. Samo dokonywanie transakcji na rachunkach bankowych nie wymaga specjalistycznej wiedzy ani umiejętności. Wykorzystanie systemu bankowego, a przede wszystkim rachunków bankowych, ze względu na możliwości dokonywania za ich pośrednictwem szybkich transakcji uznaniowych i obciążeniowych, jest łatwe, nie wymaga skomplikowanego planowania. Jeśli organizacja terrorystyczna stworzy system fikcyjnych podmiotów posiadających rachunki bankowe w kraju i za granicą, może dokonywać przelewów i płatności pomiędzy tymi podmiotami, które to transakcje z punktu widzenia uzasadnienia ekonomicznego nie będą podejrzane i bardzo trudne do zakwestionowania. W dużej ilości legalnych transakcji relatywnie łatwo jest ukryć prawdziwe przeznaczenie środków, zwłaszcza w przypadku transakcji o relatywnie niskich wartościach. GIIF dysponuje informacjami, że ten *modus operandi* może być wykorzystywany do finansowania terroryzmu. WNIOSEK: Wykorzystanie rachunku bankowego do gromadzenia i transferowania pieniędzy na rzecz terrorystów stwarza bardzo wysokie zagrożenie finansowaniem terroryzmu.

Tabela 6

Rodzaj wykorzystanych usług, produktów finansowych	Pożyczki i kredyty
Ogólny opis ryzyka	Zaciąganie pożyczek lub kredytów w instytucjach finansowych bez zamiaru spłaty powstałych zobowiązań
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	Zaciąganie przez osoby fizyczne pożyczek krótko- lub długoterminowych, pozwalających na finansowe wsparcie terrorystów, w szczególności na wyjazd do strefy konfliktu w celu walki w szeregach zagranicznych bojowników terrorystycznych.
Poziom podatności	3
Uzasadnienie dla poziomu podatności	Dostęp do kredytów i pożyczek udzielanych przez banki jest prosty. Jednakże w związku z trwającym konfliktem wojennym na Ukrainie utrudnione jest stosowanie środków bezpieczeństwa związane z prawidłową identyfikacją i weryfikacją tożsamości uchodźców z Ukrainy, zainteresowanych skorzystaniem z funkcjonujących na rynku finansowym produktów. Niekiedy problem stanowi pozyskanie szerszego spektrum dokumentów potwierdzających tożsamość lub wiarygodność takiego klienta. Tym niemniej w zawieraniu umowy pożyczki czy

[11] SPRAWOZDANIE Generalnego Inspektora Informacji Finansowej z realizacji ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu w 2021 roku, str. 43. https://www.gov.pl/web/finanse/sprawozdania-roczne-z-dzialalnosci-generalnego-inspektora-informacji-finansowej. Liczba dotyczy wszystkich zawiadomień opisowych – ML i FT.

	kredytu istnieją pewne ograniczenia związane przede wszystkim z posiadaniem przez klienta zdolności kredytowej i odpowiednich zabezpieczeń. Z ich powodów możliwość wykorzystania słupów lub przedsiębiorstw symulujących do zaciągania kredytów i pożyczek jest utrudniona. Spłaty kredytów i pożyczek można dokonywać również poprzez realizację transakcji o charakterze międzynarodowym, również przy wykorzystaniu osób lub podmiotów trzecich. Według danych Biura Informacji Kredytowej[12] - w maju 2022 r. w porównaniu do maja 2021 r. banki i SKOK-i przyznały więcej (+1,5%) tylko kredytów gotówkowych. W pozostałych rodzajach kredytów odnotowano spadki. Spadła liczba udzielonych kredytów mieszkaniowych (-43,3%), limitów na kartach kredytowych (-29,3%), a także kredytów ratalnych (-4,7%). W ujęciu wartościowym banki i SKOK-i przyznały niższą wartość we wszystkich produktach kredytowych. Najwyższy spadek wartości wystąpił w kredytach mieszkaniowych (-38,6%). Na niższą wartość przyznano limitów na kartach kredytowych (-16,3%), kredytów ratalnych (-3,9%) i gotówkowych (-0,8%). W pierwszych pięciu miesiącach 2022 r. w porównaniu do analogicznego okresu ubiegłego roku, ujemne dynamiki w obu ujęciach odnotowały karty kredytowe (-34,0% oraz -16,7%) oraz kredyty mieszkaniowe (-27,9% i -19,7%). Natomiast dodatnie dynamiki zanotowano w przypadku kredytów ratalnych (+17,4% i +2,7%), a także kredytów gotówkowych (+5,1% i +2,4%). Wszystkie podmioty oferujące ww. produkty/usługi są IO. Te podmioty stosują środki bezpieczeństwa finansowego, choć wciąż ujawniane są podczas kontroli braki w tym obszarze. Posiadają świadomość swoich obowiązków z zakresu PPP/PFT. Efektywnie analizują transakcje – najwięcej SAR, przekazywanych do GIIF, pochodzi od banków/oddziałów instytucji kredytowych/oddziałów banków zagranicznych. Instytucje obowiązane w odpowiedzi na pandemię COVID-19 musiały szybko dostosować swoje systemy sprzedażowe do wymogów w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, by utrzymać sprzedaż produktów. Wiązało się to przede wszystkim z wprowadzeniem rozwiązań technologicznych umożliwiających dystrybucję produktów w systemie sprzedaży na odległość. Występują też problemy z weryfikacją zagranicznych klientów w centralnych rejestrach beneficjentów rzeczywistych państw UE, zwłaszcza dotyczy to podmiotów o skomplikowanej strukturze kapitałowej. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej mierze zakresowi analizowanego ryzyka.
Poziom zagrożenia	3
Uzasadnienie dla poziomu zagrożenia	Zaciąganie pożyczek lub kredytów w instytucjach finansowych bez zamiaru spłaty powstałych zobowiązań może być postrzegane w Polsce jako dosyć atrakcyjna metoda sfinansowania przestępstwa o charakterze terrorystycznym. Dotyczy to zwłaszcza kredytów i pożyczek konsumpcyjnych, a zdecydowanie mniej kredytów hipotecznych. Uproszczone procedury otrzymywania takich kredytów czy pożyczek, duża gama banków i firm pożyczkowych wpływa na atrakcyjność tego *modus operandi*. Nie wymaga to od członków organizacji terrorystycznej lub osób ich wspierających specjalistycznej wiedzy, planowania czy unikalnych umiejętności. W niektórych przypadkach konieczne może jednak być sfałszowanie dokumentacji. Informacje o wykorzystaniu tego *modus operandi* do finansowania terroryzmu pochodzą przede wszystkim z zagranicy. WNIOSEK: Zaciąganie pożyczek lub kredytów w instytucjach finansowych bez zamiaru spłaty powstałych zobowiązań stanowi wysokie zagrożenie

[12] https://media.bik.pl/informacje-prasowe?offset=0 dostęp 25.06.2022 r.

	finansowaniem terroryzmu.

Tabela 7

Rodzaj wykorzystanych usług, produktów finansowych	Anonimowe karty przedpłacone – nośniki pieniądza elektronicznego wydawane przez podmioty zagraniczne – instytucje pieniądza elektronicznego oferujące swoje produkty w Polsce na podstawie paszportu europejskiego
Ogólny opis ryzyka	Korzystanie z kart prepaid w celu utrudnienia identyfikacji osób dokonujących transakcji związanych z finansowaniem terroryzmu
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Środki przeznaczone na finansowanie terroryzmu są przekazywane pomiędzy osobami fizycznymi z wykorzystaniem kart przedpłaconych zapewniających anonimowość zarówno nabywcy karty, jak i beneficjentom środków na niej zgromadzonych. 2. Sponsorowanie działalności o charakterze terrorystycznym poprzez kupno anonimowych kart przedpłaconych o międzynarodowym zasięgu (także kart do międzynarodowych połączeń telefonicznych, do gier w Internecie) i przekazywanie numeru karty osobom powiązanym z terrorystami. Karta (dokładnie jej opis i numery) jest sprzedawana przez ww. osoby, a uzyskane środki zostają wykorzystane do finansowania działalności przestępczej. 3. Środki, którymi anonimowe karty przedpłacone są zasilane przez różne osoby, są następnie transferowane na różne rachunki posiadane lub kontrolowane przez terrorystów lub wypłacane w gotówce. 4. Wykorzystanie przez terrorystów portfeli pieniądza elektronicznego do gromadzenia środków pieniężnych pod różnymi tytułami, w tym na cele charytatywne, a następnie zasilanie nimi kart płatniczych (w tym anonimowych kart przedpłaconych), z których pieniądze są pobierane w gotówce.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Dostęp do kart przedpłaconych będących nośnikiem pieniądza elektronicznego jest stosunkowo łatwy (poprzez Internet). Głównym źródłem ryzyka finansowania terroryzmu są anonimowe karty przedpłacone oferowane w Polsce, ale wydawane przez emitentów z innych krajów UE. Istnieje możliwość wydawania zgodnie z prawem pieniądza elektronicznego (zapisanego na karcie przedpłaconej lub na serwerze), bez identyfikowania i weryfikowania klienta, jakkolwiek w tym zakresie istnieją limity kwot przechowywanych na instrumencie płatniczym, a także limity kwot transakcji określone w dyrektywie 2018/843[13]. Pieniądz elektroniczny i karty przedpłacone mogą być używane do realizacji transakcji o charakterze międzynarodowym. Z uwagi na sprawowanie nadzoru nad zagranicznymi instytucjami pieniądza elektronicznego oferującymi swoje produkty i usługi w Polsce przez władze kraju macierzystego należącego do UE należy zakładać, że posiadają one i stosują się do obowiązujących procedur w zakresie przeciwdziałania praniu pieniędzy oraz finansowania terroryzmu (warto jednak pamiętać, że nie są one instytucjami obowiązanymi w myśl polskich przepisów, o ile nie działają one poprzez oddział ustanowiony w Polsce). Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia[14] i analizowania informacji, jednak w dużej mierze jest w tym zakresie uzależniony od informacji uzyskanych od zagranicznych jednostek analityki finansowej. Istnieje prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie

[13] Tj, dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/843 z dnia 30 maja 2018 r. zmieniającą dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniającą dyrektywy 2009/138/WE i 2013/36/UE (Dz. Urz. UE L 156 z 19.06.2018 r., str. 43).

[14] Zgodnie z artykułem 53 ust. 1 dyrektywy 2015/849, w przypadku gdy dana jednostka analityki finansowej otrzyma raport o transakcji podejrzanej, dotyczący innego państwa członkowskiego UE (np. Polski), niezwłocznie go przekazuje jednostce analityki finansowej tego państwa członkowskiego.

	sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	1
Uzasadnienie dla poziomu zagrożenia	Banki krajowe wydają jedynie karty przedpłacone będące rodzajem kart debetowych. Anonimowe karty przedpłacone - nośniki pieniądza elektronicznego są wydawane przez instytucje pieniądza elektronicznego z innych krajów UE i oferowane klientom w Polsce. Należy zakładać, że ryzyko finansowania terroryzmu może dotyczyć przede wszystkim tych kart, które są nabywane przez osoby fizyczne. Wymaga to od sprawców wiedzy na temat oferty zagranicznych instytucji pieniądza elektronicznego. Są informacje pochodzące głównie z zagranicy o wykorzystywaniu tego *modus operandi* do FT. WNIOSEK: Wykorzystanie anonimowych kart przedpłaconych w celu utrudnienia identyfikacji osób dokonujących transakcji związanych z finansowaniem terroryzmu jest aktualnie w Polsce na niskim poziomie zagrożenia.

Tabela 8

Rodzaj wykorzystanych usług, produktów finansowych	Transfery środków pieniężnych
Ogólny opis ryzyka	Wykorzystanie transferów do przekazywania środków do innych jurysdykcji
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Wykorzystanie transferów środków pieniężnych do przekazywania środków pod fikcyjnym tytułem (m.in. na rzecz pomocy rodzinie). Środki przekazywane są do banków ulokowanych w krajach graniczących z miejscem działalności organizacji terrorystycznych. 2. Pracownik banku, współpracujący z terrorystami, przyjmuje od nich lub ich zwolenników środki pieniężne, które następnie za pośrednictwem bezgotówkowych transferów przekazuje na wskazane przez nich rachunki bankowe, ukrywając ich źródło oraz przeznaczenie. 3. Dokonywanie przez uchodźców z Ukrainy, będących członkami bądź sympatykami jednej z organizacji panislamistycznych i fundamentalistycznych o zasięgu międzynarodowym (głoszącej w swoim programie odbudowę kalifatu, który by objął cały świat muzułmański, a która na Ukrainie działała legalnie), transferów finansowych do innych krajów, gdzie te organizacje są zdelegalizowane. Transfery finansowe z udziałem członków bądź sympatyków tej organizacji mogą być pośrednio bądź bezpośrednio związane z finansowaniem terroryzmu.
Poziom podatności	3

Uzasadnienie dla poziomu podatności	Zlecanie transferów środków pieniężnych za pośrednictwem banków jest stosunkowo łatwe. Część banków świadczy również usługi przekazów pieniężnych w imieniu zagranicznych instytucji płatniczych. Istnieje ograniczona ilość produktów ułatwiających dokonywanie anonimowych transakcji (ewentualnie jest to możliwe w przypadku dokonywania sporadycznych transakcji poniżej progu równowartości 1 tys. EUR lub w przypadku posłużenia się słupem albo przedsiębiorstwem symulującym). Transfery środków pieniężnych mają często charakter międzynarodowy. Wszystkie podmioty oferujące ww. produkty/usługi są IO. Te podmioty stosują środki bezpieczeństwa finansowego, choć wciąż ujawniane są podczas kontroli braki w tym obszarze. W związku z trwającym konfliktem wojennym na Ukrainie szczególnym wyzwaniem związanym z prawidłowym stosowaniem środków bezpieczeństwa stanowi prawidłowa identyfikacja i weryfikacja tożsamości uchodźców z Ukrainy, zainteresowanych skorzystaniem z funkcjonujących na rynku finansowym produktów. Z uwagi na trwający konflikt zbrojny utrudnione jest pozyskanie szerszego spektrum dokumentów potwierdzających tożsamość lub wiarygodność klienta. Występują poważne problemy z identyfikacją i weryfikacją osób, które albo w ogóle nie miały żadnych dokumentów, albo miały dokumenty w rodzaju paszportu wewnętrznego pisanego cyrylicą. Właściwa transkrypcja takich dokumentów na alfabet łaciński jest niezwykle utrudniona. Poza tym istniejąca bariera językowa i kulturowa pomiędzy pracownikami instytucji obowiązanych a uchodźcami korzystającymi z rachunku bankowego utrudnia rozpoznanie nietypowych zachowań klienta, zwłaszcza klienta chcącego dokonać transferu środków pieniężnych. Bariera językowa i kulturowa w istotny sposób wpływa na prawidłowe rozpoznanie czynników zwiększonego ryzyka. Stanowi ona ten czynnik behawioralny, który utrudnia prawidłową ocenę odpowiedzi klientów-uchodźców w kwestiach problematycznych, które wymagają dodatkowych informacji czy dokumentów. Instytucje obowiązane posiadają świadomość swoich obowiązków z zakresu PPP/PFT. Efektywnie analizują transakcje – ale w większości instytucji obowiązanych pracownicy realizujący zadania z zakresu PPP/PFT w dobie konfliktu zbrojnego na Ukrainie zostali z reguły obarczeni zadaniami z zakresu stosowania sankcji nałożonych na Rosję i Białoruś. Powoduje to sytuację, w której zadaniami z zakresu PPP/PFT zajmuje się faktycznie mniej osób w instytucjach obowiązanych niż przed konfliktem i do prawidłowej realizacji zadań PPP/PFT osób tych może być w niektórych przypadkach za mało. Jednakże najwięcej SAR, przekazywanych do GIIF, pochodzi od banków/oddziałów instytucji kredytowych/oddziałów banków zagranicznych. IO mają też problemy z weryfikacją zagranicznych klientów w centralnych rejestrach beneficjentów rzeczywistych państw UE, zwłaszcza dotyczy to podmiotów o skomplikowanej strukturze kapitałowej. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej mierze zakresowi analizowanego ryzyka.
Poziom zagrożenia	4

Uzasadnienie dla poziomu zagrożenia	Finansowanie terroryzmu poprzez wykorzystanie transferów do przekazywania środków finansowych do innych jurysdykcji jest jedną z najczęściej spotykanych metod. Sposób ten ze względu na dobrze rozwinięty światowy system bankowy jest szeroko dostępny i jego zastosowanie stosunkowo niewiele kosztuje. Zlecanie transferów nie wymaga wiedzy o systemie bankowym ani specjalistycznych umiejętności, jednakże realizacja tego *modus operandi* jest wtedy stosunkowo bezpieczna, gdy bank ze względu na charakter transakcji bądź miejsce transakcji nie jest zobowiązany do stosowania wzmożonych środków badania klienta. Ominięciem tego niebezpieczeństwa jest np. pozyskanie do współpracy pracownika banku. Jeśli organizacja terrorystyczna stworzy system fikcyjnych podmiotów posiadających rachunki bankowe w kraju i za granicą, może dokonywać przelewów i płatności pomiędzy tymi podmiotami, które to transakcje z punktu widzenia uzasadnienia ekonomicznego nie będą podejrzane i bardzo trudne do zakwestionowania. Wykorzystanie transferów do przekazywania środków finansowych do innych jurysdykcji w systemie bankowym jest łatwe, nie wymaga skomplikowanego planowania ani specjalistycznej wiedzy ani umiejętności. WNIOSEK: Wykorzystanie transferów do przekazywania środków finansowych do innych jurysdykcji na cele działalności terrorystycznej stwarza bardzo wysokie zagrożenie finansowaniem terroryzmu.

Pandemia COVID-19 spowodowała istotne zmiany w modelu funkcjonowaniu banków, banków spółdzielczych czy spółdzielczych kas oszczędnościowo-kredytowych. Nastąpił znaczny wzrost liczby aktywnych użytkowników korzystających z usług bankowych w elektronicznych kanałach dostępu, a także wzrost transakcji bezgotówkowych (zbliżeniowych) i płatności elektronicznych. Jednocześnie w 2022 r. w Polsce mamy do czynienia z paradoksem – wartość gotówki w obiegu rośnie pomimo tego, że jako środek płatniczy jest ona systematycznie wypierana przez inne formy płatności[15]. W kwietniu 2022 r. gotówka w obiegu stanowiła 18,7% szerokiej podaży pieniądza (M3) i 12,4% rocznego PKB. W 2009 r. płatności gotówkowe preferowało 64% Polaków, a w 2021 r. odsetek ten spadł do 21%. Jeszcze w 2013 r. 70% transakcji o wartości 11-50 zł była realizowana gotówką, obecnie jej udział spadł do 1/3.

Podatność sektora

Wszystkie podmioty oferujące produkty i usługi w sektorze bankowym są instytucjami obowiązanymi (IO). Dotyczy to zarówno banków komercyjnych, banków spółdzielczych czy spółdzielczych kas oszczędnościowo-kredytowych. Podmioty te są zobowiązane do stosowania środków bezpieczeństwa finansowego. Przeprowadzane kontrole w tym obszarze ujawniają jednak występowanie błędów i braków w tym zakresie. Wymienione w ustawie środki bezpieczeństwa finansowego obejmują przede wszystkim czynności związane z identyfikacją klienta oraz weryfikacją jego tożsamości; identyfikację beneficjenta rzeczywistego oraz podejmowanie uzasadnionych czynności w celu weryfikacji jego tożsamości oraz ustalenia struktury własności i kontroli w przypadku klienta będącego osobą prawną albo jednostką organizacyjną nieposiadającą osobowości prawnej. Ponadto podmioty sektora bankowego dokonują oceny stosunków gospodarczych klienta oraz (stosownie do sytuacji) uzyskują informacje na temat ich celu i zamierzonego charakteru. Na bieżąco też monitorują stosunki gospodarcze klienta. Podmioty sektora bankowego posiadają świadomość swoich obowiązków z zakresu PPP/PFT. Efektywnie analizują transakcje – najwięcej powiadomień o transakcjach

[15] Analiza PeKaO S.A. - https://www.wnp.pl/finanse/paradoksalna-sytuacja-gotowka-zalewa-polski-rynek,587245.html dostęp w dniu 10.12.2022 r.

podejrzanych, przekazywanych do Generalnego Inspektora Informacji Finansowej (GIIF), pochodzi właśnie od banków/oddziałów instytucji kredytowych/oddziałów banków zagranicznych. Z danych GIIF dotyczących wszczętych przez GIIF w latach 2019-2021 postępowań analitycznych wynika, że zdecydowana większość z tych postępowań dotyczyła podejrzenia prania pieniędzy lub finansowania terroryzmu w związku z wykorzystaniem do podejrzanych transakcji rachunków bankowych. W 2019 r. było to ok. 81,5% postępowań dotyczących podejrzenia prania pieniędzy lub finansowania terroryzmu w związku z wykorzystaniem do podejrzanych transakcji rachunków bankowych, w 2020 r. ok. 74,8%, a w 2021 r. ok 85,0%. Stosunkowo wysoki poziom raportowania o podejrzeniu prania pieniędzy przez pracowników sektora bankowego wynika z faktu, że w sektorze funkcjonuje wysoka świadomość narażenia na przestępstwo prania pieniędzy oraz finansowania terroryzmu oraz pracownicy tego sektora są wyszkoleni w analizie sygnałów ostrzegawczych wynikających z transakcji podejrzanych. Jak wynika z posiadanych przez GIIF informacji, instytucje sektora bankowego dysponują zaawansowanymi narzędziami i systemami informatycznymi, wspomagającymi realizację celów przeciwdziałania praniu pieniędzy oraz finansowania terroryzmu. W tych celach wykorzystywane są przez te instytucje np. systemy wspomagające proces analizy transakcji czy systemy do weryfikacji klientów pod kątem list sankcyjnych. GIIF ponadto prowadził szkolenia dla instytucji obowiązanych i jednostek współpracujących, podczas których są przekazywane teoretyczne i praktyczne wskazówki dotyczące ustalania beneficjenta rzeczywistego oraz struktury własności i kontroli klientów a także raportowania rozbieżności do organu właściwego w sprawie CRBR. Prowadzone są także szkolenia podnoszące świadomość AML/CTF w instytucjach obowiązanych. Szkolenia te organizowane są zarówno przez GIIF, jak i przez UKNF w ramach Programu CEDUR.

Należy jednak mieć na uwadze, że w związku z trwającym konfliktem wojennym na Ukrainie szczególnym wyzwaniem związanym z prawidłowym stosowaniem środków bezpieczeństwa stanowi prawidłowa identyfikacja i weryfikacja tożsamości uchodźców z Ukrainy, zainteresowanych skorzystaniem z funkcjonujących na rynku finansowym produktów. Z uwagi na trwający konflikt zbrojny, utrudnione jest pozyskanie szerszego spektrum dokumentów potwierdzających tożsamość lub wiarygodność klienta. Występują poważne problemy z identyfikacją i weryfikacją osób, które albo w ogóle nie miały żadnych dokumentów, albo miały dokumenty w rodzaju paszportu wewnętrznego pisanego cyrylicą. Właściwa transkrypcja takich dokumentów na alfabet łaciński jest niezwykle utrudniona. Poza tym istniejąca bariera językowa i kulturowa pomiędzy pracownikami instytucji obowiązanych a uchodźcami korzystającymi z rachunku bankowego utrudnia rozpoznanie nietypowych zachowań klienta, zarówno klienta pragnącego założyć np. rachunek bankowy, jak i klienta dokonującego transakcji. Bariera językowa i kulturowa w istotny sposób wpływa na prawidłowe rozpoznanie czynników zwiększonego ryzyka. Stanowi ona ten czynnik behawioralny, który utrudnia prawidłową ocenę odpowiedzi klientów-uchodźców w kwestiach problematycznych, które wymagają dodatkowych informacji czy dokumentów.

Organy administracji publicznej posiadają wiedzę nt. ryzyka prania pieniędzy oraz finansowania terroryzmu (PP/FT) w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje prawdopodobieństwo, że przypadek prania pieniędzy czy finansowania terroryzmu w zakresie analizowanych w obszarze bankowość scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Ogółem od instytucji obowiązanych GIIF otrzymał i zarejestrował w 2021 r. wpływ 3 574 SAR. Ich liczba utrzymuje się na wysokim poziomie i jest o ok. 20% wyższa niż średnia

z lat 2014-2018. Tym niemniej w instytucjach obowiązanych, w tym instytucjach sektora bankowego, pracownicy realizujący zadania z zakresu PPP/PFT w dobie konfliktu zbrojnego na Ukrainie zostali z reguły obarczeni zadaniami z zakresu stosowania sankcji nałożonych na Rosję i Białoruś. Powoduje to sytuację, w której zadaniami z zakresu PPP/PFT zajmuje się faktycznie mniej osób w instytucjach obowiązanych niż przed konfliktem i do prawidłowej realizacji tych zadań PPP/PFT osób tych może być w niektórych przypadkach za mało.

UKNF zidentyfikował także przypadki, w których, w badanych IO, nie zapewniono właściwej obsady kadrowej w komórkach AML tych instytucji – zbyt mało było pracowników w stosunku do realizowanych i dynamicznie zmieniających się obowiązków. Konsekwencją powyższego jest w szczególności bardzo wydłużony proces rozpatrywania alertów wygenerowanych przez systemy informatyczne na podstawie zaimplementowanych scenariuszy, co stanowi naruszenie obowiązków wynikających z art. 43 ust. 3 oraz 34 ust. 1 pkt 4 lit. a ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, które obligują IO do bieżącej analizy przeprowadzanych transakcji.

Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie.

Istniejące przepisy prawne odpowiadają w dużej mierze zakresowi analizowanego ryzyka.

W 2022 r. przeprowadzono w GIIF scoring ryzyka banków komercyjnych za 13 kwartałów (jako okresów sprawozdawczych) w latach 2018-2021 w zakresie występujących nieprawidłowości w bankach. Wzięto pod uwagę dane dotyczące 34 banków. Scoring obejmował badanie pod takimi kryteriami jak: nieterminowość w przekazywaniu raportów kwartalnych przez banki do GIIF na podstawie art. 76 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu; niski udział PEP-ów w ogólnej liczbie klientów; niski udział beneficjentów rzeczywistych o statusie PEP w ogólnej liczbie klientów; wysokie udział klientów niskiego ryzyka w ogólnej liczbie klientów banku; niski udział zgłoszonych przypadków / zawiadomień w ogólnej liczbie klientów; udział wybranych przypadków / zawiadomień w łącznej liczbie przypadków / zawiadomień; ilość negatywnych informacji wpływających z kanału sygnałów społecznych; ilość negatywnych informacji z Wydziałów Analitycznych GIIF wpływających do Wydziału Kontroli GIIF; ilość negatywnych informacji wpływających do GIIF od jednostek współpracujących. Siedem banków (na 34) pod względem wyżej wymienionych kryteriów zostało uznanych za instytucje, w których ryzyko wystąpienia nieprawidłowości jest wysokie. Sześć z banków zostało odpowiednio ocenionych jako takie, w których ryzyko wystąpienia nieprawidłowości było niskie, natomiast pozostałe dwadzieścia jeden banków zostały zakwalifikowanych pod względem wyżej wymienionych kryteriów jako instytucje, w których ryzyko wystąpienia nieprawidłowości było średnie.

Przeprowadzono w tym samym okresie również scoring dla spółdzielczych kas oszczędnościowo-kredytowych za okres od I kwartału 2019 do II kwartału 2021 tj. 6 okresów sprawozdawczych. Wzięto pod uwagę dane dotyczące 20 SKOK. Scoring obejmował badanie pod takimi kryteriami jak: udział klientów niskiego ryzyka w ogólnej liczbie klientów; udział PEP-ów w ogólnej liczbie klientów; udział beneficjentów rzeczywistych o statusie PEP w ogólnej liczbie klientów będących PEP-ami. Dwa SKOK-i pod względem wyżej wymienionych kryteriów zostało uznanych za instytucje, w których ryzyko wystąpienia nieprawidłowości jest wysokie. Piętnaście z ocenianych SKOK-ów zostało odpowiednio ocenionych jako takie, w

których ryzyko wystąpienia nieprawidłowości było średnie, natomiast pozostałe trzy SKOK-i zostały zakwalifikowanych pod względem wyżej wymienionych kryteriów jako instytucje, w których ryzyko wystąpienia nieprawidłowości było niskie.

Scoring za ten sam okres tj. 6 okresów sprawozdawczych przeprowadzono również dla banków spółdzielczych. Wzięto pod uwagę dane dotyczące 553 banków spółdzielczych. Scoring obejmował badanie pod takimi kryteriami jak: niski udział zgłoszonych przypadków/ zawiadomień w ogólnej liczbie klientów; wysoki udział klientów niskiego ryzyka w ogólnej liczbie klientów banku; niski udział PEP-ów w ogólnej liczbie klientów; niski udział beneficjentów rzeczywistych o statusie PEP w ogólnej liczbie klientów będących PEP-ami; udział wybranych przypadków/zawiadomień w łącznej liczbie przypadków/zawiadomień. Dwadzieścia cztery banki spółdzielcze pod względem wyżej wymienionych kryteriów zostało uznanych za instytucje, w których ryzyko wystąpienia nieprawidłowości jest wysokie. Dwieście trzynaście z ocenianych banków społdzielczych zostało odpowiednio ocenionych jako takie, w których ryzyko wystąpienia nieprawidłowości było średnie, natomiast pozostałe trzysta szesnaście banków spółdzielczych zostały zakwalifikowanych pod względem wyżej wymienionych kryteriów jako instytucje, w których ryzyko wystąpienia nieprawidłowości było niskie.

Zarówno banki komercyjne, banki spółdzielcze czy spółdzielcze kasy oszczędnościowo-kredytowe są częścią rynku finansowego, nad którym kompetencje nadzorcze wykonuje Komisja Nadzoru Finansowego. Kompetencje tego organu określone zostały w *ustawie z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym* oraz w ustawach regulujących działalność poszczególnych sektorów rynku finansowego, tj.: bankowego, ubezpieczeniowego, emerytalnego, kapitałowego, spółdzielczych kas oszczędnościowo-kredytowych i usług płatniczych. Celem nadzoru KNF[16] nad rynkiem finansowym jest zapewnienie prawidłowego funkcjonowania tego rynku, jego stabilności, bezpieczeństwa oraz przejrzystości, zaufania do rynku finansowego, a także zapewnienie ochrony interesów uczestników tego rynku również poprzez rzetelną informację dotyczącą funkcjonowania rynku. Nadzór nad rynkiem finansowym KNF realizuje pełniąc następujące funkcje: licencyjną, regulacyjną, kontrolną i dyscyplinującą. KNF wydaje bowiem zezwolenia na prowadzenie działalności przez banki, spółdzielcze kasy oszczędnościowo-kredytowe, krajowe instytucje płatnicze, zakłady ubezpieczeń i zakłady reasekuracji, otwarte fundusze emerytalne, fundusze inwestycyjne czy firmy inwestycyjne. Ustawodawca nadał KNF także szereg kompetencji w zakresie stosowania środków nadzorczych[17]. I tak np. w przypadku stwierdzenia naruszenia obowiązujących przepisów prawa KNF może nakładać kary finansowe przewidziane w przepisach prawa, a także cofnąć zezwolenie na prowadzenie działalności przez instytucję finansową. Jeśli jakaś praktyka rynkowa budzi kontrowersje, to KNF może wydać zalecenia, kierowane indywidualnie do danego podmiotu, lub rekomendacje czy wytyczne, których celem jest oddziaływanie na cały sektor rynku finansowego. KNF na bieżąco analizuje raporty przesyłane przez instytucje finansowe oraz ocenia, czy wypełniają one określone przepisami prawa wymogi kapitałowe. Do kompetencji KNF należy również prowadzenie kontroli w podmiotach nadzorowanych. W 2022 r. KNF dokonał w obszarze przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu kontroli w 5. bankach komercyjnych oraz w 5. bankach

[16] https://www.knf.gov.pl/dla_konsumenta/Ochrona_klienta_na_rynku_uslug_finansowych/KNF, dostęp w dniu 14.03.2023 r.
[17] Tamże

spółdzielczych. W wyniku czynności kontrolnych przeprowadzonych przez UKNF w tych podmiotach nadzorowanych w 2022 r. zidentyfikowano 237 nieprawidłowości. Najczęściej stwierdzane nieprawidłowości i naruszenia to: brak aktualizacji danych o klientach i ich beneficjentach rzeczywistych mających wpływ na przyznaną im wcześniej ocenę ryzyka; brak okresowej aktualizacji oceny ryzyka klienta; nieprawidłowe ustalenie lub brak ustalenia beneficjenta rzeczywistego; brak wypełnienia obowiązków związanych z bieżącą analizą transakcji oraz obowiązków związanych z analizą transakcji przeprowadzaną, jako bieżący monitoring stosunków gospodarczych klienta oraz dokumentowaniem wyników analiz transakcji; przyjęcie zbyt odległych terminów określonych na przeprowadzanie analiz transakcji i zamykanie alertów; niewystarczający zakres, jakość lub/i częstotliwość informacji zarządczej; brak odzwierciedlania w zakresach czynności pracowników zajmujących się AML/CTF wszystkich realizowanych przez nich obowiązków w powyższym zakresie; naruszenie zasady rozdzielności funkcji operacyjnych od nadzorczych w obszarze AML/CTF; określenie poziomu ryzyka związanego z ML/FT instytucji obowiązanej na zbyt niskim poziomie w odniesieniu do specyfiki podmiotu oraz ustaleń poczynionych w toku czynności kontrolnych; niezgodność regulacji wewnętrznych z obowiązującymi przepisami prawa lub brak uwzględnienia w ich treści wszystkich wymaganych ustawą zagadnień; system kontroli wewnętrznej nie obejmujący swoim zakresem kluczowych elementów procesu AML/CTF, pomimo zidentyfikowania nieprawidłowości w ramach systemu kontroli wewnętrznej, działania podejmowane celem ich wyeliminowania nie były wystarczająco skuteczne; brak realizacji zaleceń KNF lub ich częściowa realizacja. Natomiast w 2022 r. w odniesieniu do spółdzielczych kas oszczędnościowo-kredytowych, Kasa Krajowa[18] przeprowadziła w czterech Kasach kontrole w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.

Zagrożenia w sektorze

Sektor bankowy pod względem oceny zagrożenia praniem pieniędzy, ale też zagrożenia finansowania terroryzmu, jest najczęściej wykorzystywanym sektorem w związku z przestępstwami źródłowymi dla prania pieniędzy oraz finansowania terroryzmu: przestępstwami skarbowymi, handlu narkotykami, przestępstwami przeciwko mieniu oraz przeciwko obrotowi gospodarczemu, korupcji, handlu ludźmi czy oszustwami.

Zarówno pranie pieniędzy, jak i finansowanie terroryzmu poprzez produkty oferowane przez sektor bankowy (np. założone rachunki bankowe, zarówno rachunki firmowe, jak i rachunki osób fizycznych, kredyty i pożyczki, anonimowe karty przedpłacone oraz transfery środków pieniężnych), są jedną z najprostszych w wykorzystaniu metod. Z uwagi na dobrze rozwinięty w Polsce system bankowy sposób ten jest szeroko dostępny i jego zastosowanie niewiele kosztuje. Samo dokonywanie transakcji np. na rachunkach bankowych nie wymaga specjalistycznej wiedzy ani umiejętności.

Wykorzystanie systemu bankowego, a przede wszystkim rachunków bankowych, ze względu na możliwości dokonywania za ich pośrednictwem szybkich transakcji uznaniowych i obciążeniowych, jest łatwe, nie wymaga skomplikowanego planowania.

W obszarze przedmiotowego sektora należy jednak zwrócić szczególną uwagę na ryzyka dotyczące wzrostu przestępstw związanych z wyłudzeniami danych osobowych, wzrost ryzyka

[18] Dane Krajowej Spółdzielczej Kasy Oszczędnościowo-Kredytowej

wykorzystywania tzw. „słupów", zmianami w zachowaniu klientów dotyczącymi wzrostu ilości transakcji realizowanych online oraz rezygnacji z wizyt w punktach obsługi klienta. Należy także zwrócić uwagę na zwiększone wykorzystanie przelewów do prowadzenia działalności przestępczej oraz zmiany wolumenu i wartości transakcji. Oprócz tego zidentyfikowano wzrost liczby przypadków zakładania rachunków oraz udzielania pożyczek i kredytów na skradzione tożsamości (tzn. na osoby, które nigdy tych rachunków nie zakładały i nigdy tych pożyczek i kredytów nie brały).

Wśród produktów i usług szczególnie narażonych na wykorzystanie w celu popełnienia oszustw i nadużyć na rynku lub transferowania/przechowywania środków pochodzących z przestępstwa, należy zauważyć rachunki typu *collect* – oferowane przez sektor bankowy dla podmiotów pośrednictwa finansowego. Rachunki te stanowią obszar wysokiego ryzyka, ponieważ tego typu produkt utrudnia identyfikację zleceniodawców transakcji oraz jej faktycznych beneficjentów. W sektorze są jednak podsektory charakteryzujące się umiarkowanym poziomem ryzyka związanego z praniem pieniędzy i finansowaniem terroryzmu. Należy do nich korzystanie z kart prepaid w celu utrudnienia identyfikacji osób dokonujących transakcji związanych z finansowaniem terroryzmu czy sprawców prania pieniędzy.

W sektorze bankowym oprócz rachunków typu collect, oferowanych przez sektor bankowy dla podmiotów pośrednictwa finansowego obszarami i sektorami szczególnie narażonymi na ryzyko prania pieniędzy i finansowania terroryzmu są - w zakresie oferowania produktów i usług szczególnie narażonych na wykorzystanie w celu popełnienia oszustw i nadużyć na rynku lub transferowania/przechowywania środków pochodzących z przestępstwa - w szczególności usługi transferu wartości pieniądza elektronicznego/usługi przekazu pieniężnego; usługi przechowywania w skrytkach sejfowych; produkty i usługi, które z natury sprzyjają anonimowości (np. instrumenty na okaziciela), oraz instrumenty charakteryzujące się niezwykłą złożonością i strukturą bez oczywistego celu ekonomicznego. Obszarami szczególnie narażonymi na ryzyko prania pieniędzy i finansowania terroryzmu w sektorze bankowym jest ponadto działalność podmiotów świadczących usługi w zakresie tworzenia osób prawnych, które to podmioty są obsługiwane przez instytucje finansowe sektora. Ponadto narażone na ryzyko jest zawieranie stosunków gospodarczych na odległość bez fizycznej obecności klienta w instytucji obowiązanej oraz tzw. outsourcing wykonania przez instytucję obowiązaną środków bezpieczeństwa finansowego. Nieprawidłowe wykonywanie środków bezpieczeństwa finansowego może też się wiązać z wysoką fluktuacją pracowników operacyjnie zaangażowanych w wykonywanie obowiązków z zakresu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu w instytucji obowiązanej. Narażenie na ryzyko prania pieniędzy i finansowania terroryzmu w sektorze bankowym wiąże się również z nawiązywaniem stosunków gospodarczych z osobami, które faktycznie nie dysponują wartościami majątkowymi, a są jedynie wykorzystywane jako tzw. słupy przez inne osoby/podmioty do ukrycia tożsamości osób, które faktycznie dysponują tymi wartościami majątkowymi. Podobne ryzyko wiąże się z faktem nawiązywania stosunków gospodarczych z podmiotami zajmującymi się tzw. crowdfunding'iem społecznościowym. Finansowanie społecznościowe tzw. crowdfunding sprzyja ukryciu źródła pochodzenia środków i generuje ryzyko prania pieniędzy oraz finansowania terroryzmu dla instytucji obowiązanych zwłaszcza w przypadkach niewłaściwie przeprowadzonego procesu KYC i w konsekwencji niedostateczną wiedzą instytucji finansowej o obsługiwanym podmiocie. Innymi obszarami i sektorami szczególnie narażonymi na ryzyko prania pieniędzy i finansowania terroryzmu

w sektorze bankowym jest brak zidentyfikowania przez instytucję obowiązaną, czy beneficjent rzeczywisty klienta jest osobą zajmującą eksponowane stanowiska polityczne. Ewentualnie brak zidentyfikowania przez instytucję obowiązaną beneficjentów rzeczywistych klienta będących obywatelami lub mieszkających na terenie państwa uznanego za kraj wysokiego ryzyka prania pieniędzy oraz finansowania terroryzmu, a także brak weryfikacji beneficjentów rzeczywistych klienta na listach sankcyjnych.

W kontekście zagrożeń związanych z potencjalnym finansowaniem terroryzmu, konflikt na Ukrainie generuje dla Polski zagrożenie związane z przenikaniem przez wschodnią granicę i możliwą działalnością na terenie kraju członków jednej z organizacji panislamistycznych i fundamentalistycznych o zasięgu międzynarodowym. Organizacja ta głosi w swoim programie odbudowę kalifatu, który by objął cały świat muzułmański. Komórki tej organizacji pojawiają się w Polsce, zaś propaganda kierowana jest do konwertytów, migrantów z obszaru MENA oraz Czeczenów. Jest wysoce prawdopodobne, że wśród uchodźców z Ukrainy lub Rosji znajdować się mogą także zwolennicy tej organizacji, zwłaszcza, że przed zajęciem Krymu przez Rosję organizacja ta działała tam w sposób całkowicie legalny. W kilku krajach zachodnich organizacja ta działa legalnie, natomiast w Wielkiej Brytanii czy Niemczech została zdelegalizowana. Przepływy finansowe z udziałem członków bądź sympatyków tej organizacji mogą być związane z finansowaniem terroryzmu. Należy mieć też na uwadze, że finansowanie terroryzmu dokonuje się zarówno za pomocą środków pochodzących z legalnych, jak i nielegalnych źródeł. Zwykle środki finansowe deponowane na rachunku bankowym, gdy pochodzą z udokumentowanych, legalnych źródeł, nie budzą żadnych podejrzeń w chwili otwierania rachunku bankowego. Zwłaszcza, gdy wpłacane na rachunki środki finansowe należą do osób niezaangażowanych bezpośrednio w działania terrorystyczne. Osoby te to np. rodzina i znajomi osób podejrzewanych o działalność terrorystyczną. Same środki są natomiast często wypłacane z rachunków bankowych poprzez bankomaty, bez udziału pracowników sektora bankowego. Wypłacać je mogą w ten sposób inne osoby, niż posiadacze rachunków bankowych.

Uśredniony poziom zagrożenia sektora bankowego – ML – 2,75 i FT – 3,0

Uśredniony poziom podatności sektora bankowego – ML – 2,75 i FT – 2,75

Oszacowany poziom prawdopodobieństwa dla sektora – ML – 2,75 i FT - 2,85

Poziom ryzyka jest ostatecznie określany przez kombinację zagrożenia i podatności. Macierz ryzyka określająca ten poziom ryzyka opiera się na wadze 40% (zagrożenie) + 60% (podatność) – przy założeniu, że komponent podatności ma większą zdolność określania poziomu ryzyka. Zakłada się, że poziom podatności może zwiększyć atrakcyjność, a tym samym zamiary przestępców/terrorystów, aby użyć danego modus operandi – wpływając w ten sposób ostatecznie na poziom zagrożenia. Poziom ryzyka sektora, z uwzględniem oszacowanego prawdopobieństwa i konsekwencji (współczynnik 2,5 dla PP i 1,5 dla FT), jest ustalany zgodnie z metodyką krajowej oceny ryzyka – aneks nr 1.

Ryzyko FT sektora bankowego – 2.31	
1 – 1,5	Niskie

1,6 – 2,5	Średnie
2,6 – 3,5	Wysokie
3,6 – 4	Bardzo wysokie
Ryzyko ML sektora bankowego – 2,65	
1 – 1,5	Niskie
1,6 – 2,5	Średnie
2,6 – 3,5	Wysokie
3,6 – 4	Bardzo wysokie

WNIOSEK 1: Poziom ryzyka wykorzystania sektora bankowego do finansowania terroryzmu w Polsce znajduje się na poziomie średnim.

WNIOSEK 2: Poziom ryzyka wykorzystania sektora bankowego do prania pieniędzy w Polsce znajduje się na wysokim.

Mitygacja zidentyfikowanych ryzyk:

W celu ograniczenia prawdopodobieństwa wykorzystania sektora bankowego do prania pieniędzy lub finansowania terroryzmu, zasadne jest podjęcie odpowiednich działań. Stosowanie zaproponowanych działań mitygujących powinno następować z uwzględnieniem rozpoznanego przez danę instytucję obowiązaną ryzyka.

Podmioty sektora bankowego powinny kontynuować działania związane z odpowiednią oceną stosunków gospodarczych klienta oraz uzyskiwaniem informacji na temat ich celu i zamierzonego charakteru, a także powinny utrzymywać bieżący monitoring stosunków gospodarczych.

Ze względu na wagę sektora bankowego w systemie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, podmioty z tego sektora powinny przywiązywać szczególną wagę do identyfikacji czynników wskazujących na wyższe ryzyko prania pieniędzy oraz finansowania terroryzmu, w szczególności wymienionych w art. 43 ust. 2 ustawyz dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. W przypadku produktów i usług oferowanych klientom, w tym tych ułatwiających zachowanie anonimowości, takich jak usługi collect, banki powinny z jednej strony zweryfikować cel gospodarczy wykorzystania tej usługi przez klienta, a z drugiej strony powinny w ramach bieżącego monitorowania transakcji weryfikować trendy wskazujące na wykorzystanie usługi collect niezgodnie z przeznaczeniem, lub jej nadużywanie.

W sektorze bankowym powinny być podejmowane działania gwarantujące utrzymanie wysokiej świadomości narażenia na przestępstwo prania pieniędzy oraz finansowania terroryzmu, jak również utrzymujące poziom wyszkolenia pracowników tego sektora w analizie sygnałów ostrzegawczych wynikających z transakcji podejrzanych.

Zalecane jest dalsze rozwijanie przez instytucje sektora bankowego zaawansowanych narzędzi i systemów informatycznych, wspomagających realizację celów przeciwdziałania praniu pieniędzy oraz finansowania terroryzmu.

Kontynuowane powinny być szkolenia dla instytucji obowiązanych i jednostek współpracujących, podczas których będą przekazywane teoretyczne i praktyczne wskazówki dotyczące ustalania beneficjenta rzeczywistego oraz struktury własności i kontroli klientów a także raportowania rozbieżności do organu właściwego w sprawie CRBR. Zalecane jest uczestnictwo przedstawicieli instytucji obowiązanych w szkoleniach podnoszących świadomość AML/CTF, organizowanych zarówno przez GIIF, jak i przez UKNF w ramach Programu CEDUR. Z uwagi na identyfikowane ryzyka związane z wykorzystywaniem fałszywych dokumentów, personel instytucji obowiązanych zajmujący się identyfikacją i weryfikacją tożsamości klienta, powinien być na bieżąco szkolony w zakresie typowania dokumentów fałszywych, również w zakresie dokumentów innych niż Polskie.

Instytucje obowiązane powinny zwracać uwagę na stosunki gospodarcze ich klientów z podmiotami zagranicznymi, szczególnie gdy działalność oraz transakcje podmiotów zagranicznych nie wykazują związku z terytorium Polski. Instytucje obowiązane prowadzące rachunki bankowe lub płatnicze powinny zwracać szczególną uwagę na transfery środków do jurysdykcji charakteryzujących się wyższym ryzykiem prania pieniędzy oraz finansowania terroryzmu. W szczególności należy zwracać uwagę na cykliczne transfery środków z enigmatycznym tytułem przelewu, czy też powtarzające się transfery środków pieniężnych do danej jurysdykcji, przy braku uzasadnienia ekonomicznego dla tego typu transferów. Instytucje obowiązane powinny położyć szczególny nacisk na ustalenie danych dotyczących źródła pochodzenia transferowanych wartości majątkowych, jak również dokumentów wskazujących na uzasadnienie przeprowadzenia danej transakcji.

Instytucje obowiązane powinny przykładać szczególną wagę do czynników geograficznych mogących wskazywać na wyższe ryzyko prania pieniędzy czy też finansowania terroryzmu, takich jak niestabilna sytuacja polityczna czy konflikt zbrojny, czego najdobitniejszym przykładem w ostatnich latach jest wojna prowadzona przez Rosję przeciwko Ukrainie. Z uwagi na wysokie ryzyko transferowania środków pochodzących z nielegalnego handlu, przemytu ludzi, handlu bronią, czy też działań zmierzających do omijania sankcji gospodarczych, szczególnie istotne jest analizowanie przez instytucje obowiązane nie tylko danych dotyczących samych stron transakcji, ale również beneficjentów rzeczywistych, czy też faktycznych celów przeprowadzania danych transakcji.

2. Obszar – usługi płatnicze (oferowane przez inne podmioty niż banki)

Opis sektora – zawarty jest w podrozdziałach KOR 2.1.2 - „Sektory rynku finansowego" oraz w podrozdziale 7.2.1 - „*Podatność rynku finansowego*", a także w rozdziale 6.3. „Najczęstsze metody stosowane w celu finansowania terroryzmu".

Scenariusze wystąpienia ryzyka (tj. możliwe przykłady wystąpienia ryzyka) zarówno w przypadku prania pieniędzy, jak i finansowania terroryzmu - dotyczyły wykorzystania do prania pieniędzy i finansowania terroryzmu produktów i usług finansowych w postaci przekazów pieniężnych, internetowych usług płatniczych oraz systemu transferów typu Hawala. Szczegółowy opis znajduje się w scenariuszach do konkretnego obszaru ryzyka poniżej.

Pranie pieniędzy

Tabela 9

Rodzaj wykorzystanych usług, produktów finansowych	Przekazy pieniężne
Ogólny opis ryzyka	Wykorzystanie dostawców usług z zakresu transferu środków pieniężnych do transferowania pieniędzy pochodzących z nielegalnych źródeł
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Wykorzystanie przekazów pieniężnych do transferowania środków pochodzących z nielegalnych źródeł poza granice kraju w celu ich wykorzystania w innej jurysdykcji. 2. Wykorzystanie przekazów pieniężnych do otrzymania środków pochodzących z nielegalnych, zagranicznych źródeł, aby następnie je wypłacić w gotówce. 3. Wykorzystanie bezprzewodowego terminala POS (*ang. point of sale*) do księgowania środków pochodzących z nielegalnych źródeł na rachunek bankowy przy wykorzystaniu kart płatniczych wydanych przez zagraniczne instytucje bankowe. Aktywność ta, może wskazywać na kradzież kart lub tzw. skimming. W związku z wykorzystaniem zagranicznych kart, utrudnione jest ustalenie źródła pochodzenia środków. Metoda ta, używana jest w celu uwiarygodnienia, iż otrzymane środki pochodzą z legalnie prowadzonej działalności gospodarczej, tj. ze sprzedaży towarów / usług. W scenariuszu tym, transakcje kartowe mogą zostać wykorzystane za pomocą transakcji zbliżeniowych z telefonu komórkowego przy użyciu systemu płatności mobilnych Google Pay oraz Apple Pay.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Usługi przekazów pieniężnych są stosunkowo łatwo dostępne. Istnieje ograniczona możliwość ukrycia danych identyfikacyjnych zleceniodawców i beneficjentów przekazów pieniężnych w przypadku dokonywania sporadycznych transakcji poniżej progu równowartości 1 tys. EUR lub w przypadku posłużenia się słupem albo przedsiębiorstwem symulującym. Transfery środków pieniężnych mają często charakter międzynarodowy. Prawie wszystkie podmioty oferujące te usługi są IO za wyjątkiem instytucji płatniczych z innych krajów UE świadczących usługi płatnicze na terytorium Polski za pośrednictwem agentów. W marcu 2021 r. Visa ogłosiła[19] uruchomienie platformy płatności push w czasie rzeczywistym z usługą Visa Direct Payouts, co umożliwia klientom i partnerom Visa (modele P2P, B2B, B2C) na całym świecie przesyłanie za pośrednictwem jednego połączenia z VisaNet płatności na kwalifikujące się karty do wypłat krajowych oraz kwalifikujące się karty lub konta do płatności transgranicznych. Elastyczne interfejsy API Visa Direct Payouts zmniejszają złożoność często związaną z zarządzaniem i wysyłaniem pieniędzy przez wiele sieci i pośredników na całym

[19] Raport NBP Ocena funkcjonowania polskiego systemu płatniczego w I półroczu 2021 r. str. 110.

	świecie. Platforma Visa Direct jest adaptowana do płatności w systemach podmiotów współpracujących (dotychczas m.in. TransferWise, Western Union, Remitly), dzięki czemu znacząco wzrosła liczba dokonywanych za jej pośrednictwem transferów w czasie rzeczywistym. Podobnie brytyjski FinTech TransferGo wdrożył rozwiązanie oparte na platformie Visa Direct i zaoferował swoim klientom realizowanie transgranicznych przelewów pieniężnych w czasie zbliżonym do rzeczywistego na ich karty płatnicze bez konieczności korzystania z bankowości internetowej albo wprowadzania IBAN. Te podmioty posiadają pewną świadomość swoich obowiązków z zakresu PPP/PFT, choć wciąż ujawniane są braki w ich wypełnianiu. Przekazują one relatywnie niewiele SAR-ów. Występują też problemy z weryfikacją zagranicznych klientów w centralnych rejestrach beneficjentów rzeczywistych państw UE, zwłaszcza dotyczy to podmiotów o skomplikowanej strukturze kapitałowej. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek prania pieniędzy w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	4
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie dostawców usług z zakresu transferu środków pieniężnych oraz bezprzewodowych terminali POS (*ang. point of sale*) do transferowania pieniędzy pochodzących z nielegalnych źródeł poza granice kraju bądź w celu otrzymania nielegalnych środków jest jedną z często używanych metod prania pieniędzy. Jest to sposób szeroko dostępny, jego zastosowanie niewiele kosztuje i jest postrzegany przez sprawców jako atrakcyjny. Do realizacji tego typu transferu pieniądza nie jest potrzebne posiadanie przez płatnika rachunku płatniczego. W celu ukrycia beneficjenta rzeczywistego częstokroć wykorzystywane są słupy. Wykorzystanie dostawców usług z zakresu transferu środków pieniężnych oraz bezprzewodowych terminali POS (ang. point of sale) do transferowania pieniędzy pochodzących z nielegalnych źródeł poza granice kraju nie wymaga specjalistycznej wiedzy. GIIF otrzymywał informacje o wykorzystaniu tej metody do prania pieniędzy. WNIOSEK: Wykorzystanie dostawców usług z zakresu transferu środków pieniężnych do transferowania pieniędzy - w formie przekazu pieniężnego - pochodzących z nielegalnych źródeł poza granice kraju bądź w celu otrzymania nielegalnych środków stwarza bardzo wysokie zagrożenie prania pieniędzy.

Tabela 10

Rodzaj wykorzystanych usług, produktów finansowych	Internetowe usługi płatnicze
Ogólny opis ryzyka	Korzystanie z internetowych usług płatniczych przez sprawców w celu transferowania środków pochodzących z nielegalnych źródeł

Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Wykorzystanie internetowych usług płatniczych przez sprawców celem wytransferowania środków pochodzących z nielegalnych źródeł z rachunku bankowego, na którym zostały zgromadzone, a następnie ich "przerzucanie" pomiędzy różnymi kontami otwartymi u dostawców usług płatniczych, aby w końcu je przekazać na rachunek bankowy, należący do osoby fizycznej lub podmiotu gospodarczego, kontrolowanego przez sprawców. 2. Agent instytucji płatniczej (względnie pracownik instytucji płatniczej), współpracujący ze sprawcami, przyjmuje od nich środki pieniężne pochodzące z nielegalnych źródeł, które następnie za pośrednictwem bezgotówkowych transferów przekazuje na wskazane przez nich rachunki bankowe, ukrywając ich źródło oraz przeznaczenie.
Poziom podatności	3
Uzasadnienie dla poziomu podatności	Internetowe usługi przekazów są stosunkowo łatwo dostępne - wystarczy mieć dostęp do Internetu. Istnieją możliwości ukrycia danych identyfikacyjnych osoby korzystającego z tego typu usług płatniczych (w związku z COVID-19 wiele instytucji umożliwiło realizację transakcji do określonej kwoty bez weryfikacji danych identyfikacyjnych, a sama weryfikacja danych identyfikacyjnych jest uproszczona - opiera się na przekazanym przez klienta skanie paszportu lub prawa jazdy, zdjęciu z kamery internetowej i danych geolokalizacyjnych klienta). Transfery środków pieniężnych mają często charakter międzynarodowy. Na polskim rynku coraz większego znaczenia nabierają innowacyjne instrumenty i usługi płatnicze, takie jak Google Pay, Apple Pay, Revolut i inne. Tylko część podmiotów oferujących te usługi jest IO. Nie są nimi instytucje płatnicze świadczące usługi płatnicze za pomocą internetowych platform, zarejestrowane w innych krajach (poza oddziałami unijnych instytucji płatniczych, oddziałami unijnych i zagranicznych instytucji pieniądza elektronicznego). IO z obszaru usług płatniczych posiadają pewną świadomość swoich obowiązków z zakresu PPP/PFT, choć wciąż ujawniane są braki w ich wypełnianiu. Przekazują one relatywnie niewiele SAR-ów. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek prania pieniędzy w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	2
Uzasadnienie dla poziomu zagrożenia	Wykorzystywanie internetowych usług płatniczych, które umożliwiają płatności *online* i transfer pieniędzy przez Internet, będących elektroniczną alternatywą dla tradycyjnych metod, takich jak czeki i polecenia zapłaty, jest metodą prania pieniędzy, z którą GIIF zetknął się, ale wydaje się, że nie jest to metoda postrzegana przez potencjalnych „praczy" jako atrakcyjna. Zbyt duży wolumen obrotów szybko może zwrócić uwagę. Istnieją też limity łącznej wartości transakcji realizowanych w określonym czasie. Mogą występować też trudności w kontaktach z operatorem w razie nieprawidłowości. Powoduje to pewne kłopoty w zastosowaniu tej metody, zwłaszcza że wymaga ona odpowiedniego planowania i wiedzy specjalistycznej. GIIF posiada informacje o wykorzystywaniu tej metody do prania pieniędzy. WNIOSEK: Wykorzystywanie internetowych usług płatniczych stwarza średnie zagrożenie prania pieniędzy.

Tabela 11

Rodzaj wykorzystanych usług, produktów finansowych	Systemy transferów typu Hawala
Ogólny opis ryzyka	Wykorzystanie sieci Hawala lub innych nieformalnych systemów transferu do przekazywania środków pochodzących z nielegalnych źródeł
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Wykorzystanie podmiotów oferujących nielegalnie usługi płatnicze do transferu środków pochodzących z przestępczej działalności. M.in. osoba oferująca takie usługi wykorzystuje rachunki bankowe, na które wpłaca pieniądze pochodzące od swoich klientów. Środki są transferowane następnie na rachunki podmiotów prowadzących legalne usługi płatnicze. 2. Transferowanie środków pochodzących z zysków organizacji przestępczych utworzonych przez przestępców pochodzących z tego samego regionu świata poza granice kraju. 3. Środki przekazane w procesie prania pieniędzy podlegają wymieszaniu z innymi przekazami pieniężnymi w ramach sieci Hawala w celu zatarcia śladu po dokonanych transakcjach.
Poziom podatności	4
Uzasadnienie dla poziomu podatności	Usługi systemów typu Hawala znacznie ułatwiają dokonywanie szybkich i anonimowych transakcji, o międzynarodowym charakterze. Z uwagi na fakt, że świadczą je podmioty pozostające poza kontrolą państwa - brak jest danych na temat ilości i wartości transakcji realizowanych w ramach tego systemu w Polsce. Podmioty oferujące te usługi nie są IO. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF nie ma możliwości gromadzenia i analizowania informacji od tego typu podmiotów. Istnieje prawdopodobieństwo, że przypadek prania pieniędzy w zakresie analizowanego ryzyka nie zostanie wykryty. Wiedza organów ścigania o operacjach typu Hawala pochodzi przede wszystkim z wiedzy operacyjnej oraz od innych służb zagranicznych. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	1
Uzasadnienie dla poziomu zagrożenia	System typu Hawala jest rodzajem nieformalnego systemu bankowego. Wykorzystywany jest m.in. w handlu międzynarodowym, często do transferowania pieniędzy na duże odległości. Ważnym jego elementem jest możliwość zachowania pełnej anonimowości oraz wykorzystania kilku pośredników przy zlecaniu przekazu. Osoba wpłacająca gotówkę nie jest proszona o żaden dokument tożsamości i z reguły jest nieznana lub słabo znana danemu pośrednikowi. Podobnie wypłacający, który może odebrać przesłane środki finansowe podając jedynie ustalone hasło. W ten sposób podmiot oferujący usługi w systemie typu Hawala z reguły nie wie, od kogo, za co i komu transferuje środki pieniężne. Najważniejsze jest zaufanie pomiędzy pośrednikami, którzy najczęściej stanowią grono członków jednej rodziny, przyjaciół lub osoby polecone i działają w kilku lub kilkunastu krajach. Ważne jest również to, że wpłacający i wypłacający pieniądze nie muszą wcale posiadać rachunku płatniczego w danym kraju (często, z uwagi na restrykcyjne, lokalne przepisy bankowe, nie mogą tego konta otworzyć w tym kraju). Nie jest znany rozmiar (wolumen) płatności/obrotów realizowanych poprzez tego typu nieformalne systemy. Zastosowanie tego *modus operandi* wymaga wiedzy na temat osób oferujących tego typu usługi. W Polsce nie ma licznych mniejszości etnicznych, w których systemy typu Hawala są rozpowszechnione. WNIOSEK: Wykorzystanie nieformalnego systemu bankowego Hawala do transferowania środków pochodzących z nielegalnych źródeł stwarza niskie zagrożenie dla prania pieniędzy.

Finansowanie terroryzmu

Tabela 12

Rodzaj wykorzystanych usług, produktów finansowych	Przekazy pieniężne
Ogólny opis ryzyka	Wykorzystanie dostawców usług z zakresu transferu środków pieniężnych do przekazywania wartości majątkowych przeznaczonych na finansowanie terroryzmu
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Wykorzystanie przez osoby powiązane z terrorystami możliwości stosowania przez dostawców usług z zakresu transferu środków pieniężnych uproszczonych środków bezpieczeństwa finansowego przy niskich kwotach transakcji. Umożliwia to transfer środków w sposób utrudniający identyfikację zleceniodawcy i beneficjenta. Wpłata środków pieniężnych zostanie dokonana w Polsce a wypłata w krajach charakteryzujących się dużą aktywnością organizacji terrorystycznych. 2. Wykorzystanie przekazów pieniężnych do finansowego wsparcia zagranicznych bojowników terrorystycznych przebywających albo podróżujących do strefy konfliktu. 3. Korzystanie przez osoby finansujące terroryzm z usług dostawców działających na terenie Polski, lecz nie przekazujących informacji o transakcjach podejrzanych do polskiej jednostki analityki finansowej.
Poziom podatności	3
Uzasadnienie dla poziomu podatności	Usługi przekazów pieniężnych są stosunkowo łatwo dostępne. Istnieje ograniczona możliwość ukrycia danych identyfikacyjnych zleceniodawców i beneficjentów przekazów pieniężnych w przypadku dokonywania sporadycznych transakcji poniżej progu równowartości 1 tys. EUR lub w przypadku posłużenia się słupem albo przedsiębiorstwem symulującym. Transfery środków pieniężnych mają często charakter międzynarodowy. Prawie wszystkie podmioty oferujące te usługi są IO za wyjątkiem instytucji płatniczych z innych krajów UE świadczących usługi płatnicze na terytorium Polski za pośrednictwem agentów. W marcu 2021 r. Visa ogłosiła[20] uruchomienie platformy płatności push w czasie rzeczywistym z usługą Visa Direct Payouts, co umożliwia klientom i partnerom Visa (modele P2P, B2B, B2C) na całym świecie przesyłanie za pośrednictwem jednego połączenia z VisaNet płatności na kwalifikujące się karty do wypłat krajowych oraz kwalifikujące się karty lub konta do płatności transgranicznych. Elastyczne interfejsy API Visa Direct Payouts zmniejszają złożoność często związaną z zarządzaniem i wysyłaniem pieniędzy przez wiele sieci i pośredników na całym świecie. Platforma Visa Direct jest adaptowana do płatności w systemach podmiotów współpracujących (dotychczas m.in. TransferWise, Western Union, Remitly), dzięki czemu znacząco wzrosła liczba dokonywanych za jej pośrednictwem transferów w czasie rzeczywistym. Podobnie brytyjski FinTech TransferGo wdrożył rozwiązanie oparte na platformie Visa Direct i zaoferował swoim klientom realizowanie transgranicznych przelewów pieniężnych w czasie zbliżonym do rzeczywistego na ich karty płatnicze, bez konieczności korzystania z bankowości internetowej albo wprowadzania IBAN. Te podmioty posiadają pewną świadomość swoich obowiązków z zakresu PPP/PFT, choć wciąż ujawniane są braki w ich wypełnianiu. Przekazują one relatywnie niewiele SAR-ów. Występują też problemy z weryfikacją zagranicznych klientów w centralnych rejestrach beneficjentów rzeczywistych państw UE, zwłaszcza dotyczy to podmiotów o skomplikowanej strukturze kapitałowej. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa

[20] Raport NBP Ocena funkcjonowania polskiego systemu płatniczego w I półroczu 2021 r. str. 110.

	nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	4
Uzasadnienie dla poziomu zagrożenia	Przy transakcjach niskokwotowych dostawcy usług transferu środków pieniężnych mogą stosować uproszczone środki bezpieczeństwa finansowego. Przekazywane mogą być środki pochodzące z zupełnie legalnych źródeł. Aktualnie działalność terrorystyczna jest niskonakładowa (przykładowo w 2021 r. w zakończonych atakach terrorystycznych w Europie wykorzystano jedynie uzbrojenie w postaci broni ostrzowej [noży], pojazdów [w celu staranowania] oraz niskokosztowych improwizowanych urządzeń wybuchowych). Zwłaszcza w wypadku pojedynczych zamachowców lub małych grup terrorystycznych występuje zjawisko samofinansowania działalności terrorystycznej. Tym niemniej otrzymanie jednego bądź kilku niskokwotowych przekazów pieniężnych jest jedną z często używanych, znanych metod finansowania terroryzmu. Jest to sposób szeroko dostępny, jego zastosowanie niewiele kosztuje i jest postrzegany przez sprawców jako atrakcyjny. Do realizacji tego typu transferu pieniądza nie jest potrzebne posiadanie przez płatnika rachunku płatniczego. W celu ukrycia beneficjenta rzeczywistego częstokroć wykorzystywane są słupy, podmioty współpracujące bądź rodzina. Wykorzystanie dostawców usług z zakresu transferu środków pieniężnych do przesyłania pieniędzy pochodzących z legalnych bądź nielegalnych źródeł wymaga minimalnej specjalistycznej wiedzy o systemie transferu środków, jest relatywnie niezbyt drogie pod kątem opłat i stosunkowo bezpieczne. WNIOSEK: Powyższe informacje oraz fakt przebywania w Polsce osób z państw i regionów podwyższonego ryzyka, a także potencjalna możliwość przenikania przez wschodnią granicę i możliwą działalność na terenie kraju członków organizacji panislamistycznej i fundamentalistycznej o zasięgu międzynarodowym, głoszącej w swoim programie odbudowę kalifatu, który by objął cały świat muzułmański, zdelegalizowanej w niektórych krajach UE powoduje, że wykorzystanie schematu z dostawcami usług z zakresu transferu środków pieniężnych do transferowania pieniędzy – w formie przekazu pieniężnego – przeznaczonych na cele finansowania terroryzmu stwarza bardzo wysokie zagrożenie finansowaniem terroryzmu.

Tabela 13

Rodzaj wykorzystanych usług, produktów finansowych	Internetowe usługi płatnicze
Ogólny opis ryzyka	Korzystanie z internetowych usług płatniczych przez podmioty uczestniczące w procesie finansowania terroryzmu, w szczególności przez potencjalnych zagranicznych bojowników terrorystycznych

Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Wykorzystanie internetowych usług płatniczych przez zagranicznych bojowników terrorystycznych do dokonywania zakupów w sklepach internetowych ekwipunku niezbędnego do przebywania w strefie konfliktu. 2. Korzystanie z omawianych usług przez osoby wpłacające środki na rzecz organizacji charytatywnych, uczestniczących w procesie finansowania terroryzmu. 3. Transferowanie środków pomiędzy poszczególnymi osobami zaangażowanymi w działalność terrorystyczną. 4. Wykorzystanie bezgotówkowych transferów środków pieniężnych (poniżej progu, od którego wymagana jest identyfikacja klienta) do przekazywania środków pod fikcyjnym tytułem (m.in. na rzecz pomocy rodzinie). Środki przekazywane są do agencji instytucji płatniczych ulokowanych w krajach graniczących z miejscem działalności organizacji terrorystycznych. 5. Agent instytucji płatniczej (względnie pracownik instytucji płatniczej), współpracujący z terrorystami, przyjmuje od nich lub ich zwolenników środki pieniężne, które następnie za pośrednictwem bezgotówkowych transferów przekazuje na wskazane przez nich rachunki bankowe, ukrywając ich źródło oraz przeznaczenie.
Poziom podatności	3
Uzasadnienie dla poziomu podatności	Internetowe usługi przekazów są stosunkowo łatwo dostępne - wystarczy mieć dostęp do Internetu. Istnieją możliwości ukrycia danych identyfikacyjnych osoby korzystającego z tego typu usług płatniczych (w związku z COVID-19 wiele instytucji umożliwiło realizację transakcji do określonej kwoty bez weryfikacji danych identyfikacyjnych, a sama weryfikacja danych identyfikacyjnych jest uproszczona - opiera się na przekazanym przez klienta skanie paszportu lub prawa jazdy, zdjęciu z kamery internetowej i danych geolokalizacyjnych klienta). Transfery środków pieniężnych mają często charakter międzynarodowy. Na polskim rynku coraz większego znaczenia nabierają innowacyjne instrumenty i usługi płatnicze, takie jak Google Pay, Apple Pay, Revolut i inne. Tylko część podmiotów oferujących te usługi jest IO. Nie są nimi instytucje płatnicze świadczące usługi płatnicze za pomocą internetowych platform, zarejestrowane w innych krajach. IO z obszaru usług płatniczych posiadają pewną świadomość swoich obowiązków z zakresu PPP/PFT, choć wciąż ujawniane są braki w ich wypełnianiu. Przekazują one relatywnie niewiele SAR-ów. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	4
Uzasadnienie dla poziomu zagrożenia	Wykorzystywanie internetowych usług płatniczych, które umożliwiają płatności online i transfer pieniędzy przez Internet, będących elektroniczną alternatywą dla tradycyjnych papierowych metod, takich jak czeki i polecenia zapłaty, jest w miarę atrakcyjną metodą finansowania terroryzmu. Przedsięwzięcia terrorystyczne należą do względnie tanich inwestycji, w stosunku do wywołanych strat oraz wzbudzonej paniki. Aktualnie w Polsce przebywają osoby z państw i regionów podwyższonego ryzyka, a także potencjalnie mogą przebywać uchodźcy z Ukrainy, będący członkami bądź sympatykami organizacji panislamistycznej i fundamentalistycznej o zasięgu międzynarodowym, głoszącej w swoim programie odbudowę kalifatu, który by objął cały świat muzułmański (zdelegalizowanej w niektórych krajach UE), a która na Ukrainie działała legalnie. Dla tych osób oferowane usługi płatnicze umożliwiające przedsiębiorcom i konsumentom posiadającym adres e-mail wysyłanie oraz odbieranie płatności przez Internet są atrakcyjne. Ze względu na względnie niskie kwotowo przepływy pieniężne mogą one nie zostać odnotowane jako podejrzane, a ponadto są łatwe do zastosowania, choć wymagają planowania i wiedzy. WNIOSEK: Wykorzystywanie internetowych usług płatniczych stwarza bardzo

	wysokie zagrożenie finansowaniem terroryzmu.

Tabela 14

Rodzaj wykorzystanych usług, produktów finansowych	Systemy transferów typu Hawala
Ogólny opis ryzyka	Wykorzystanie sieci Hawala lub innych nieformalnych systemów transferu wartości majątkowych do finansowania terroryzmu
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Wpłata środków pieniężnych w kraju X, charakteryzującym się wysokim zagrożeniem terrorystycznym, połączona z wypłatą na terenie Polski w celu sfinansowania działalności o charakterze terrorystycznym. Wykorzystanie nieformalnej sieci transferu środków o charakterze przestępczym w celu uniemożliwienia wykrycia przepływu środków. 2. Środki przekazane na finansowanie terroryzmu podlegają wymieszaniu z innymi przekazami pieniężnymi w ramach sieci Hawala w celu zatarcia śladu po dokonanych transakcjach. 3. Wykorzystanie podmiotów oferujących nielegalnie usługi płatnicze do transferu gotówki na rzecz terrorystów. M.in. osoba oferująca takie usługi wykorzystuje rachunki bankowe, na które wpłaca pieniądze pochodzące od swoich klientów. Środki są transferowane następnie na rachunki podmiotów prowadzących legalne usługi płatnicze. 4. Zaufane podmioty w kraju o stosunkowo niskim zagrożeniu terrorystycznym otrzymują przekazy pieniężne o stosunkowo niewielkiej, jednorazowej wartości. Środki przekazują rodziny bojowników, walczących np. w ramach Państwa Islamskiego. Otrzymane kwoty są przekazywane w ramach sieci Hawala do krajów graniczących ze strefą konfliktu na cele terrorystyczne bądź na powrót dla Foreign Terrorist Fighters. W ramach systemów typu Hawala stosowane jest m.in. złoto do clearingu rozrachunków. Jest ono łatwe do upłynnienia, zwłaszcza w niektórych krajach azjatyckich i afrykańskich, gdzie są rozbudowane rynki obrotu tym metalem.
Poziom podatności	4
Uzasadnienie dla poziomu podatności	Usługi systemów typu Hawala znacznie ułatwiają dokonywanie szybkich i anonimowych transakcji, o międzynarodowym charakterze. Z uwagi na fakt, że świadczą je podmioty pozostające poza kontrolą państwa - brak jest danych na temat ilości i wartości transakcji realizowanych w ramach tego systemu w Polsce. Podmioty oferujące te usługi nie są IO. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF nie ma możliwości gromadzenia i analizowania informacji od tego typu podmiotów. Istnieje prawdopodobieństwo, że przypadek FT w zakresie analizowanego ryzyka nie zostanie wykryty. Wiedza organów ścigania o operacjach typu Hawala pochodzi przede wszystkim z wiedzy operacyjnej oraz od innych służb zagranicznych. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	3

Uzasadnienie dla poziomu zagrożenia	System transferów typu Hawala jest rodzajem nieformalnego systemu bankowego. Wykorzystywana jest w handlu międzynarodowym, często do transferowania środków na duże odległości. Ważnym elementem tego systemu nieformalnej bankowości jest możliwość zachowania pełnej anonimowości oraz wykorzystania kilku pośredników przy zlecaniu przekazu. Osoba wpłacająca gotówkę nie jest proszona o żaden dokument tożsamości i z reguły jest nieznana lub słabo znana danemu pośrednikowi. Podobnie wypłacający, który może odebrać przesłane środki finansowe podając jedynie ustalone hasło. W ten sposób podmiot oferujący usługi w zakresie systemu typu Hawala z reguły nie wie, od kogo, za co, i komu dokonuje transakcji. Najważniejsze jest zaufanie pomiędzy pośrednikami, którzy najczęściej stanowią grono członków jednej rodziny, przyjaciół lub osoby polecone i działają w kilku lub kilkunastu krajach. Ważne jest również to, że wpłacający i wypłacający pieniądze nie muszą wcale posiadać rachunku płatniczego w danym kraju (często, z uwagi na restrykcyjne, lokalne przepisy bankowe, nie mogą tego konta otworzyć w tym kraju). Nie jest znany rozmiar (wolumen) płatności poprzez ten nieformalny system. W Polsce nie mamy dużych liczebnie mniejszości etnicznych, w których system typu Hawala jest rozpowszechniony (jakkolwiek zauważono coraz bardziej rosnącą liczbę cudzoziemców z państw podwyższonego ryzyka, przebywających w RP). Jednak należy też wziąć pod uwagę obecność w Polsce dużej liczby uchodźców z Ukrainy, która dla pojedynczych bojowników, którzy operowali wcześniej w Syrii i Iraku w różnych grupach powiązanych z Państwem Islamskim oraz bojowników z Emiratu Kaukaskiego była i jest krajem, gdzie mogli uzyskać potrzebne im dokumenty, a następnie przez Polskę przedostać się do Europy Zachodniej. W dobie konfliktu wojennego na Ukrainie taka migracja bojowników jest potencjalnie ułatwiona. Polskie służby odnotowały już w pracy operacyjnej przypadki wykorzystania tej metody do transferu środków przeznaczonych na działalność terrorystyczną. WNIOSEK: Poziom zagrożenia z użyciem nieformalnego systemu bankowego Hawala do transferowania wartości majątkowych na cele działalności terrorystycznej stwarza wysokie zagrożenie finansowaniem terroryzmu.

Podstawę regulacji europejskiego rynku usług płatniczych stanowi[21] Dyrektywa 2007/64/WE Parlamentu Europejskiego i Rady z dnia 13 listopada 2007 r. w sprawie usług płatniczych w ramach rynku wewnętrznego zmieniająca dyrektywy 97/7/WE, 2002/65/WE, 2005/60/WE i 2006/48/WE i uchylająca dyrektywę 97/5/WE (PSD). Celem tej dyrektywy było przede wszystkim otwarcie rynku finansowego na nowe podmioty, tak aby umożliwić podmiotom innym niż banki świadczenie usług płatniczych wymienionych w załączniku do tej dyrektywy, poprzez objęcie tych podmiotów nadzorem ostrożnościowym oraz zapewnienie ochrony użytkownikom korzystającym z usług tych podmiotów. Przed uchwaleniem PSD działalność w zakresie usług płatniczych mogła być prowadzona na zasadzie swobody działalności gospodarczej. Jednakże mając na uwadze ryzyka jej towarzyszące, PSD wprowadziła wymóg uzyskania zezwolenia na świadczenia usług przez instytucje płatnicze oraz możliwość – pod pewnymi warunkami – prowadzenia w ograniczonym zakresie działalności w zakresie usług płatniczych bez konieczności uzyskania zezwolenia, a jedynie na podstawie wpisu do rejestru prowadzonego przez właściwy organ nadzoru (w Polsce – Komisję Nadzoru Finansowego) oraz ramy prawne dotyczące świadczenia usług płatniczych przez ich dostawców.

Do polskiego porządku prawnego przepisy PSD wdrożone zostały *ustawą z dnia 19 sierpnia 2011 r. o usługach płatniczych*. Przepisy tej ustawy wprowadziły zasadę, że usługi płatnicze mogą być wykonywane jedynie przez dostawców usług płatniczych, czyli oprócz banków,

[21]Źródło:https://www.knf.gov.pl/dla_rynku/procesy_licencyjne/platniczy/informacje_ogolne/zakres_uslug_platniczych dostęp: dnia 12.12 2022 r.

także m.in. przez instytucje płatnicze, instytucje pieniądza elektronicznego, biura usług płatniczych. Oznacza to, że świadczenie usług płatniczych, jeśli nie jest wykonywane przez żaden z podmiotów uprawnionych (np. banki na podstawie odpowiednich postanowień statutu), wymaga uzyskania zezwolenia Komisji Nadzoru Finansowego na prowadzenie działalności w charakterze krajowej instytucji płatniczej, małej instytucji płatniczej lub wpisu do rejestru usług płatniczych jako biuro usług płatniczych.

Brak jest definicji usług płatniczych, a jedynie określony jest zamknięty katalog określonych rodzajów działalności, którą należy traktować jako usługi płatnicze. Przez usługi płatnicze rozumie się działalność polegającą na[22]:

1) przyjmowaniu wpłat gotówki i dokonywaniu wypłat gotówki z rachunku płatniczego oraz wszelkie działania niezbędne do prowadzenia rachunku;
2) wykonywaniu transakcji płatniczych, w tym transferu środków pieniężnych na rachunek płatniczy u dostawcy użytkownika lub u innego dostawcy:
    a) przez wykonywanie usług polecenia zapłaty, w tym jednorazowych poleceń zapłaty,
    b) przy użyciu karty płatniczej lub podobnego instrumentu płatniczego,
    c) przez wykonywanie usług polecenia przelewu , w tym stałych zleceń;
3) wykonywaniu transakcji płatniczych wymienionych w punkcie 2 powyżej, w ciężar środków pieniężnych udostępnionych użytkownikowi z tytułu kredytu, a w przypadku instytucji płatniczej lub instytucji pieniądza elektronicznego - kredytu, o którym mowa w art. 74 ust. 3 *ustawy o usługach płatniczych* lub art. 132j ust. 3 UUP;
4) wydawaniu instrumentów płatniczych;
5) umożliwianiu wykonania transakcji płatniczych, zainicjowanych przez akceptanta lub za jego pośrednictwem, instrumentem płatniczym płatnika, w szczególności na obsłudze autoryzacji, przesyłaniu do wydawcy karty płatniczej lub systemów płatności zleceń płatniczych płatnika lub akceptanta, mających na celu przekazanie akceptantowi należnych mu środków, z wyłączeniem czynności polegających na jej rozliczaniu i rozrachunku w ramach systemu płatności w rozumieniu ustawy o ostateczności rozrachunku (acquiring);
6) świadczeniu usługi przekazu pieniężnego;
7) wykonywaniu transakcji płatniczych, w przypadku których zgoda płatnika na wykonanie transakcji udzielana jest przy użyciu urządzenia telekomunikacyjnego, cyfrowego lub informatycznego, a płatność przekazywana jest dostawcy usług telekomunikacyjnych, cyfrowych lub informatycznych, działającemu jedynie jako pośrednik pomiędzy użytkownikiem zlecającym transakcję płatniczą a odbiorcą.

KNF prowadzi rejestr o nazwie System ERUP 2 KNF[23], do którego wpisywane są krajowe instytucje płatnicze, małe instytucje płatnicze, biura usług płatniczych, spółdzielcze kasy oszczędnościowo-kredytowe i Krajowa Spółdzielcza Kasa Oszczędnościowo-Kredytowa, krajowe instytucje pieniądza elektronicznego oraz oddziały zagranicznych instytucji pieniądza elektronicznego. Jest on jawny i dostępny dla osób trzecich przez stronę internetową KNF.

[22] Tamże
[23]https://e-rup.knf.gov.pl/index.html

System Hawala opiera się natomiast na sieci pośredników zwanych hawaladars lub bankami Hawala, działającymi zazwyczaj nieoficjalnie, pod przykryciem innej działalności gospodarczej. Pośrednik Hawala prowadzi de facto podziemny bank, udzielając pożyczek, przyjmując wpłaty i realizując przelewy na całym globie, praktycznie bez użycia oficjalnego systemu bankowego, używając jednorazowych haseł. Najważniejszą cechą systemu Hawala jest szybkość dokonywanych transferów, anonimowość, możliwość przekazania praktycznie dowolnej kwoty, brak jakiejkolwiek formalności czy dokumentów oraz pozostawanie całkowicie niewidocznym dla oficjalnego systemu bankowego. Istotne są również opłacalność, niezawodność i uniknięcie opodatkowania. Transakcje Hawala dokonywane są niezwłocznie po przyjęciu gotówki u pośrednika i podaniu hasła. Pośrednik przyjmując gotówkę od wpłacającego, zleca natychmiast poprzez faks, pocztę elektroniczną, rozmowę telefoniczną, czat, wpis na portalu społecznościowym, ogłoszenie w Internecie, lub w inny nie budzący jakichkolwiek podejrzeń sposób, wypłatę środków uprawnionej osobie w innym państwie. Całość transakcji oparta jest na zaufaniu pomiędzy pośrednikami. Ważnym elementem systemu nieformalnej bankowości jest możliwość zachowania pełnej anonimowości, zarówno wpłacającego, jak i wypłacającego, oraz wykorzystania kilku pośredników przy zlecaniu przekazu. W ten sposób operator systemu Hawala z reguły nie wie, od kogo, za co, i komu dokonuje transakcji.

Podatność sektora

Wszystkie podmioty będące dostawcami usług płatniczych oferujące usługi przekazów pieniężnych (za wyjątkiem instytucji płatniczych z innych krajów UE świadczących usługi płatnicze na terytorium Polski za pośrednictwem agentów) są instytucjami obowiązanymi (IO). Podmioty te stosują środki bezpieczeństwa finansowego, określone w ustawie, choć wciąż ujawniane są podczas kontroli braki w tym obszarze. Wymienione w ustawie środki bezpieczeństwa finansowego obejmują przede wszystkim czynności związane z identyfikacją klienta oraz weryfikacją jego tożsamości; identyfikację beneficjenta rzeczywistego oraz podejmowanie uzasadnionych czynności w celu weryfikacji jego tożsamości oraz ustalenia struktury własności i kontroli w przypadku klienta będącego osobą prawną albo jednostką organizacyjną nieposiadającą osobowości prawnej. Ponadto podmioty świadczące usługi płatnicze powinny dokonywać oceny stosunków gospodarczych klienta oraz (stosownie do sytuacji) uzyskiwać informacje na temat ich celu i zamierzonego charakteru. Na bieżąco też powinny monitorować stosunki gospodarcze swoich klientów. Jednakże, jak wynika z posiadanych informacji, działalność małych instytucji płatniczych oraz biur usług płatniczych wiąże się z trudnościami z rzeczywistym monitorowaniem transakcji swoich klientów. Podmioty sektora instytucji płatniczych posiadają świadomość swoich obowiązków z zakresu PPP/PFT. W zakresie pozabankowych transferów pieniężnych w latach 2019-2021 GIIF otrzymał i zrealizował 28 powiadomień o transakcjach podejrzanych. W 2019 r. było to ok. 2,3% wszystkich postępowań dotyczących podejrzenia prania pieniędzy lub finansowania terroryzmu w związku z wykorzystaniem do podejrzanych transakcji pozabankowych transferów pieniężnych, w 2020 r. ok. 0,9%, a w 2021 r. ok 1,5%.

Trzeba zauważyć, że rozwój sektora usług płatniczych jest niezwykle dynamiczny, są wprowadzane innowacyjne technologie i nowe, coraz bardziej złożone usługi płatnicze, znacznie wyprzedzające możliwości techniczne niektórych schematów i systemów płatności. W związku z powyższym występują na rynku usług płatniczych istotne problemy z należytym wypełnianiem obowiązków przewidzianych przez Rozporządzenie 2015/847 dotyczące transferów środków pieniężnych przechodzących przez wielu dostawców usług płatniczych

i piętrowe struktury obsługi transferu. W szczególności dotyczy to transferów realizowanych w łańcuchu płatności przez bankowych i niebankowych dostawców usług płatniczych. W tego typu sytuacjach, w trakcie realizacji transferu, bardzo często dochodzi do zatarcia lub zniekształcenia w łańcuchu płatności danych faktycznych płatników jak i odbiorców, a w niektórych przypadkach dane te nie są w ogóle zapewniane przez dostawcę usług płatniczych płatnika. Biorąc powyższe pod uwagę połączone nadzory, tj.: Europejski Urząd Nadzoru Bankowego - EBA, Europejski Urząd Nadzoru Giełd i Papierów Wartościowych - ESMA i Europejski Urząd Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych – EIOPA wydały, na mocy art. 25 Rozporządzenia 2015/847, wspólne wytyczne dotyczące środków, które dostawcy usług płatniczych powinni podjąć w celu wykrycia brakujących lub niekompletnych informacji o płatniku lub odbiorcy oraz procedur, które powinni wprowadzić w celu zarządzania transferem środków pieniężnych, w przypadku którego brakuje wymaganych informacji. Jak zauważa UKNF - brak wypełniania wymogów Rozporządzenia 2015/847 wpływa na bezpieczeństwo systemu płatniczego i generuje dodatkowe ryzyko wykorzystania tego systemu do działalności przestępczej, w tym prania pieniędzy i finansowania terroryzmu. Ma także wpływ na możliwość realizacji szczególnych środków ograniczających wobec osób i podmiotów, o których mowa w art. 118 ust. 1 *ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.*

Jak wynika z posiadanych przez GIIF informacji, instytucje sektora usług płatniczych - dostawcy usług płatniczych powinni (zgodnie z rekomendacjami UKNF) analizować dane dotyczące transakcji oraz poleceń zapłaty i posiadać narzędzia do oceny dzienników zdarzeń. Z uwagi na koszty posiadania zaawansowanych, dedykowanych narzędzi informatycznych, nie wszystkie instytucje sektora usług płatniczych dysponują takimi zaawansowanymi, automatycznymi narzędziami i systemami informatycznymi, wspomagającymi realizację celów przeciwdziałania praniu pieniędzy oraz finansowania terroryzmu.

W celu podnoszenia świadomości AML/CTF w instytucjach obowiązanych – w tym w sektorze instytucji płatniczych, GIIF prowadził szkolenia dla instytucji obowiązanych i jednostek współpracujących, podczas których były przekazywane teoretyczne i praktyczne wskazówki dotyczące ustalania beneficjenta rzeczywistego oraz struktury własności i kontroli klientów a także raportowania rozbieżności do organu właściwego w sprawie CRBR. Ponadto prowadzone były także szkolenia w innych aspektach AML/CTF, organizowane zarówno przez GIIF, jak i przez UKNF w ramach Programu CEDUR.

Z uwagi na trwający konflikt zbrojny na Ukrainie utrudnione jest też pozyskanie szerszego spektrum dokumentów potwierdzających tożsamość lub wiarygodność klienta. Występują poważne problemy z identyfikacją i weryfikacją osób. Występująca bariera językowa i kulturowa w istotny sposób wpływa na prawidłowe rozpoznanie czynników zwiększonego ryzyka. Stanowi ona ten czynnik behawioralny, który utrudnia prawidłową ocenę odpowiedzi klientów-uchodźców w kwestiach problematycznych, które wymagają dodatkowych informacji czy dokumentów. Biorąc pod uwagę rosnącą aktywność gospodarczą podmiotów świadczących usługi płatnicze na terytorium Polski, zwraca uwagę niewielka ilość zawiadomień zgłaszanych przez te podmioty do GIIF. Ponadto w stosunku do działalności w Polsce zagranicznych instytucji płatniczych, dla których rachunki prowadzone są przez krajowe banki – zachodzi ryzyko nieposiadania przez krajowe banki dostatecznej ilości informacji o podmiotach zagranicznych, które obsługują. Występują również problemy z weryfikacją zagranicznych klientów w centralnych rejestrach beneficjentów rzeczywistych

państw UE, zwłaszcza dotyczy to podmiotów o skomplikowanej strukturze kapitałowej. Oprócz tego działalność instytucji płatniczych zarówno jako podmiotów zaangażowanych w pranie pieniędzy, jak i wykorzystywanych do prania pieniędzy przez ich klientów, polega na działalności tych instytucji płatniczych w zakresie otwierania dla podmiotów zagranicznych licznych rachunków płatniczych. Związane jest to z nasileniem zjawiska zakładania rachunków na podstawie fikcyjnych dokumentów, służących głównie do prania pieniędzy pochodzących z przestępstw potocznie nazywanych „fraudami". Tworzone są też instytucje płatnicze jedynie w celu realizacji transferów środków przestępczego pochodzenia.

Internetowe usługi przekazów są stosunkowo łatwo dostępne - wystarczy mieć dostęp do Internetu. Istnieją możliwości ukrycia danych identyfikacyjnych osoby korzystającego z tego typu usług płatniczych (w związku z COVID-19 wiele instytucji umożliwiło realizację transakcji do określonej kwoty bez weryfikacji danych identyfikacyjnych, a sama weryfikacja danych identyfikacyjnych jest uproszczona - opiera się na przekazanym przez klienta skanie paszportu lub prawa jazdy, zdjęciu z kamery internetowej i danych geolokalizacyjnych klienta). Transfery środków pieniężnych mają często charakter międzynarodowy. Na polskim rynku coraz większego znaczenia nabierają innowacyjne instrumenty i usługi płatnicze, takie jak Google Pay, Apple Pay, Revolut i inne. Tylko część z podmiotów oferujących internetowe usługi przekazów jest IO. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek ML czy FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców.

Od strony legislacyjnej w zakresie usługi przekazów pieniężnych należy zauważyć, że w Polsce jako w państwie członkowskim UE stosuje się wprost rozporządzenie UE 2015/847 w sprawie informacji towarzyszących przekazom pieniężnym. Oznacza to, że dostawcy usług płatniczych (jako instytucje obowiązane) wykonują swoje usługi tylko wtedy, gdy przekazom pieniężnym towarzyszą pełne informacje o płatniku (inicjatorze przekazu), w tym jego nazwa, numer rachunku płatniczego, adres, numer urzędowego dokumentu osobistego, numer identyfikacyjny klienta lub data oraz miejsce urodzenia. Muszą oni też mieć pewność, że przekazowi pieniężnemu towarzyszą informacje o odbiorcy (beneficjencie), w szczególności nazwa odbiorcy oraz jego numer rachunku płatniczego lub, jeżeli nie jest on dokonywany z/lub na rachunek płatniczy, unikalny identyfikator transakcji. Same informacje o płatniku i odbiorcy płatności są przechowywane przez dostawców usług płatniczych przez okres pięciu lat (z możliwością przedłużenia). Ponadto *ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* określa w art. 148 kary administracyjne dla instytucji obowiązanych, które nie wypełniają obowiązków zapewnienia, aby przekazom pieniężnym towarzyszyły informacje o płatniku lub odbiorcy lub wdrożenia skutecznych procedur wykrywania braku informacji o płatniku lub odbiorcy. Dostawcy usług płatniczych muszą również wdrożyć skuteczne procedury, w tym, w stosownych przypadkach, monitorowanie ex-post lub w czasie rzeczywistym, w celu wykrycia braku informacji o płatniku lub odbiorcy. U każdego dostawcy usług płatniczych muszą być określone skuteczne procedury, oparte na analizie ryzyka, umożliwiające stwierdzenie, czy wykonać, odrzucić lub wstrzymać transfer środków pieniężnych, w przypadku którego brakuje wymaganych informacji o płatniku oraz odbiorcy, oraz podjęcie stosownych dalszych kroków.

Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie.

Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.

Natomiast usługi systemów typu Hawala są świadczone przez podmioty pozostające poza kontrolą państwa. Z tego powodu brak jest danych na temat ilości i wartości transakcji realizowanych w ramach tego systemu w Polsce. Podmioty oferujące te usługi nie są IO. Z uwagi na brak uprawnień operacyjnych oraz brak raportowania przez podmioty o transakcjach typu Hawala GIIF nie ma możliwości gromadzenia i analizowania informacji od podmiotów przeprowadzających tego typu transakcje. Istnieje prawdopodobieństwo, że przypadek ML czy FT w zakresie analizowanego ryzyka nie zostanie wykryty. Wiedza organów ścigania o operacjach typu Hawala pochodzi przede wszystkim z wiedzy operacyjnej oraz od innych służb zagranicznych. W usługach typu Hawala mamy do czynienia z dużą ilością transakcji o złożonym i transgranicznym charakterze, których nie dotyczy nadzór AML/CTF w sektorze, ukierunkowany zgodnie z podejściem opartym na analizie ryzyka. Niemożliwe jest ustalenie ścieżki audytu finansowego ani monitorowanie transakcji.

Zagrożenia w sektorze

Sektor usług płatniczych (oferowanych przez inne podmioty niż banki) pod względem oceny zagrożenia praniem pieniędzy, ale też zagrożenia finansowania terroryzmu, jest często wykorzystywanym sektorem w związku z przestępstwami źródłowymi dla prania pieniędzy oraz finansowania terroryzmu: przestępstwami skarbowymi, handlu narkotykami, przestępstwami przeciwko mieniu oraz przeciwko obrotowi gospodarczemu, korupcji, handlu ludźmi czy oszustwami.

Zarówno pranie pieniędzy, jak i finansowanie terroryzmu poprzez produkty oferowane przez sektor usług płatniczych (oferowanych przez inne podmioty niż banki) w postaci np. przekazów pieniężnych czy internetowych przekazów pieniężnych, są jedną z najprostszych w wykorzystaniu metod. Dzieje się tak, ponieważ są możliwości stosowania przez dostawców usług z zakresu transferu środków pieniężnych uproszczonych środków bezpieczeństwa finansowego przy niskich kwotach transakcji. Ma to istotne znaczenie zwłaszcza w wypadku potencjalnych transakcji finansowania terroryzmu. Z uwagi na dobrze rozwinięty w Polsce system usług płatniczych sposób ten jest szeroko dostępny i jego zastosowanie niewiele kosztuje. Nie wymaga też specjalistycznej wiedzy ani umiejętności. Szczególnie wysokim ryzykiem ML i FT charakteryzują się tzw. konstrukcje kaskadowe, gdzie instytucje płatnicze obsługują inne instytucje płatnicze. Ustalenie faktycznego zleceniodawcy i beneficjenta transakcji jest utrudnione lub niemożliwe. Szczególną uwagę w takich sytuacjach należy zwracać na instytucje płatnicze, które:

- zarejestrowane są w Polsce, ale należą do obcokrajowców;
- zagraniczne, które poza posiadaniem rachunku/rachunków w Polsce wydają się nie mieć z Polską żadnych innych związków;
- które są powiązane osobowo z innymi instytucjami płatniczymi (chodzi o przypadki, gdy dana osoba zakłada kolejne instytucje płatnicze – z reguły BUP);
- świadczące usługi, do których nie są uprawnione lub przekraczające progi obrotów dla danej kategorii instytucji.

Ponadto ze względu na względnie niskie kwotowo przepływy pieniężne mogą one nie zostać w systemie odnotowane jako podejrzane, a ponadto są łatwe do zastosowania, choć wymagają planowania i wiedzy.

W przypadku systemu Hawala ważnym elementem tego systemu nieformalnej bankowości jest możliwość zachowania pełnej anonimowości oraz wykorzystania kilku pośredników przy zlecaniu przekazu. Osoba wpłacająca gotówkę nie jest proszona o żaden dokument tożsamości i z reguły jest nieznana lub słabo znana danemu pośrednikowi. Podobnie wypłacający, który może odebrać przesłane środki finansowe podając jedynie ustalone hasło. Co istotne, to polskie organy ścigania odnotowały już w pracy operacyjnej przypadki wykorzystania systemu Hawala jako metody do transferu środków przeznaczonych zarówno do prania pieniędzy, jak i potencjalnie na działalność terrorystyczną.

W kontekście zagrożeń związanych z potencjalnym finansowaniem terroryzmu konflikt na Ukrainie generuje dla Polski zagrożenie związane z przenikaniem przez wschodnią granicę i możliwą działalnością na terenie kraju członków jednej z organizacji panislamistycznych i fundamentalistycznych o zasięgu międzynarodowym. Organizacja ta głosi w swoim programie odbudowę kalifatu, który by objął cały świat muzułmański. Komórki tej organizacji pojawiają się w Polsce, zaś propaganda kierowana jest do konwertytów, migrantów z obszaru MENA oraz Czeczenów. Jest wysoce prawdopodobne, że wśród uchodźców z Ukrainy lub Rosji znajdować się mogą także zwolennicy tej organizacji, zwłaszcza, że przed zajęciem Krymu przez Rosję organizacja ta działała tam w sposób całkowicie legalny. W kilku krajach zachodnich organizacja ta działa legalnie, natomiast w Wielkiej Brytanii czy Niemczech została zdelegalizowana. Przepływy finansowe z udziałem członków bądź sympatyków tej organizacji mogą być związane z finansowaniem terroryzmu.

Uśredniony poziom zagrożenia sektora usług płatniczych – ML – 2,33 i FT – 3,67

Uśredniony poziom podatności sektora usług płatniczych – ML – 3,0 i FT – 3,33

Oszacowany poziom prawdopodobieństwa dla sektora – ML – 2,73 i FT - 3,47

Poziom ryzyka jest ostatecznie określany przez kombinację zagrożenia i podatności. Macierz ryzyka określająca ten poziom ryzyka opiera się na wadze 40% (zagrożenie) + 60% (podatność) – przy założeniu, że komponent podatności ma większą zdolność określania poziomu ryzyka. Zakłada się, że poziom podatności może zwiększyć atrakcyjność, a tym samym zamiary przestępców/terrorystów, aby użyć danego modus operandi – wpływając w ten sposób ostatecznie na poziom zagrożenia. Poziom ryzyka sektora, z uwzględniem prawdopobieństwa i konsekwencji (współczynnik 2,5 dla PP i 1,5 dla FT), jest ustalany zgodnie z metodyką krajowej oceny ryzyka – aneks nr 1.

Ryzyko FT sektora usług płatniczych –2,68	
1 – 1,5	Niskie
1,6 – 2,5	Średnie
2,6 – 3,5	Wysokie

3,6 – 4	Bardzo wysokie
Ryzyko ML sektora usług płatniczych – 2,64	
1 – 1,5	Niskie
1,6 – 2,5	Średnie
2,6 – 3,5	Wysokie
3,6 – 4	Bardzo wysokie

WNIOSEK 1: Poziom ryzyka wykorzystania sektora usług płatniczych (oferowanych przez inne podmioty niż banki) do finansowania terroryzmu w Polsce znajduje się na poziomie wysokim.

WNIOSEK 2: Poziom ryzyka wykorzystania sektora usług płatniczych (oferowanych przez inne podmioty niż banki) do prania pieniędzy w Polsce znajduje się na poziomie wysokim.

Mitygacja zidentyfikowanych ryzyk:

W celu ograniczenia prawdopodobieństwa wykorzystania sektora usług płatniczych do prania pieniędzy lub finansowania terroryzmu, zasadne jest podjęcie odpowiednich działań. Stosowanie zaproponowanych działań mitygujących powinno następować z uwzględnieniem rozpoznanego przez danę instytucję obowiązaną ryzyka.

Podmioty sektora usług płatniczych powinny kontynuować działania związane z odpowiednią oceną stosunków gospodarczych klienta oraz uzyskiwaniem informacji na temat ich celu i zamierzonego charakteru, a także powinny wzmocnić bieżący monitoring stosunków gospodarczych.

W sektorze usług płatniczych powinny być podejmowane działania wzmacniające poziom świadomości narażenia na przestępstwo prania pieniędzy oraz finansowania terroryzmu, jak również podnoszące poziom wyszkolenia pracowników tego sektora w analizie sygnałów ostrzegawczych wynikających z transakcji podejrzanych.

Zalecane jest dalsze rozwijanie przez instytucje sektora usług płatniczych zaawansowanych narzędzi i systemów informatycznych, wspomagających realizację celów przeciwdziałania praniu pieniędzy oraz finansowania terroryzmu oraz wdrażanie takich rozwiązań przez podmioty dotychczas z nich niekorzystające.

Kontynuowane powinny być szkolenia dla instytucji obowiązanych z sektora usług płatniczych, podczas których będą przekazywane teoretyczne i praktyczne wskazówki dotyczące ustalania beneficjenta rzeczywistego oraz struktury własności i kontroli klientów a także raportowania rozbieżności do organu właściwego w sprawie CRBR. Zalecane jest uczestnictwo przedstawicieli instytucji obowiązanych w szkoleniach podnoszących świadomość AML/CTF, organizowanych zarówno przez GIIF, jak i przez UKNF w ramach Programu CEDUR.

Instytucje Obowiązane prowadzące rachunki płatnicze powinny zwracać szczególną uwagę na transfery środków do jurysdykcji charakteryzujących się wyższym ryzykiem prania pieniędzy

oraz finansowania terroryzmu. W szczególności należy zwracać uwagę na cykliczne transfery środków z enigmatycznym tytułem przelewu, czy też powtarzające się transfery środków pieniężnych do danej jurysdykcji, przy braku uzasadnienia ekonomicznego dla tego typu transferów. Instytucje obowiązane powinny położyć szczególny nacisk na ustalenie danych dotyczących źródła pochodzenia transferowanych wartości majątkowych, jak również dokumentów wskazujących na uzasadnienie przeprowadzenia danej transakcji.

Instytucje obowiązane powinny przykładać szczególną wagę do czynników geograficznych mogących wskazywać na wyższe ryzyko prania pieniędzy czy też finansowania terroryzmu, takich jak niestabilna sytuacja polityczna czy konflikt zbrojny, czego najdobitniejszym przykładem w ostatnich latach jest wojna prowadzona przez Rosję przeciwko Ukrainie. Z uwagi na wysokie ryzyko transferowania środków pochodzących z nielegalnego handlu, przemytu ludzi, handlu bronią, czy też działań zmierzających do omijania sankcji gospodarczych, szczególnie istotne jest analizowanie przez instytucje obowiązane nie tylko danych dotyczących samych stron transakcji, ale również beneficjentów rzeczywistych, czy też faktycznych celów przeprowadzania danych transakcji.

Instytucje obowiązane powinny zwracać szczególną uwagę na podstawę przeprowadzenia danej transakcji, w szczególności w celu potwierdzenia, że transakcje są zgodne z wiedzą instytucji obowiązanej o kliencie.

W przypadku korzystania przez klienta instytucji obowiązanej z rozwiązań umożliwiających płatności przez terminale płatnicze czy też z aplikacji służących realizowaniu płatności, czynnikiem branym pod uwagę przez instytucję obowiązaną powinny być okoliczności wskazujące na nieproporcjonalnie dużą wartość transakcji w odniesieniu do profilu działalności gospodarczej klienta, czy też w odniesieniu do dotychczas zgromadzonych informacji o kliencie.

Czynnikiem ograniczającym ryzyko podmiotów z sektora usług płatniczych pozostaje obowiązek rejestracji podmiotu we właściwym rejestrze, a także działania nadzorcze Komisji Nadzoru Finansowego.

3. Obszar – ubezpieczenia

Opis sektora – zawarty jest w rozdziale 2.1.2. KOR „Sektory rynku finansowego" oraz w rozdziale 6.3. „Najczęstsze metody stosowane w celu finansowania terroryzmu".

Scenariusze wystąpienia ryzyka (tj. możliwe przykłady wystąpienia ryzyka) zarówno w przypadku prania pieniędzy, jak i finansowania terroryzmu - dotyczyły wykorzystania do prania pieniędzy i finansowania terroryzmu produktów i usług finansowych w postaci polisy ubezpieczenia na życie, a w przypadku finansowania terroryzmu także polisy ubezpieczenia komunikacyjnego. Ich opis znajduje się poniżej.

Pranie pieniędzy

Tabela 15

Rodzaj wykorzystanych usług, produktów finansowych	Ubezpieczenia na życie
Ogólny opis ryzyka	Wykorzystanie możliwości oferowanych przez ubezpieczenia na życie powiązane z funduszem inwestycyjnym
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Środki pochodzące z nielegalnych źródeł są lokowane przez przestępców w ramach wykupionych na siebie lub swoich bliskich ubezpieczeń na życie i dożycie lub ubezpieczeń na życie połączonych z funduszem inwestycyjnym, tytułem składek dodatkowych. Po pewnym czasie środki z tych składek są wycofywane i przekazywane dalej na rachunek bankowy przestępcy lub osoby przez niego kontrolowanej. 2. Zakładanie polisy ubezpieczeniowej z opcjami dodatkowymi np. możliwością częściowego wykupu polisy, wycofywaniu wpłaconych składek, możliwością przelewania środków na rachunek polisy przez osoby trzecie. W ten sposób mogą być realizowane transakcje poza typowym rachunkiem bankowym np. przy omijaniu egzekucji na rachunkach bankowych.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Uzyskanie ubezpieczenia na życie/dożycie jest stosunkowo łatwe. Trudno jest ukryć dane identyfikacyjne ubezpieczonego, czy uposażonego. Istnieje możliwość realizacji transakcji o charakterze międzynarodowym w przypadku, gdy klient polskiego towarzystwa ubezpieczeniowego jest rezydentem innego kraju lub dokonuje transakcji finansowej za pośrednictwem rachunku zagranicznego. Wszystkie podmioty oferujące te usługi są IO. IO z obszaru ubezpieczeń posiadają pewną świadomość swoich obowiązków z zakresu PPP/PFT, choć wciąż ujawniane są braki w ich wypełnianiu. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje prawdopodobieństwo, że przypadek prania pieniędzy w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiada zakresowi analizowanego ryzyka.
Poziom zagrożenia	2
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie możliwości oferowanych przez ubezpieczenia na życie powiązane z funduszem inwestycyjnym do legitymizowania środków z przestępczej działalności jest jedną ze zidentyfikowanych metod prania pieniędzy. GIIF otrzymywał od instytucji obowiązanych i jednostek współpracujących informacje o wykorzystywaniu takiego *modus operandi*, ale ten sposób jest postrzegany jako mało atrakcyjny i stosunkowo niebezpieczny. W wypadku tego *modus operandi* potrzebne jest planowanie, wiedza i umiejętności do jego zastosowania. Wymaga przygotowania i aktualizowania dokumentacji na potrzeby ubezpieczenia. Nie jest to też sposób tani. WNIOSEK: Wykorzystanie możliwości oferowanych przez ubezpieczenia na życie powiązane z funduszem inwestycyjnym do legitymizowania środków z

	przestępczej działalności stwarza średnie zagrożenie dla prania pieniędzy.

Finansowanie terroryzmu

Tabela 16

Rodzaj wykorzystanych usług, produktów finansowych	Ubezpieczenia komunikacyjne
Ogólny opis ryzyka	Wyłudzanie odszkodowań z ubezpieczeń w celu finansowania terroryzmu
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	Celowe wywołanie kolizji drogowej w celu uzyskania odszkodowania, które zostanie przeznaczone na finansowanie terroryzmu.
Poziom podatności	4
Uzasadnienie dla poziomu podatności	Uzyskanie ubezpieczenia komunikacyjnego jest stosunkowo łatwe. Trudne jest ukrycie danych identyfikacyjnych ubezpieczonego czy uposażonego. Istnieje możliwość realizacji transakcji o charakterze międzynarodowym w przypadku, gdy klient polskiego towarzystwa ubezpieczeniowego jest rezydentem innego kraju lub dokonuje transakcji finansowej za pośrednictwem rachunku zagranicznego. Podmioty oferujące te usługi nie są IO. Organy administracji publicznej posiadają podstawową wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF nie ma możliwości gromadzenia i analizowania informacji dot. tego typu usług. Istnieje prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy nie zostanie wykryty. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne nie odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	1
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie mechanizmu wyłudzenia odszkodowania z ubezpieczeń może być jedną z form finansowania terroryzmu. Jednakże stopień skomplikowania procedury uzyskiwania odszkodowania, przygotowanie odpowiedniej dokumentacji oraz ryzyko kontaktu z organami ścigania powoduje nieatrakcyjność tej formy finansowania działalności terrorystycznej. W warunkach polskich brak jest jednoznacznej informacji o wykorzystywaniu tego *modus operandi* dla finansowania terroryzmu. Jest on trudny do zastosowania z uwagi na konieczność posiadania wiedzy specjalistycznej, a istnieją tańsze i łatwiejsze sposoby finansowania działalności terrorystycznej. WNIOSEK: Wykorzystanie mechanizmu wyłudzenia odszkodowania z ubezpieczeń w celu gromadzenia środków na finansowanie działalności terrorystycznej stwarza niskie zagrożenie finansowaniem terroryzmu.

Tabela 17

Rodzaj wykorzystanych usług, produktów finansowych	Ubezpieczenia na życie
Ogólny opis ryzyka	Przeznaczenie pieniędzy z polisy na finansowanie terroryzmu
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	Likwidacja polisy ubezpieczenia na życie w celu uzyskania pieniędzy z wpłaconych wcześniej składek przed podróżą zagranicznych bojowników terrorystycznych do strefy konfliktu.
Poziom podatności	2

Uzasadnienie dla poziomu podatności	Uzyskanie ubezpieczenia na życie/dożycie jest stosunkowo łatwe. Trudno jest ukryć dane identyfikacyjne ubezpieczonego czy uposażonego. Istnieje możliwość realizacji transakcji o charakterze międzynarodowym w przypadku, gdy klient polskiego towarzystwa ubezpieczeniowego jest rezydentem innego kraju lub dokonuje transakcji finansowej za pośrednictwem rachunku zagranicznego. Wszystkie podmioty oferujące te usługi są IO. Posiadają one świadomość swoich obowiązków z zakresu PPP/PFT, choć relatywnie niewiele informacji o podejrzanych transakcjach/podejrzanej działalności jest przekazywanych przez towarzystwa ubezpieczeń na życie. Należy jednak pamiętać, że ubezpieczyciele w związku z pandemią COVID-19 dostosowali swoje systemy sprzedaży do faktycznych warunków gospodarczych i aby utrzymać sprzedaż umów ubezpieczenia na życie wprowadzili rozwiązania technologiczne umożliwiające udostępnianie umów ubezpieczenia na życie na odległość. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Wewnątrz samych zakładów ubezpieczeń funkcjonują struktury mające na celu wykrywanie oszustw. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają zakresowi analizowanego ryzyka.
Poziom zagrożenia	1
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie środków finansowych pochodzących z likwidowanej polisy na życie może być jedną z form finansowania terroryzmu. Jednakże ten *modus operandi* może być stosunkowo kosztowny z uwagi na możliwość utraty części środków (związaną z warunkami umowy ubezpieczenia), a przez to stopień atrakcyjności tej formy finansowania działalności terrorystycznej jest dosyć niski. W Polsce, gdzie nie odnotowano stosunkowo wielu przypadków podróży bojowników terrorystycznych do strefy konfliktu, brak jest jednoznacznej informacji o wykorzystywaniu tego *modus operandi* dla finansowania terroryzmu. Istnieją tańsze i łatwiejsze sposoby finansowania działalności terrorystycznej. WNIOSEK: Wykorzystanie środków finansowych ze zlikwidowanej polisy na życie w celu sfinansowania działalności terrorystycznej, zwłaszcza na podróż bojowników do strefy konfliktu, stwarza niskie zagrożenie finansowaniem terroryzmu.

Zgodnie z raportem Insurance Europe, w 2020 r. największym europejskim rynkiem ubezpieczeniowym pozostawała Wielka Brytania[24]. Za nią plasowała się Francja i Niemcy. Na koniec 2021 r. łączna wartość aktywów krajowych zakładów ubezpieczeń wynosiła 201,6 mld zł. Aby ocenić wielkość polskiego rynku ubezpieczeniowego należy wiedzieć, że ogółem wartość zebranych składek ubezpieczeniowych w 2021 r. wyniosła 69,2 mld zł[25], z czego ubezpieczenia na życie stanowiły 32%, a ubezpieczenia majątkowe około 68% Łączna wartość wypłaconych przez ubezpieczycieli odszkodowań i świadczeń wyniosła w 2021 r. 41,3 mld zł. Odszkodowania i świadczenia w poszczególnych grupach (Dział I) wyniosły 18,4 mld zł, w tym świadczenia z ubezpieczenia na życie wyniosły 7,5 mld zł., z OC komunikacyjnego 9,3 mld zł oraz Autocasco 6,0 mld zł. Liczba polis pozostałych ubezpieczeń osobowych i majątkowych (oprócz OC posiadaczy pojazdów mechanicznych oraz polis Autocasco) na koniec 2021 r. to 58 135 637. Udział bancassurance (forma wymiany usług pomiędzy bankiem a zakładem ubezpieczeń, polegająca na wzajemnym oferowaniu produktów, ubezpieczeń klientom banku i produktów bankowych klientom zakładu ubezpieczeń) w składce

[24] Raport Polskiej Izby Ubezpieczeń „Ubezpieczenia w liczbach 2021 Rynek ubezpieczeń w Polsce"
[25] Tamże

ubezpieczeń życiowych to 19,0%. Wartość składki życiowej to 4,2 mld zł, a wartość składki majątkowej to 2,6 mld zł.

W segmencie ubezpieczeń na życie wypłaty z tytułu polis na życie wyniosły po III kwartałach 2022 r. 14,5 mld zł, z czego 5,1 mld zł to wypłaty z ubezpieczeń na życie o charakterze ochronnym. Było to o 8 % mniej niż w analogicznym okresie roku poprzedniego. W 2022 r. roku zakłady ubezpieczeń notują niższe wskaźniki śmiertelności niż w poprzednim, stąd obserwowany spadek wypłat w tym segmencie rynku. Na koniec III kwartału 2022 r. łączne przychody ze składek z ubezpieczeń na życie wyniosły 15,9 mld zł. Z tego aż 12,7 mld zł (wzrost o 5,1%) przypadło na ochronne ubezpieczenia na życie (7,1 mld zł) oraz wypadkowe i chorobowe (5,6 mld zł).

Według danych Polskiej Izby Ubezpieczeń[26] w 2021 roku w Polsce wykryto ponad 25 tysięcy przypadków wyłudzeń odszkodowań. Ponad 4,5 tys. przypadków dotyczyło ubezpieczeń na życie, większość, bo prawie 21 tys., ubezpieczeń majątkowych. Udaremniono nienależne wypłaty na kwotę prawie 442 mln złotych – 34 mln w ubezpieczeniach na życie oraz 408 mln zł w ubezpieczeniach majątkowych. Wyłudzenia dotyczyły nie tylko majątku, ale również szkód osobowych, które mają znaczny wpływ na wysokość nienależnych świadczeń. W ubezpieczeniach na życie, podobnie jak w roku 2020, najczęściej występujące przypadki to leczenie szpitalne i operacyjne. To ponad 50% wszystkich wyłudzeń z ubezpieczeń działu I. 18% to sprawy związane z trwałym inwalidztwem lub uszczerbkami na zdrowiu powstałymi wskutek nieszczęśliwego wypadku. Podobnie jak w roku 2020, spadła liczba fałszywych zgłoszeń związanych ze zgonem ubezpieczonego, zarówno pod względem liczbowym, jak i wysokości udaremnionych wypłat.

Działalność zakładów ubezpieczeń w Polsce podlega nadzorowi sprawowanemu przez Komisję Nadzoru Finansowego. Rejestr pośredników ubezpieczeniowych dostępny jest na stronach KNF. Rejestr pośredników ubezpieczeniowych składa się z rejestru agentów i rejestru brokerów.

Podatność sektora

Wszystkie podmioty oferujące usługi ubezpieczenia są IO. Posiadają one świadomość swoich obowiązków z zakresu PPP/PFT, choć relatywnie niewiele informacji o podejrzanych transakcjach/podejrzanej działalności jest przekazywanych przez towarzystwa ubezpieczeń na życie. W zakresie polis ubezpieczeniowych w latach 2019-2021 GIIF otrzymał i zrealizował jedynie 4 powiadomienia o transakcjach podejrzanych. Statystycznie liczba spraw zrealizowanych przez GIIF dotycząca polis ubezpieczeniowych stanowiła w 2019 r. ok. 0,2% wszystkich postępowań dotyczących podejrzenia prania pieniędzy lub finansowania terroryzmu w związku z wykorzystaniem do podejrzanych transakcji polis ubezpieczeniowych, w 2020 r. ok. 0,2%, a w 2021 r. ok 0,4%. Podmioty sektora ubezpieczeniowego stosują środki bezpieczeństwa finansowego, określone w ustawie, choć wciąż ujawniane są podczas kontroli braki w tym obszarze. Wymienione w ustawie środki bezpieczeństwa finansowego obejmują przede wszystkim czynności związane z identyfikacją klienta oraz weryfikacją jego tożsamości; identyfikację beneficjenta rzeczywistego oraz podejmowanie uzasadnionych czynności w celu weryfikacji jego tożsamości oraz ustalenia struktury własności i kontroli w przypadku klienta będącego osobą prawną albo jednostką organizacyjną nieposiadającą

[26] https://piu.org.pl/analiza-przestepczosc-ubezpieczeniowa-w-2021-r/ dostęp w dniu 13.12.2022 r.

osobowości prawnej. Ponadto podmioty świadczące usługi ubezpieczeniowe powinny dokonywać oceny stosunków gospodarczych klienta oraz (stosownie do sytuacji) uzyskiwać informacje na temat ich celu i zamierzonego charakteru. Na bieżąco też powinny monitorować stosunki gospodarcze swoich klientów. Należy jednak pamiętać, że ubezpieczyciele w związku z pandemią COVID-19 dostosowali swoje systemy sprzedaży do faktycznych warunków gospodarczych, spełniając wymagania w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, aby utrzymać wolumen sprzedaży umów ubezpieczenia na życie. Wiązało się to przede wszystkim z wprowadzeniem rozwiązań technologicznych umożliwiających dystrybucję umów ubezpieczenia na życie na odległość. Na sektor ubezpieczeniowy mają wpływ czynniki zewnętrzne tj. pandemia COVID-19 oraz wybuch wojny na Ukrainie. W ocenie rynku ubezpieczeniowego czynniki te w znacznym stopniu wpływają na obecny poziom ryzyka związany z prowadzeniem działalności ubezpieczeniowej, w szczególności w kontekście prawidłowego stosowania przez podmioty nadzorowane wzmożonych środków bezpieczeństwa finansowego, w tym dotyczących powiązań klientów zakładów ubezpieczeń o charakterze osobowym, kapitałowym lub biznesowym z podmiotami z Federacji Rosyjskiej lub Republiki Białorusi. Zakłady ubezpieczeń w istotnie większym zakresie muszą obecnie monitorować stosunki gospodarcze z klientami, czy weryfikować beneficjentów rzeczywistych w umowach ubezpieczenia. Jak wynika z posiadanych przez GIIF informacji instytucje sektora ubezpieczeniowego dysponują zaawansowanymi, automatycznymi narzędziami i systemami informatycznymi, wspomagającymi nie tylko analizę stopnia podejrzaności transakcji ubezpieczeniowych, ale też wspomagające realizację celów przeciwdziałania praniu pieniędzy oraz finansowania terroryzmu. W tych to celach wykorzystywane są przez instytucje ubezpieczeniowe np. systemy wspomagające proces analizy transakcji czy systemy do weryfikacji klientów pod kątem list sankcyjnych. GIIF ponadto prowadził szkolenia dla instytucji obowiązanych i jednostek współpracujących, podczas których są przekazywane teoretyczne i praktyczne wskazówki dotyczące np. ustalania beneficjenta rzeczywistego oraz struktury własności i kontroli klientów a także raportowania rozbieżności do organu właściwego w sprawie CRBR. Prowadzone są także szkolenia podnoszące świadomość AML/CTF w instytucjach obowiązanych. Szkolenia te organizowane są zarówno przez GIIF, jak i przez UKNF w ramach Programu CEDUR.

Intensywność i szczegółowość stosowanych przez zakłady ubezpieczeń środków bezpieczeństwa finansowego, forma i zakres ich zindywidualizowanego zastosowania, modyfikacja ich szczegółowych zasad wdrożenia, zależą od przeprowadzonej w tym kontekście środków należytej staranności wobec klienta (CDD - odnosi się do monitorowania klientów i ich aktywności w celu upewnienia się czy klient nie zmienił się znacząco w czasie), mającej na celu ograniczenie możliwości dokonywania transakcji ryzykownych z punktu widzenia AML i CTF. Niezbędne w takich wypadkach prawidłowe ustalenie tożsamości i statusu stron umów ubezpieczenia na życie, w tym beneficjenta i, w stosownych przypadkach, beneficjenta rzeczywistego (beneficjentów rzeczywistych), określi zakres kontroli, które należy przeprowadzić, w szczególności w wypadkach, kiedy potencjalnie ma się do czynienia z osobą zajmującą eksponowane stanowisko polityczne (PEP).

W kontekście prawidłowego stosowania środków bezpieczeństwa finansowego oraz z uwagi na trwający konflikt zbrojny na Ukrainie utrudnione jest w niektórych przypadkach pozyskanie szerszego spektrum dokumentów potwierdzających tożsamość lub wiarygodność klienta. Występują poważne problemy z identyfikacją i weryfikacją osób. Występująca bariera językowa i kulturowa w istotny sposób wpływa na prawidłowe rozpoznanie czynników

zwiększonego ryzyka. Stanowi ona ten czynnik behawioralny, który utrudnia prawidłową ocenę odpowiedzi klientów-uchodźców w kwestiach problematycznych, które wymagają dodatkowych informacji czy dokumentów. Biorąc pod uwagę dużą w Polsce liczbę polis ubezpieczeń osobowych i majątkowych, zwraca uwagę niewielka ilość zawiadomień zgłaszanych przez te podmioty ubezpieczeniowe do GIIF. Występują również problemy z weryfikacją zagranicznych klientów w centralnych rejestrach beneficjentów rzeczywistych państw UE, zwłaszcza dotyczy to podmiotów o skomplikowanej strukturze kapitałowej.

Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w zakresie sektora ubezpieczeń. GIIF ma możliwość gromadzenia i analizowania informacji w tym zakresie. Istnieje duże prawdopodobieństwo, że przypadek ML oraz FT z wykorzystaniem produktów rynku ubezpieczeń, szczególnie ubezpieczeń na życie, zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Co istotne, wewnątrz samych zakładów ubezpieczeń funkcjonują profesjonalne struktury mające na celu wykrywanie i przeciwdziałanie oszustwom ubezpieczeniowym.

Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie.

Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.

Zagrożenia w sektorze

Chociaż pod względem produktowym sektor ubezpieczeń na życie jest potencjalnie mniej narażony na ryzyko ML i FT niż np. sektor bankowy, to jednak w wypadku nawet stosunkowo mało elastycznych produktów ubezpieczeniowych na życie istnieje ryzyko, że środki wykorzystane do zakupu ubezpieczenia na życie mogą pochodzić z przestępstwa. Istnieje również ryzyko, stosunkowo ograniczone, że środki wycofane z umów ubezpieczenia na życie mogłyby zostać wykorzystane do finansowania terroryzmu. W wypadku produktów ubezpieczeniowych ważne są kanały sprzedaży tych produktów. Np. duży wolumen sprzedaży polis ubezpieczeniowych na życie odbywa się za pośrednictwem pośredników, w przypadku których ubezpieczyciel na życie będzie miał ograniczony lub żaden bezpośredni kontakt z posiadaczem polisy. Istotne są również niektóre cechy produktów ubezpieczeniowych, których obecność w produkcie może stwarzać zwiększone zagrożenie w kontekście ML i FT. Chodzi tu mianowicie o tak zaprojektowane produkty, by mogły one przechowywać fundusze lub majątek ubezpieczonego, produkty z potencjalnymi wieloma rachunkami inwestycyjnymi, produkty oferujące opcje przeniesienia posiadanych aktywów do polisy.

Z punktu widzenia zagrożeń ML i FT wzrost zagrożenia może powodować również szybki wzrost bazy klientów ubezpieczyciela lub rotacja tej bazy. Zwłaszcza gdy nie jest to związane w czasie z prowadzonymi kampaniami reklamowymi. Innym zagrożeniem są klienci, których nieprzejrzysta struktura własnościowa czy zarządcza czyni ich trudnymi do zidentyfikowania pod kątem beneficjenta rzeczywistego ubezpieczonego lub beneficjenta.

Zagrożenie może również być związane z metodami płatności za produkty ubezpieczeniowe. Są nimi gotówka lub inne formy płatności sprzyjające anonimowości, płatności z różnych kont bankowych należących do niepowiązanych osób trzecich. Zagrożenie mogą stwarzać także niejasne lub podejrzane źródła pochodzenia środków inwestycyjnych, które są zaangażowane w relacje biznesowe (np. wykupienie produktu z dużym udziałem inwestycyjnym przez osobę o niskich dochodach bez wyraźnego źródła pochodzenia środków finansowych). Ponadto

wyższe zagrożenie mogą stwarzać produkty, które pozwalają na wcześniejsze wycofanie się z inwestycji i mają wcześniej zagwarantowaną wartość wykupu. Z podmiotowego punktu widzenia zagrożenia ML i FT mogą stwarzać osoby i podmioty - klienci, beneficjenci, ubezpieczający i/lub powiązane osoby trzecie, które mają siedzibę lub są powiązane z krajami o wyższym ryzyku prania pieniędzy lub finansowania terroryzmu, ewentualnie które mieszkają w krajach uważanych za niechętne do współpracy w dostarczaniu informacji o beneficjentach rzeczywistych.

W sektorze ubezpieczeń występują jednak i obszary w których użycie produktów ubezpieczeniowych powoduje niewielkie zagrożenie oraz wykazywana jest niska podatność na pranie pieniędzy i finansowanie terroryzmu. Przykładami takich obszarów sektora ubezpieczeń o niższym ryzyku są produkty wypłacane tylko w przypadku śmierci i/lub niepełnosprawności ubezpieczonego czy polisy ubezpieczeniowe dla programów emerytalnych, jeśli nie ma klauzuli wykupu i polisa nie może być wykorzystana jako zabezpieczenie. Należą tu też programy emerytalne, które zapewniają pracownikom świadczenia emerytalne, gdzie składki są odprowadzane z wynagrodzenia, a zasady programu nie zezwalają na cesję udziału członka w ramach programu (np. niewielkie składki ubezpieczeniowe). Niższe zagrożenie stwarza też obsługa klientów, którzy są spółkami publicznymi notowanymi na giełdach z odpowiednimi wymogami dotyczącymi ujawniania w celu zapewnienia przejrzystości własności rzeczywistej. Nie powodują zwiększonego zagrożenia ML i FT transakcje obejmujące kwoty de minimis, takie jak polisy ubezpieczeniowe na życie, gdzie składka roczna nie przekracza kwoty 1 000 USD/EUR lub jednorazowa składka nie przekracza 2 500 USD/EUR.

Pranie pieniędzy, jak i finansowanie terroryzmu poprzez produkty oferowane przez sektor ubezpieczeniowy ma uzasadnienie ekonomiczne, jednakże stopień skomplikowania procedury uzyskiwania odszkodowania, przygotowanie odpowiedniej dokumentacji oraz ryzyko kontaktu z organami ścigania powoduje stosunkową nieatrakcyjność tej formy prania pieniędzy czy finansowania działalności terrorystycznej. W wypadku użycia produktów ubezpieczeniowych potrzebne jest planowanie, wiedza i umiejętności do jego zastosowania. Użycie produktów ubezpieczeniowych wymaga przygotowania i aktualizowania dokumentacji na potrzeby ubezpieczenia.

Uśredniony poziom zagrożenia sektora ubezpieczeniowego – ML – 2,0 i FT – 1,0

Uśredniony poziom podatności sektora ubezpieczeniowego – ML – 2,0 i FT – 3,0

Oszacowany poziom prawdopodobieństwa dla sektora – ML – 2,00 i FT - 2,20

Poziom ryzyka jest ostatecznie określany przez kombinację zagrożenia i podatności. Macierz ryzyka określająca ten poziom ryzyka opiera się na wadze 40% (zagrożenie) + 60% (podatność) – przy założeniu, że komponent podatności ma większą zdolność określania poziomu ryzyka. Zakłada się, że poziom podatności może zwiększyć atrakcyjność, a tym samym zamiary przestępców/terrorystów, aby użyć danego modus operandi – wpływając w ten sposób ostatecznie na poziom zagrożenia. Poziom ryzyka sektora, z uwzględniem prawdopobieństwa i konsekwencji (współczynnik 2,5 dla PP i 1,5 dla FT), jest ustalany zgodnie z metodyką krajowej oceny ryzyka – aneks nr 1.

Ryzyko FT sektora ubezpieczeniowego –1,92	
1 – 1,5	Niskie
1,6 – 2,5	Średnie
2,6 – 3,5	Wysokie
3,6 – 4	Bardzo wysokie
Ryzyko ML sektora ubezpieczeniowego – 2,20	
1 – 1,5	Niskie
1,6 – 2,5	Średnie
2,6 – 3,5	Wysokie
3,6 – 4	Bardzo wysokie

WNIOSEK 1: Poziom ryzyka wykorzystania sektora usług ubezpieczeniowych do finansowania terroryzmu w Polsce znajduje się na poziomie średnim.

WNIOSEK 2: Poziom ryzyka wykorzystania sektora usług ubezpieczeniowych do prania pieniędzy w Polsce znajduje się na poziomie średnim.

Mitygacja zidentyfikowanych ryzyk:

W celu ograniczenia prawdopodobieństwa wykorzystania sektora usług ubezpieczeniowych do prania pieniędzy lub finansowania terroryzmu, zasadne jest podjęcie odpowiednich działań. Stosowanie zaproponowanych działań mitygujących powinno następować z uwzględnieniem rozpoznanego przez danę instytucję obowiązaną ryzyka.

Podmioty sektora usług ubezpieczeniowych powinny kontynuować działania związane z odpowiednią oceną stosunków gospodarczych klienta oraz uzyskiwaniem informacji na temat ich celu i zamierzonego charakteru, a także powinny utrzymywać bieżący monitoring stosunków gospodarczych.

Kontynuowane powinny być szkolenia dla instytucji obowiązanych z sektora usług ubezpieczeniowych, podczas których będą przekazywane teoretyczne i praktyczne wskazówki dotyczące ustalania beneficjenta rzeczywistego oraz struktury własności i kontroli klientów a także raportowania rozbieżności do organu właściwego w sprawie CRBR. Zalecane jest uczestnictwo przedstawicieli instytucji obowiązanych w szkoleniach podnoszących świadomość AML/CTF, organizowanych zarówno przez GIIF, jak i przez UKNF w ramach Programu CEDUR.

Instytucje Obowiązane sektora usług ubezpieczeniowych powinny zwracać szczególną uwagę na beneficjentów polis ubezpieczeniowych z jurysdykcji charakteryzujących się wyższym ryzykiem prania pieniędzy oraz finansowania terroryzmu. W szczególności należy zwracać

uwagę na cesję polis, przy braku uzasadnienia dla tego typu działań (w szczególności brak realnych powiązań osobistych, czy też kapitałowych między cedentem a cesjonariuszem).

Instytucje obowiązane powinny przykładać szczególną wagę do czynników geograficznych mogących wskazywać na wyższe ryzyko prania pieniędzy czy też finansowania terroryzmu, takich jak niestabilna sytuacja polityczna czy konflikt zbrojny, czego najdobitniejszym przykładem w ostatnich latach jest wojna prowadzona przez Rosję przeciwko Ukrainie. Z uwagi na wysokie ryzyko transferowania środków pochodzących z nielegalnego handlu, przemytu ludzi, handlu bronią, czy też działań zmierzających do omijania sankcji gospodarczych, szczególnie istotne jest analizowanie przez instytucje obowiązane nie tylko danych dotyczących samych stron transakcji, ale również beneficjentów rzeczywistych, czy też faktycznych celów przeprowadzania danych transakcji (zawierania polis, czy też ich cesji).

4. Obszar – inne instytucje finansowe

Opis sektora – zawarty jest w podrozdziałach KOR 2.1.2 - „Sektory rynku finansowego" oraz w podrozdziale 7.2.1 - „Podatność rynku finansowego".

Scenariusze wystąpienia ryzyka (tj. możliwe przykłady wystąpienia ryzyka) zarówno w przypadku prania pieniędzy, jak i finansowania terroryzmu - dotyczyły wykorzystania do prania pieniędzy i finansowania terroryzmu produktów i usług finansowych w postaci usług na rynku finansowym Forex, faktoringu, leasingu, jednostek funduszy inwestycyjnych oraz rachunków papierów wartościowych i rachunków pieniężnych służących do ich obsługi. Opis scenariuszy znajduje się poniżej.

Pranie pieniędzy

Tabela 18

Rodzaj wykorzystanych usług, produktów finansowych	Usługi na rynku walutowym FOREX
Ogólny opis ryzyka	Wykorzystanie firmy brokerskiej działającej na rynku FOREX jako "market maker" do legitymizowania środków pochodzących z nielegalnych źródeł
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Firma działająca legalnie na rynku FOREX jako broker i *market maker*, jest kontrolowana przez osoby powiązane z przestępcami, którzy potajemnie finansują jej działalność. Przestępcy zakładają konta na platformie transakcyjnej prowadzonej przez tą firmę. Dzięki poufnym informacjom oraz korzystniejszym warunkom otrzymanym od tej firmy pomnażają swój kapitał, który jest wykazywany przed urzędem skarbowym jako zysk z inwestycji na rynku FOREX. 2. Przedkładanie bankowi nierzetelnej/sfabrykowanej umowy faktoringowej w celu uprawdopodobnienia przeprowadzanych transakcji.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Usługi na rynku FOREX są dostępne za pośrednictwem brokerów. Raczej trudno jest ukryć dane identyfikacyjne zlecającego transakcje na tym rynku za pośrednictwem licencjonowanego brokera. Mogą występować transakcje o charakterze międzynarodowym w przypadku, gdy klient jest rezydentem innego kraju lub dokonuje transakcji finansowej za pośrednictwem rachunku zagranicznego albo korzysta z usług podmiotu zagranicznego. Wszystkie podmioty oferujące usługi brokerskie są IO (domy maklerskie bądź banki posiadające w swoich strukturach biura maklerskie) - jakkolwiek klienci mogą korzystać z usług oferowanych przez Internet przez podmioty zagraniczne. IO z tego obszaru posiadają pewną świadomość swoich obowiązków z zakresu PPP/PFT, choć wciąż ujawniane są braki w ich wypełnianiu.[27] Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek prania pieniędzy w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	2

[27] Podczas wszystkich przeprowadzonych w latach 2019 - 2020 r. przez UKNF kontroli (m.in. w 3 domach maklerskich, u 2 agentów firm inwestycyjnych, w 1 banku prowadzącym działalność maklerską) ujawniono nieprawidłowości i uchybienia w badanych obszarach, głównie w zakresie oceny ryzyka i stosowania środków bezpieczeństwa finansowego, tj. np. błędna ocena ryzyka w obszarze usług maklerskich, czy brak zgodności działalności tych podmiotów z obowiązującymi przepisami prawa.

Uzasadnienie dla poziomu zagrożenia	Forex to międzynarodowy rynek wymiany walut, o charakterze hurtowym, w ramach którego banki, wielkie korporacje międzynarodowe oraz inwestorzy instytucjonalni z całego świata przeprowadzają operacje wymiany walut 24 godziny na dobę przy wykorzystaniu sieci telefonicznych, łączy informatycznych oraz systemów informacyjnych. Wykorzystanie legalnej, ale kontrolowanej przez przestępców firmy działającej na rynku FOREX jako brokera w modelu "market maker" do legitymizowania środków pochodzących z nielegalnych źródeł jest metodą prania pieniędzy mało atrakcyjną i stosunkowo niebezpieczną. Ten *modus operandi* wymaga specjalistycznej wiedzy o rynku walutowym, umiejętności i planowania. W modelu *market maker* wykazywane przez inwestorów zyski z udziału w rynku FOREX są stratą brokera. Nie może on ponosić ciągłych strat, ponieważ budzi to podejrzenia. Są informacje o wykorzystaniu tego typu działalności do popełniania przestępstw bazowych dla prania pieniędzy. WNIOSEK: Wykorzystanie firmy brokerskiej działającej na rynku FOREX jako "market maker" do legitymizowania środków pochodzących z nielegalnych źródeł stwarza średnie zagrożenie dla prania pieniędzy.

Tabela 19

Rodzaj wykorzystanych usług, produktów finansowych	Faktoring
Ogólny opis ryzyka	Wykorzystanie faktoringu do legitymizowania środków pochodzących z nielegalnych źródeł
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	Firma działająca na rynku polskim (faktorant) zawarła umowę faktoringu z 2 zagranicznymi podmiotami (faktorzy) w ramach której płaciła za nabywany towar. Środki pieniężne zasilające rachunki firmy polskiej pochodziły m.in. z wpłat gotówkowych realizowanych we wpłatomatach przez obcokrajowców. Wykorzystana do przestępstwa polska spółka została zakupiona przez obcokrajowca jako tzw. 'gotowa' spółka, w celu utrudnienia znalezienia organom ścigania osób faktycznie kierujących procederem.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Usługi faktoringu w postaci wykupu przez podmiot świadczący usługę faktoringu nieprzeterminowanych wierzytelności przedsiębiorstw należnych im od kontrahentów z tytułu dostaw i usług są stosowane na rynku finansowym. Raczej trudno jest ukryć dane identyfikacyjne zlecającego transakcje na tym rynku. Mogą występować transakcje o charakterze międzynarodowym na linii faktorant – faktorzy. Przedsiębiorstwo korzystające z usługi faktoringu szybciej otrzymuje środki finansowe wynikające z zawartej transakcji. Wszystkie podmioty oferujące te usługi są IO. Podmioty prowadzące działalność w tym obszarze posiadają pewną świadomość swoich obowiązków z zakresu PPP/PFT. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek prania pieniędzy w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	2

Uzasadnienie dla poziomu zagrożenia	Faktoring jest usługą świadczoną przez faktora, która polega na wykupie faktur od podmiotu, który jest dostawcą towarów lub wykonawcą usług na rzecz swoich kontrahentów. Przestępcy mogą wykorzystywać legalnie działającą firmę faktoringową (która jest przez nich kontrolowana) do legitymizowania środków pieniężnych pochodzących z nielegalnych źródeł. Wskazana metoda prania pieniędzy jest metodą prania pieniędzy mało atrakcyjną dla przestępców. Są informacje o wykorzystaniu tego typu działalności do popełniania przestępstw bazowych dla prania pieniędzy. WNIOSEK: Wykorzystanie faktoringu do legitymizowania środków pochodzących z nielegalnych źródeł stwarza średnie zagrożenie dla prania pieniędzy.

Tabela 20

Rodzaj wykorzystanych usług, produktów finansowych	Leasing
Ogólny opis ryzyka	Transakcje leasingu (podobnie jak w przypadku umów faktoringu) mogą być wykorzystywane do wprowadzania do obrotu finansowego wartości majątkowych pochodzących z nielegalnych źródeł przez zorganizowane grupy przestępcze
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Ulokowanie środków pochodzących z przestępstwa na rachunku przypisanym do umowy leasingowej i następnie wniosek do firmy leasingowej o zwrot nadpłaconych środków. 2. Ulokowanie środków pochodzących z przestępstwa poprzez założenie firmy – 'przedsiębiorstwo symulujące' (stworzenie pozorów prowadzonej działalności gospodarczej), a następnie przekazywanie środków pochodzących z przestępstwa na rachunek firmy leasingowej w celu uruchomienia kredytu na zakup samochodu.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Transakcja leasingu (podobnie jak w przypadku umowy faktoringu) może być wykorzystywana do wprowadzania do obrotu finansowego środków pochodzących z przestępstwa. Decydować może o tym jej złożony charakter (przestępcy używają często kilku metod PP/FT powiązanych z transakcją leasingu). Te cechy mają o tyle istotne znaczenie, iż im bardziej złożony, skomplikowany obrót transakcyjny, tym łatwiej jest zalegalizować, ukryć przestępcze pochodzenie środków pieniężnych. Podmioty oferujące usługi w zakresie leasingu finansowego są IO. Podmioty prowadzące działalność w tym obszarze posiadają pewną świadomość swoich obowiązków z zakresu PPP/PFT. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek prania pieniedzy w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	2
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie możliwości zawarcia umowy leasingowej, a następnie ich spłata środkami pochodzącymi z nielegalnych źródeł nie jest postrzegana w Polsce jako atrakcyjna metoda prania pieniędzy. Są nieliczne informacje o wykorzystaniu tego typu działalności do popełniania przestępstw bazowych dla prania pieniędzy. WNIOSEK: Wykorzystanie leasingu do legitymizowania środków pochodzących z nielegalnych źródeł stwarza średnie zagrożenie dla prania pieniędzy.

Tabela 21

Rodzaj wykorzystanych usług, produktów finansowych	Jednostki funduszy inwestycyjnych
Ogólny opis ryzyka	Zakup jednostek uczestnictwa w funduszach inwestycyjnych za środki pochodzące z nielegalnych źródeł
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	Sprawcy regularnie kupują jednostki uczestnictwa w funduszach inwestycyjnych za niewielkie kwoty, aby następnie po ich skumulowaniu je odsprzedać, a środki wytransferować poza granice kraju
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Dostęp do jednostek uczestnictwa w funduszach inwestycyjnych (FI) jest relatywnie łatwy. Trudno jest ukryć dane identyfikacyjne klientów funduszy inwestycyjnych. Mogą występować transakcje o charakterze międzynarodowym związane z kupnem i sprzedażą jednostek uczestnictwa jedynie w przypadku, gdy klient polskiego FI jest rezydentem innego kraju lub dokonuje transakcji finansowej za pośrednictwem rachunku zagranicznego albo jednostki uczestnictwa są kupowane od zagranicznego FI. Wszystkie podmioty oferujące te usługi są IO – jakkolwiek klienci mogą korzystać z usług oferowanych przez podmioty zagraniczne. IO z tego obszaru posiadają pewną świadomość swoich obowiązków z zakresu PPP/PFT, choć wciąż ujawniane są braki w ich wypełnianiu. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek prania pieniędzy w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	2
Uzasadnienie dla poziomu zagrożenia	Ponieważ fundusze inwestycyjne różnią się między sobą poziomem ryzyka i związanym z nim rodzajem instrumentu finansowego, w który lokują swoje aktywa, różny bywa uzyskiwany poziom zysku/straty na zakupionej jednostce funduszu. Te różnice wynikają także z horyzontu czasowego inwestycji i jej celów. GIIF miał nieliczne informacje o inwestowaniu nielegalnych środków finansowych w fundusze inwestycyjne. Wymaga to zawsze od inwestującego planowania, umiejętności i specjalistycznej wiedzy o rynku finansowym. *Modus operandi* prania pieniędzy z wykorzystaniem zakupu jednostek uczestnictwa w funduszach inwestycyjnych za środki pochodzące z nielegalnych źródeł postrzegany jest jednak jako mało atrakcyjny. WNIOSEK: Zakup jednostek uczestnictwa w funduszach inwestycyjnych za środki pochodzące z nielegalnych źródeł stwarza średnie zagrożenie dla prania pieniędzy.

Tabela 22

Rodzaj wykorzystanych usług, produktów finansowych	Rachunki papierów wartościowych i rachunki pieniężne służące do ich obsługi
Ogólny opis ryzyka	Wykorzystanie rachunków papierów wartościowych i rachunków pieniężnych służących do ich obsługi w celu transferowania i legitymizowania środków pochodzących z nielegalnych źródeł

Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Sprawcy, za pośrednictwem firm utworzonych w szczególności w rajach podatkowych, lokują środki pozyskane z nielegalnych źródeł na rynku kapitałowym. 2. Sprawcy wykorzystują rachunek pieniężny służący do obsługi rachunków papierów wartościowych, założony na rzecz osoby fizycznej lub firmy powiązanej z nimi, jako "skrzynkę rozdzielczą". Na rachunek są transferowane środki z nielegalnych źródeł w celu ich dalszego transferowania na rachunki bankowe innych podmiotów kontrolowanych przez przestępców. 3. Rachunek papierów wartościowych należący do osoby lub podmiotu kontrolowanego przez przestępców jest wykorzystywany do kupna papierów wartościowych za pieniądze pochodzące z nielegalnych źródeł zgromadzonych na rachunku pieniężnym służącym do obsługi ww. rachunku, a następnie ich odsprzedaży w relatywnie krótkim czasie. Ewentualne straty wynikające z tych transakcji są wówczas kosztem legalizacji tych środków.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Otwarcie tego typu rachunków jest stosunkowo łatwe. Raczej trudno jest ukryć dane identyfikacyjne klientów. Występują transakcje o charakterze międzynarodowym. Wszystkie podmioty oferujące te usługi są IO. Posiadają one pewną świadomość swoich obowiązków z zakresu PPP/PFT, choć wciąż ujawniane są braki w ich wypełnianiu. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek prania pieniędzy w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	3
Uzasadnienie dla poziomu zagrożenia	GIIF posiada pewne informacje o wykorzystywaniu tego *modus operandi* przez przestępców. Wpłaty na rachunek pieniężny służący do obsługi rachunku papierów wartościowych, a następnie różne formy operacji inwestycyjnych tymi środkami bądź wypłata lub przelew na inny rachunek jest pozorowaniem legalnego pochodzenia wartości majątkowych uzyskanych w wyniku działalności przestępczej. Wiąże się to z domniemaniem, że środki, które znajdują się na rachunku pieniężnym służącym obsłudze rachunku papierów wartościowych, pochodzą z operacji finansowych dokonywanych na giełdzie. Ten *modus operandi* postrzegany jest przez sprawców jako dosyć atrakcyjna forma prania pieniędzy. Stopień skomplikowania rynku kapitałowego jest dużym atutem dla przestępczej działalności mającej na celu pranie pieniędzy. Wykorzystanie rachunków papierów wartościowych i rachunków pieniężnych służących do ich obsługi w celu transferowania i legitymizowania środków wymaga co prawda specjalistycznej wiedzy, umiejętności i planowania, ale brak w organach ścigania specjalistów wysokiej klasy od rynku kapitałowego czyni ten sposób stosunkowo bezpiecznym. WNIOSEK: Wykorzystanie rachunków papierów wartościowych i rachunków pieniężnych służących do ich obsługi w celu transferowania i legitymizowania środków pochodzących z nielegalnych źródeł stwarza wysokie zagrożenie dla prania pieniędzy.

Finansowanie terroryzmu

Tabela 23

Rodzaj wykorzystanych usług, produktów finansowych	Usługi na rynku walutowym FOREX
Ogólny opis ryzyka	Wykorzystanie firmy brokerskiej działającej na rynku FOREX do oszustwa w celu pozyskania środków na działalność terrorystyczną
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Sprawcy rejestrują spółkę, która rozpoczyna działalność jako firma brokerska na rynku FOREX bez uzyskania odpowiedniego zezwolenia na prowadzenie działalności inwestycyjnej/maklerskiej. Oferta firmy jest dostępna w kilku językach i zachęca wysokimi zyskami. Dzięki temu oraz wykorzystaniu technik agresywnego marketingu budowana jest baza klientów, którzy dokonują wpłat na rachunek podmiotu z zamiarem zasilenia swojego konta maklerskiego. Inwestorzy nie zdają sobie sprawy, że transakcje, których dokonują są fikcyjne, a środki zostaną w pewnym momencie przywłaszczone przez nielegalnie działającą firmę inwestycyjną. Wprzypadku firm będących tzw. market makerami[28], istnieje także możliwość, że oferowane im będą gorsze warunki niż rynkowe, tak aby ponieśli straty, a pozyskane w ten sposób środki zasilą organizacje terrorystyczne. 2. Sprawcy rejestrują spółkę, która rozpoczyna działalność jako firma brokerska na rynku FOREX bez uzyskania odpowiedniego zezwolenia na prowadzenie działalności inwestycyjnej/maklerskiej. Sympatycy organizacji terrorystycznych, którzy przelewali środki zawierają niekorzystne dla siebie transakcje (zwłaszcza w sytuacji, gdy firma działa jako market maker) lub godzą się na wygórowaną prowizję lub też przepadek środków w momencie zakończenia działalności tego podmiotu. Pozyskane w ten sposób środki transferowane są do organizacji terrorystycznych.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Usługi na rynku FOREX są dostępne za pośrednictwem brokerów. Raczej trudno jest ukryć dane identyfikacyjne zlecającego transakcje na tym rynku za pośrednictwem licencjonowanego brokera. Mogą występować transakcje o charakterze międzynarodowym jedynie w przypadku, gdy klient jest rezydentem innego kraju lub dokonuje transakcji finansowej za pośrednictwem rachunku zagranicznego albo korzystka z usług podmiotu zagranicznego. Wszystkie podmioty oferujące te usługi są IO (domy maklerskie bądź banki posiadające w swoich strukturach biura maklerskie) - jakkolwiek klienci mogą korzystać z usług oferowanych przez Internet przez podmioty zagraniczne. IO z tego obszaru posiadają pewną świadomość swoich obowiązków z zakresu PPP/PFT, choć wciąż ujawniane są braki w ich wypełnianiu. Relatywnie niewiele informacji o podejrzanych transakcjach/podejrzanej działalności jest przekazywanych przez domy maklerskie. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	1
Uzasadnienie dla poziomu zagrożenia	FOREX to międzynarodowy rynek wymiany walut, o charakterze hurtowym, w ramach którego banki, wielkie korporacje międzynarodowe oraz inwestorzy instytucjonalni z całego świata przeprowadzają operacje wymiany walut 24 godziny na dobę przy wykorzystaniu sieci telefonicznych, łączy informatycznych

[28] Podmiot, który wystawia i kwotuje instrumenty finansowe, jednocześnie występuje jako drugą stroną transakcji zawieranych przez klienta.

	oraz systemów informacyjnych. Wykorzystanie legalnej – choć nieposiadającej odpowiedniego zezwolenia na prowadzenie działalności inwestycyjnej/maklerskiej i kontrolowanej przez przestępców – firmy działającej na rynku FOREX jako brokera w modelu market maker jest mało atrakcyjną metodą pozyskania i przeznaczenia środków na działalność terrorystyczną. Ten *modus operandi* wymaga specjalistycznej wiedzy o rynku walutowym, umiejętności i planowania. W modelu market maker wykazywane przez inwestorów straty z udziału w rynku FOREX (w wyniku oszustwa czy świadomej działalności) są zyskiem brokera i mogą być transferowane do organizacji terrorystycznych. GIIF nie posiada informacji o zamiarze wykorzystania tego *modus operandi*. WNIOSEK: Wykorzystanie firmy brokerskiej działającej na rynku FOREX jako market maker do oszustwa w celu pozyskania środków na działalność terrorystyczną stwarza niskie zagrożenie finansowaniem terroryzmu

Tabela 24

Rodzaj wykorzystanych usług, produktów finansowych	Jednostki funduszy inwestycyjnych (FI)
Ogólny opis ryzyka	Obrót jednostkami uczestnictwa w funduszach inwestycyjnych w celu gromadzenia środków na działalność terrorystyczną
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	Sprawcy regularnie kupują jednostki uczestnictwa w funduszach inwestycyjnych za niewielkie kwoty, aby następnie po ich skumulowaniu je odsprzedać, a środki wytransferować poza granice kraju.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Dostęp do jednostek uczestnictwa w funduszach inwestycyjnych jest relatywnie łatwy. Trudno jest ukryć dane identyfikacyjne klientów funduszy inwestycyjnych. Mogą występować transakcje o charakterze międzynarodowym związane z kupnem i sprzedażą jednostek uczestnictwa jedynie w przypadku, gdy klient polskiego FI jest rezydentem innego kraju lub dokonuje transakcji finansowej za pośrednictwem rachunku zagranicznego albo jednostki uczestnictwa są kupowane od zagranicznego FI. Występują jednak problemy z weryfikacją zagranicznych klientów w centralnych rejestrach beneficjentów rzeczywistych państw UE, zwłaszcza dotyczy to podmiotów o skomplikowanej strukturze kapitałowej. Wszystkie podmioty oferujące te usługi są IO – jakkolwiek klienci mogą korzystać z usług oferowanych przez podmioty zagraniczne. IO z tego obszaru posiadają pewną świadomość swoich obowiązków z zakresu PPP/PFT, choć wciąż ujawniane są braki w ich wypełnianiu. Relatywnie niewiele informacji o podejrzanych transakcjach/podejrzanej działalności jest przekazywanych przez towarzystwa funduszy inwestycyjnych i FI. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	1
Uzasadnienie dla poziomu zagrożenia	Zakup i obrót jednostkami uczestnictwa w funduszach inwestycyjnych w celu gromadzenia środków na działalność terrorystyczną może być jednym z *modus operandi* dla finansowania terroryzmu. GIIF nie miał jednak informacji o inwestowaniu nielegalnych bądź legalnych środków finansowych w fundusze inwestycyjne w tym celu. Obrót jednostkami uczestnictwa w funduszach inwestycyjnych jest trudną do zastosowania formą działania z uwagi na konieczność posiadania wiedzy specjalistycznej o rynku kapitałowym, a istnieją tańsze i łatwiejsze sposoby

	finansowania działalności terrorystycznej. WNIOSEK: Wykorzystanie zakupu i obrotu jednostkami uczestnictwa w funduszach inwestycyjnych w celu gromadzenia środków na działalność terrorystyczną stwarza niskie zagrożenie finansowaniem terroryzmu.

Tabela 25

Rodzaj wykorzystanych usług, produktów finansowych	Rachunki papierów wartościowych i rachunki pieniężne służące do ich obsługi
Ogólny opis ryzyka	Wykorzystanie rachunków papierów wartościowych i rachunków pieniężnych służących do ich obsługi w celu gromadzenia środków na działalność terrorystyczną
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Sprawcy, za pośrednictwem firm utworzonych w szczególności w rajach podatkowych, lokują środki pozyskane z nielegalnych lub legalnych źródeł na rynku kapitałowym. Zakupione papiery wartościowe są następnie sprzedawane, a uzyskane środki służą do finansowania działalności terrorystycznej. 2. Na rachunek pieniężny służący do obsługi rachunku papierów wartościowych, należący do spółki zagranicznej, kontrolowanej przez zwolenników organizacji terrorystycznej, są przelewane środki z rachunku bankowego prowadzonego w innym kraju na rzecz osoby fizycznej pod fikcyjnym tytułem inwestycji w akcje spółki publicznej. Środki są następnie - w krótkim odstępie czasu - przekazywane na rachunek bankowy prowadzony w kraju trzecim, należący do ww. spółki pod tytułem zysku z obrotu papierami wartościowymi.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Otwarcie tego typu rachunków jest stosunkowo łatwe. Raczej trudno jest ukryć dane identyfikacyjne klientów. Natomiast mogą występować problemy z weryfikacją zagranicznych klientów w centralnych rejestrach beneficjentów rzeczywistych państw UE i innych państw spoza UE, zwłaszcza dotyczy to podmiotów o skomplikowanej strukturze kapitałowej. Występują transakcje o charakterze międzynarodowym. Wszystkie podmioty oferujące te usługi są IO. Posiadają one pewną świadomość swoich obowiązków z zakresu PPP/PFT, choć wciąż ujawniane są braki w ich wypełnianiu. Relatywnie niewiele informacji o podejrzanych transakcjach/podejrzanej działalności jest przekazywanych przez domy maklerskie. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	1
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie rachunków papierów wartościowych i rachunków pieniężnych służących do ich obsługi w celu gromadzenia środków na działalność terrorystyczną może być jedną z form finansowania terroryzmu. Jednakże stopień skomplikowania rynku papierów wartościowych powoduje nieatrakcyjność tej formy finansowania działalności terrorystycznej. Brak jest jednak jednoznacznej informacji o wykorzystywaniu tego *modus operandi* dla finansowania terroryzmu. Jest on trudny do zastosowania z uwagi na konieczność posiadania wiedzy specjalistycznej o rynku kapitałowym, a istnieją tańsze i łatwiejsze sposoby finansowania działalności terrorystycznej. WNIOSEK: Wykorzystanie rachunków papierów wartościowych i rachunków pieniężnych służących do ich obsługi w celu gromadzenia środków na działalność terrorystyczną stwarza niskie zagrożenie finansowaniem terroryzmu.

W oparciu o *rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 575/2013* oraz *ustawę z dnia 29 sierpnia 1997 r. - Prawo bankowe* instytucje finansowe zostały zdefiniowane jako podmioty, których zakres obejmuje:

- przedsiębiorstwa, których podstawową działalnością jest wykonywanie co najmniej jednego z następujących rodzajów działalności: udzielanie kredytów, leasing, usługi płatnicze, emisja środków płatności w rodzaju czeków, udzielanie gwarancji, obrót niektórymi instrumentami finansowymi (czekami, wekslami, certyfikatami depozytowymi, dewizami, opcjami i kontraktami terminowymi, swapami, papierami wartościowymi), uczestniczenie w emisji papierów wartościowych, doradztwo w zakresie struktury kapitałowej czy strategii przemysłowej oraz przekształceń własnościowych, pośrednictwo na rynku pieniężnym, zarządzanie portfelem inwestycyjnym i doradztwo w tym zakresie, przechowywanie i administrowanie papierami wartościowymi oraz emisja pieniądza elektronicznego;
- instytucje płatnicze oraz spółki holdingowe instytucji finansowych (z wyjątkiem spółek holdingowych instytucji ubezpieczeniowych);
- instytucje pożyczkowe działające na podstawie *ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim*.

Z uwagi na stosunkową różnorodność usług oferowanych przez wymienione wyżej instytucje finansowe, w przedmiotowym aneksie do Krajowej Oceny Ryzyka w obszarze – instytucje finansowe jako rodzaj wykorzystanych usług, produktów finansowych, wymienione są scenariusze dotyczące usług na rynku finansowym FOREX, jednostek funduszy inwestycyjnych oraz rachunki papierów wartościowych i rachunki pieniężne służące do ich obsługi.

Rynek Forex jest międzynarodowym zdecentralizowanym rynkiem, na którym uczestnicy (głównie banki, fundusze, firmy ubezpieczeniowe i inne instytucje finansowe) wymieniają jeden rodzaj waluty na inny. Ponieważ można tu znaleźć nie tylko waluty największych gospodarek świata, Forex jest rynkiem o największej płynności na świecie (tj. codziennie około 5 bilionów dolarów). W polskiej praktyce dynamicznie rozwijającego się od kilku lat rynku Forex jego usługi są oferowane zarówno przez krajowe firmy inwestycyjne (domy maklerskie lub biura maklerskie działające w strukturach banków), jak i przez licencjonowane podmioty zagraniczne, które działają przede wszystkim transgranicznie, czyli przez Internet (mowa tu o zagranicznych firmach inwestycyjnych, prowadzących działalność maklerską w Polsce za pośrednictwem oddziału lub transgranicznie – bez konieczności jego otwierania, które posiadają siedzibę na terytorium Unii Europejskiej lub EOG i notyfikowały prowadzenie takiej działalności lub też mają stosowne zezwolenie KNF). Usługi te wiążą się z bardzo aktywnymi i wciąż rozwijanymi działaniami promocyjnymi oraz marketingowymi, mającymi na celu pozyskanie klientów, którzy zaangażują swoje środki finansowe w transakcje na rynku Forex. Samo zjawisko rosnącego zainteresowania rynkiem Forex wynika z potrzeby inwestorów lokowania kapitału w nowych formach finansowych, ale przede wszystkim wynika z wiążącej się z przedmiotowym rynkiem możliwości wypracowania zysków znacząco wyższych niż na rynku regulowanym (oeracje na rynku Forex umożliwiają zastosowanie tzw. dźwigni finansowej). Niektóre z firm oferujących inwestowanie na rynku Forex działają jednak

nielegalnie. Potencjalny odbiorca usług na rynku Forex powinien dokładnie zweryfikować kto i na jakich zasadach będzie pośredniczył w transakcjach. KNF na swojej stronie internetowej prowadzi rejestr - listę ostrzeżeń publicznych. Znajdują się na niej podmioty rynku finansowego, których działalność budzi wątpliwości i zostało wobec tych podmiotów złożone zawiadomienie o podejrzeniu popełnienia przestępstwa.

Fundusze inwestycyjne są przede wszystkim formą zbiorowego inwestowania. Fundusz inwestycyjny jest osobą prawną. Do ich zadań należy inwestowanie pozyskanego od inwestorów kapitału. Pieniądze są najczęściej lokowane w papiery wartościowe, instrumenty rynku pieniężnego, inne prawa majątkowe. W funduszu inwestycyjnym może inwestować zarówno osoba fizyczna, jak i osoba prawna oraz podmiot, który nie posiada osobowości prawnej[29]. Przystąpienie do funduszy wiąże się z koniecznością złożenia zlecenia nabycia jednostek uczestnictwa oraz wpłatą pieniężną. Fundusze inwestycyjne deklarują w statucie, w jakie instrumenty finansowe będą inwestować. Od tych instrumentów zależeć będzie potencjalny zysk, jaki fundusz będzie miał szansę wypracować, oraz ryzyko, jakie będzie się wiązać z inwestycją w ten fundusz. Pod względem kryterium zawartości portfela, dzieli fundusze na 4 grupy:

- pieniężne (inwestują głównie w papiery rynku pieniężnego, oczekiwany zysk i ryzyko ograniczone),

- dłużne (inwestują głównie w obligacje, oczekiwany zysk i ryzyko wyższe niż w pieniężnych),

- mieszane (inwestują zarówno w akcje, jak i obligacje, zysk i ryzyko z reguły wyższe niż w obligacyjnych),

- akcji (większość portfela stanowią akcje, najwyższy oczekiwany zysk i ryzyko).

Fundusz inwestycyjny jest tworzony przez Towarzystwo Funduszy Inwestycyjnych, które jest jego organem, zarządza nim i reprezentuje w stosunkach z osobami trzecimi. Zgodę na utworzenie publicznego funduszu inwestycyjnego wydaje Komisja Nadzoru Finansowego, która sprawuje stały nadzór nad jego działalnością. Fundusze inwestycyjne w Polsce są tworzone i działają na podstawie *ustawy o funduszach inwestycyjnych* i zarządzaniu alternatywnymi funduszami inwestycyjnymi, zharmonizowanej z dyrektywami unijnymi, dotyczącymi przedsięwzięć zbiorowego inwestowania w zbywalne papiery wartościowe.

Pod względem kryterium formy prawnej fundusze inwestycyjne dzielą się na trzy kategorie: fundusze inwestycyjne otwarte, specjalistyczne fundusze inwestycyjne otwarte, fundusze inwestycyjne zamknięte. Fundusz inwestycyjny otwarty może lokować aktywa w: papiery wartościowe, instrumenty rynku pieniężnego, tytuły uczestnictwa w funduszach inwestycyjnych, depozyty bankowe. Specjalistyczny Fundusz Inwestycyjny Otwarty jest formą funduszu otwartego. Oferta nabycia jednostek uczestnictwa takiego funduszu może być skierowana do określonej grupy osób, np. instytucji lub uczestników programów emerytalnych. W statucie funduszu mogą być też wprowadzone dodatkowe warunki dotyczące odkupywania jednostek uczestnictwa. Fundusz inwestycyjny zamknięty może zaciągać pożyczki i kredyty do wysokości 75 % wartości aktywów netto funduszu. Większa swoboda w kształtowaniu strategii inwestowania, a także brak konieczności posiadania przez cały czas odpowiednio wysokiego

[29]https://businessinsider.com.pl/poradnik-finansowy/oszczedzanie/jakie-sa-rodzaje-funduszy-inwestycyjnych/r0hfs9e dostęp w dniu 11.01.2023 r.

salda wolnej gotówki umożliwia funduszom inwestycyjnym zamkniętym tworzenie zróżnicowanych strategii inwestycyjnych efektywnego wykorzystania posiadanych środków finansowych, co daje potencjał osiągania wyższych dochodów niż w przypadku funduszy otwartych. Na koniec sierpnia 2022 r. funkcjonowały 685 fundusze inwestycyjne zarządzane przez 64 TFI[30]. Wartość aktywów ogółem zgromadzonych przez TFI według stanu na koniec czerwca 2022 r. wynosiła 360,7 mld zł. Fundusze podlegają obowiązkowi wpisu do rejestru funduszy inwestycyjnych. Rejestr prowadzi Sąd Okręgowy w Warszawie (sąd rejestrowy).

Działalność maklerska obejmuje wykonywanie, między innymi czynności polegających na: przyjmowaniu i przekazywaniu zleceń nabycia lub zbycia instrumentów finansowych; nabywaniu lub zbywaniu na własny rachunek instrumentów finansowych; zarządzaniu portfelami, w skład których wchodzi jeden lub większa liczba instrumentów finansowych; doradztwie inwestycyjnym oraz oferowaniu instrumentów finansowych. Firmą inwestycyjną, prowadzącą działalność maklerską, może być dom maklerski lub bank prowadzący działalność maklerską. Dom maklerski może prowadzić działalność maklerską w formie: spółki akcyjnej; spółki komandytowo-akcyjnej; spółki z ograniczoną odpowiedzialnością; spółki komandytowej; spółki partnerskiej; spółki jawnej. Prowadzenie w Polsce działalności maklerskiej wymaga uzyskania zezwolenia Komisji Nadzoru Finansowego. Sama działalność domów maklerskich podlega ścisłej kontroli ze strony Komisji Nadzoru Finansowego. Indywidualny inwestor inwestując środki poprzez biuro maklerskie nie jest stroną podczas transakcji. Kupno i sprzedaż papierów wartościowych w imieniu klienta dokonuje dom maklerski. Klient biura maklerskiego posiada rachunek maklerski, który jest rodzajem rachunku służącego do przechowywania papierów wartościowych i instrumentów finansowych oraz zlecania transakcji ich kupna i sprzedaży na giełdzie. Jest elektronicznym zapisem prowadzonym przez uprawniony dom lub biuro maklerskie na rzecz klienta, który może być osobą indywidualną lub prawną. Pieniądze z transakcji na rachunku maklerskim można wypłacić tylko na konto osobiste połączone z rachunkiem inwestycyjnym lub dowolne konto zdefiniowane jako dodatkowy rachunek do przelewów. Przepisy ustawowe wymagają także od domów maklerskich zatrudnienia na podstawie umowy o pracę odpowiedniej liczby pracowników (maklerów papierów wartościowych i/lub doradców inwestycyjnych). Określają także, jakie warunki muszą spełniać członkowie zarządu i rady nadzorczej oraz wskazują tryb powołania prezesa zarządu. Organizacją zrzeszającą domy i biura maklerskie w Polsce jest Izba Domów Maklerskich. Na koniec sierpnia 2022 r. wśród całkowitej liczby 44 firm inwestycyjnych prowadzących działalność maklerską, 9 z nich było bankami prowadzącymi działalność maklerską, a 35 niezależnymi domami maklerskimi[31].

Pod koniec 2022 r. zaszła również ważna zmiana dotycząca instytucji finansowych, zajmujących się udzielaniem pożyczek. Wprowadzono mianowicie nadzór Komisji Nadzoru Finansowego nad instytucjami pożyczkowymi[32] z możliwościami nakładania kar na członka zarządu do 150 tys. zł, a na instytucję pożyczkową do 15 mln zł bądź wykreślenie jej z rejestru. Ma to przeciwdziałać próbom nadmiernego, nieuzasadnionego wzbogacania się kosztem konsumentów.

Podatność sektora

[30] https://www.gov.pl/web/finanse/fundusze-inwestycyjne dostęp w dniu 13.01.1023 r.
[31] https://www.gov.pl/web/finanse/domy-i-biura-maklerskie dostęp w dniu 13.01.2023 r.
[32] Objęcie instytucji pożyczkowych pełnym nadzorem KNF, w rozumieniu przepisów ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim, nastąpi w dniu 1 stycznia 2024 r. W chwili obecnej KNF nie sprawuje pełnego nadzoru nad tymi instytucjami.

Zdecydowana większość podmiotów sektora innych instytucji finansowych (biorąc pod uwagę definicję z *rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 575/2013* oraz *ustawy z dnia 29 sierpnia 1997 r. - Prawo bankowe* są instytucjami obowiązanymi (IO). Podmioty te są zobowiązane do stosowania środków bezpieczeństwa finansowego, określonych w ustawie z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, choć wciąż ujawniane są podczas kontroli braki w tym obszarze. Wymienione w ustawie środki bezpieczeństwa finansowego obejmują przede wszystkim czynności związane z identyfikacją klienta oraz weryfikacją jego tożsamości; identyfikację beneficjenta rzeczywistego oraz podejmowanie uzasadnionych czynności w celu weryfikacji jego tożsamości oraz ustalenia struktury własności i kontroli w przypadku klienta będącego osobą prawną albo jednostką organizacyjną nieposiadającą osobowości prawnej. Ponadto podmioty sektora innych instytucji finansowych powinny dokonywać oceny stosunków gospodarczych klienta oraz (stosownie do sytuacji) uzyskiwać informacje na temat ich celu i zamierzonego charakteru. Na bieżąco też powinny monitorować stosunki gospodarcze swoich klientów. Duże instytucje obowiązane przedmiotowego sektora, jak biura maklerskie czy towarzystwa funduszy inwestycyjnych mają możliwości faktyczne rzeczywistego monitorowaniem transakcji swoich klientów. Podmioty przedmiotowego sektora innych instytucji finansowych posiadają świadomość swoich obowiązków z zakresu PPP/PFT. W zakresie usługi faktoringu, instrumentów rynku kapitałowego, kart prepaid, kredytów i pożyczek (w dziale instytucje finansowe), leasingu - w latach 2019-2021 GIIF otrzymał i zrealizował łącznie 33 sprawy analityczne, dotyczące transakcji podejrzanych. W 2019 r. było to ok. 1,4% wszystkich postępowań dotyczących podejrzenia prania pieniędzy lub finansowania terroryzmu w związku z wykorzystaniem do podejrzanych transakcji instytucji sektora innych instytucji finansowych, w 2020 r. ok. 3,1%, a w 2021 r. ok 1,5%.

Podmioty sektora innych instytucji finansowych są zobowiązane do wdrożenia skutecznych procedur, w tym, w stosownych przypadkach, dotyczących monitorowania ex-post lub w czasie rzeczywistym, w celu wykrycia braku informacji o stronach transakcji bądź czynności. U każdego podmiotu tego sektora muszą być określone skuteczne procedury, oparte na analizie ryzyka, umożliwiające stwierdzenie, czy wykonać, odrzucić lub wstrzymać konkretną usługę bądź transakcję, w przypadku których brakuje wymaganych informacji o stronach czynności bądź transakcji oraz podjęcie stosownych dalszych kroków.

W wyniku współpracy GIIF z organami ścigania te ostatnie często korzystają z informacji przechowywanych w bazach danych GIIF (przede wszystkim informacji finansowych). Na podstawie art. 106 ust. 1 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu w przypadku powzięcia podejrzenia popełnienia przestępstwa skarbowego lub innego przestępstwa niż przestępstwo prania pieniędzy lub finansowania terroryzmu GIIF przekazuje informacje uzasadniające to podejrzenie właściwym organom wskazanym w art. 105 ust. 1 i 4 tej ustawy w celu podjęcia czynności wynikających z ich ustawowych zadań. Natomiast w przypadku powzięcia uzasadnionego podejrzenia naruszenia przepisów związanych z funkcjonowaniem rynku finansowego GIIF przekazuje KNF informacje uzasadniające to podejrzenie.

Podmioty sektora innych instytucji finansowych nadzorowane przez KNF powinny (zgodnie z rekomendacjami UKNF), analizować dane dotyczące usług i transakcji oraz posiadać narzędzia do oceny dzienników zdarzeń. Z uwagi na koszty posiadania zaawansowanych, dedykowanych narzędzi informatycznych, nie wszystkie instytucje sektora innych instytucji

finansowych dysponują takimi zaawansowanymi, automatycznymi narzędziami i systemami informatycznymi, wspomagającymi realizację celów przeciwdziałania praniu pieniędzy oraz finansowania terroryzmu. Duże instytucje obowiązane przedmiotowego sektora, przeprowadzające najwięcej transakcji, jak biura maklerskie czy towarzystwa funduszy inwestycyjnych, dysponują takimi systemami.

W celu podnoszenia świadomości AML/CTF w instytucjach obowiązanych – w tym w sektorze innych instytucji finansowych, GIIF prowadził szkolenia zarówno dla instytucji obowiązanych, jak i jednostek współpracujących, podczas których były przekazywane teoretyczne i praktyczne wskazówki dotyczące przeciwdziałania praniu pieniędzy oraz finansowania terroryzmu. Istotnym tematem szkoleń był blok szkoleniowy dotyczący ustalania beneficjenta rzeczywistego oraz struktury własności i kontroli klientów a także raportowania rozbieżności do organu właściwego w sprawie CRBR. Ponadto dla przedmiotowych podmiotów sektora były także prowadzone szkolenia w innych aspektach AML/CTF, organizowane zarówno przez GIIF, jak i przez UKNF w ramach Programu CEDUR.

Podmioty sektora innych usług finansowych świadczące usługi bądź dokonujące transakcji w postaci usług na rynku finansowym Forex, handlu jednostkami funduszy inwestycyjnych oraz dokonujące transakcji na rachunkach papierów wartościowych i rachunkach pieniężnych służących do ich obsługi są podmiotami bądź licencjonowanymi, bądź podmiotami działającymi na podstawie uzyskanych zezwoleń, wydanych przez Komisję Nadzoru Finansowego.

W działalności podmiotów przedmiotowego sektora mogą występować kłopoty związane z pozyskaniem od klientów szerszego spektrum dokumentów potwierdzających tożsamość lub wiarygodność klienta. W związku z konfliktem na Ukrainie i obecnością w Polsce dużej liczby uchodźców występują poważne problemy z identyfikacją i weryfikacją osób. Występująca bariera językowa i kulturowa w istotny sposób wpływa na prawidłowe rozpoznanie czynników zwiększonego ryzyka. Taka bariera stanowi czynnik behawioralny, który utrudnia prawidłową ocenę odpowiedzi klientów-uchodźców w kwestiach problematycznych, które wymagają dodatkowych informacji czy dokumentów.

Zwraca uwagę stosunkowo niewielka ilość zawiadomień zgłaszanych przez podmioty sektora innych instytucji finansowych do GIIF.

W 2022 r. przeprowadzono w GIIF scoring oceny ryzyka domów i biur maklerskich za okres od I kwartału 2019 do II kwartału 2021 tj. 6 okresów sprawozdawczych. Wzięto pod uwagę dane dotyczące 30 biur i domów maklerskich. Scoring obejmował badanie pod takimi kryteriami jak: udział klientów niskiego ryzyka w ogólnej liczbie klientów; udział PEP-ów w ogólnej liczbie klientów; udział beneficjentów rzeczywistych o statusie PEP w ogólnej liczbie klientów będących PEP. Siedem z biur i domów maklerskich (na 30) pod względem wyżej wymienionych kryteriów zostało uznanych za instytucje, w których ryzyko jest wysokie bądź średnio-wysokie. Sześć z biur i domów maklerskich zostało odpowiednio ocenionych jako takie, w których ryzyko było niskie, natomiast pozostałe siedemnaście biur i domów maklerskich zostały zakwalifikowanych pod względem wyżej wymienionych kryteriów jako instytucje, w których ryzyko było średnie. Podobny scoring przeprowadzono dla Towarzystw Funduszy Inwestycyjnych. Wzięto pod uwagę dane dotyczące 50 TFI. Przyjęte kryteria oceny ryzyka dla TFI były takie same, jak dla domów i biur maklerskich. Siedem z TFI (na 50) pod względem wyżej wymienionych kryteriów zostało uznanych za instytucje, w których ryzyko

jest wysokie bądź średnio-wysokie. Piętnaście z ocenianych TFI zostało odpowiednio ocenionych jako takie, w których ryzyko było niskie, natomiast pozostałe dwadzieścia osiem TFI zostały zakwalifikowanych pod względem wyżej wymienionych kryteriów jako instytucje, w których ryzyko było średnie.

Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w zakresie przedmiotowego sektora. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek ML czy FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców.

Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie.

Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.

Zagrożenia w sektorze

Sektor usług świadczonych przez inne instytucje finansowe pod względem oceny zagrożenia praniem pieniędzy, ale też zagrożenia finansowania terroryzmu, jest sektorem potencjalnie mogącym być wykorzystanym w związku z przestępstwami źródłowymi dla prania pieniędzy oraz finansowania terroryzmu: przestępstwami skarbowymi, handlu narkotykami, przestępstwami przeciwko mieniu oraz przeciwko obrotowi gospodarczemu, korupcji, handlu ludźmi czy oszustwami. Stopień skomplikowania rynku kapitałowego oraz rynku pieniężnego jest dużym atutem dla przestępczej działalności mającej na celu przede wszystkim pranie pieniędzy. Organy ścigania nie dysponują wieloma fachowcami na najwyższym poziomie wiedzy i doświadczenia na tych rynkach, a szybkość dokonywanych na rynku kapitałowym oraz rynku pieniężnym transakcji, wielokrotna możliwość zamiany środków finansowych na instrumenty finansowe po różnych kursach powoduje zaciemnianie obrazu transakcji jako przestępstwa bazowego bądź przestępstwa prania pieniędzy, gdy środki pochodzą z czynu zabronionego.

Pomimo, że inwestowanie na rynku Forex jest legalne, to zauważalny jest wyraźny wzrost liczby przestępstw z wykorzystaniem tego rynku. Przestępstwa te polegają przede wszystkim na oszukańczym działaniu podmiotów pośredniczących w inwestowaniu. Przestępcy często działają w zorganizowanej grupie przestępczej[33]. Jest wiele wariantów wyłudzeń. Dokonujący przestępstwa świadczą doradztwo inwestycyjne, rekomendują realizację transakcji na rynku Forex za pośrednictwem platform inwestycyjnych, zarządzają też niekiedy portfelami klientów. Różne scenariusze tego typu wyłudzeń łączą wspólne elementy, które mają zachęcić klientów do szybkiego zarobku. Należy tu zapewnianie o możliwości szybkich i wysokich zysków rynku Forex; gwarancja zysku dla „każdego"; pomoc „brokera" i konieczność pierwszej wpłaty (tzw. opłaty rejestracyjnej); konieczność instalacji aplikacji (na komputerze lub telefonie), która umożliwia automatyzację operacji związanej z operacjami na rynku Forex; konieczność przesłania „brokerowi" skanów (zdjęć) dokumentu tożsamości, selfie z dokumentem tożsamości czy bieżącego rachunku w celu potwierdzenia tożsamości. Przestępcy mogą również informować, że będą wypłacać zwrot z inwestycji bezpośrednio na kartę klienta. Proszą pod tym pretekstem o podanie szczegółowych danych karty. Na wyłudzone dane

[33] Informacja Komendy Głównej Policji i FinCERT.pl – Bankowego Centrum Cyberbezpieczeństwa ZBP o zagrożeniu związanym z ofertami inwestycji na rynku Forex i kryptowalut z dnia 24.03 2021 r.

osobowe brane są pożyczki i kredyty, np. przez internet, a czasem klient podmiotu pośredniczącego w inwestowaniu na rynku Forex nieświadomie zostaje włączony w działalność przestępczą. Podczas niektórych ataków przestępcy wykorzystują pokrzywdzonego do procederu prania pieniędzy pochodzących z przestępstw (w transferze środków pochodzących z oszustw u innego poszkodowanego):

- nakłaniają do przelania inwestowanych środków na konta innych osób. Ma to im ułatwić kontynuację inwestowania w związku z rzekomymi działaniami prewencyjnymi podejmowanymi przez niektóre banki;
- w tym samym celu uzgadniają z niektórymi klientami, że na ich rachunek w banku wpłyną środki od innej osoby dla późniejszego przekazania ich dalej. Dzięki temu pokrzywdzony rzekomo będzie mógł łatwiej uzyskać zysk ze swoich „inwestycji" lub odrobić straty.

Pranie pieniędzy może również mieć miejsce w szczególności w przypadku kontrolowania brokera przez przestępców i realizacji zleceń składanych przez przestępców lub na podstawione przez nich osoby. Operacje finansowe na instrumentach finansowych rynku Forex wykazywane są wtedy jako zysk z inwestycji na tym rynku.

Papiery wartościowe mogą być przedmiotem transakcji realizowanych zarówno w ramach obrotu zorganizowanego, jak również poza nim. Rynek papierów wartościowych jest rynkiem globalnym, tym rynkiem, który odgrywa kluczową rolę w światowej gospodarce. Jego uczestnikami są wielonarodowe, mające wiele biur firmy finansowe, zatrudniające wiele tysięcy osób, a z drugiej strony uczestnikami tego rynku są jednoosobowe biura oferujące usługi maklerskie lub doradztwo finansowe.

Za pośrednictwem sektora rynku papierów wartościowych (ale także inwestowania w jednostki funduszy inwestycyjnych) osoby i podmioty mogą uzyskać dostęp do systemu finansowego, co stwarza przestępcom okazję do nadużycia tego systemu. Na tym rynku w ofercie biur maklerskich czy firm inwestycyjnych pojawiają się i są rozwijane wciąż nowe produkty i usługi. Te nowe produkty wymusza zapotrzebowanie inwestorów, warunki rynkowe oraz dynamiczny postęp technologiczny. Dla zagrożeń związanych z praniem pieniędzy na tym rynku znaczenie ma złożoność samych oferowanych produktów. Niektóre z usług i produktów są przeznaczone do sprzedaży dla ogółu społeczeństwa, a inne są dostosowane do potrzeb pojedynczego nabywcy. Transakcje dokonywane są przede wszystkim drogą elektroniczną i ponad granicami narodowymi. Charakterystyczne dla rynku papierów wartościowych cechy, takie jak szybkość wykonywania transakcji, globalny zasięg i zdolność adaptacji, czynią ten rynek atrakcyjnym dla przestępców, którzy wykorzystają go do nielegalnych celów, w tym do prania pieniędzy i finansowania terroryzmu. Co więcej, sektor papierów wartościowych jest o tyle wyjątkowy wśród branż, ponieważ może być wykorzystywany zarówno do prania środków pochodzących z przestępstw popełnionych gdzie indziej, jak i do popełniania przestępstw źródłowych poprzez oszukańcze działania na rynku papierów wartościowych. Same transakcje i techniki związane z jednej strony z praniem pieniędzy, a z drugiej strony przestępstwami źródłowymi dotyczącymi papierów wartościowych są często trudne do odróżnienia. W praktyce GIIF posiada pewne informacje o wykorzystywaniu przez przestępców rachunków papierów wartościowych i rachunków pieniężnych służących do ich obsługi do prania pieniędzy. Na przykład proceder prania pieniędzy związany jest z funkcjonującym domniemaniem, że środki, które znajdują się na rachunku pieniężnym

służącym obsłudze rachunku papierów wartościowych, pochodzą z operacji finansowych dokonywanych na giełdzie. Tym samym wszystkie wpłaty na rachunek pieniężny służący do obsługi rachunku papierów wartościowych, a następnie różne formy operacji inwestycyjnych tymi środkami bądź wypłata lub przelew na inny rachunek jest pozorowaniem legalnego pochodzenia wartości majątkowych, które zostały wcześniej uzyskane w wyniku działalności przestępczej.

Sporym zagrożeniem z punktu widzenia prania pieniędzy oraz finansowania terroryzmu może być inwestowanie w fundusze inwestycyjne zamknięte (FIZ) - posiadacz certyfikatów posiada je anonimowo, może dokonywać obrotu nimi bez wiedzy organów podatkowych, organów nadzoru nad rynkiem kapitałowym. Za pośrednictwem FIZ nabywane mogą być udziały, akcje, nieruchomości, a dochody generowane przez FIZ (z pewnymi wyjątkami) nie są opodatkowane.

W aspekcie finansowania terroryzmu wykorzystanie do celów finansowania terroryzmu produktów i usług finansowych w postaci usług na rynku finansowym Forex, jednostek funduszy inwestycyjnych oraz rachunków papierów wartościowych i rachunków pieniężnych służących do ich obsługi ma wspólne cechy, polegające na tym, że wymienione modus operandi wymagają jednak specjalistycznej wiedzy o rynku walutowym czy kapitałowym oraz umiejętności i planowania. GIIF nie miał jak dotąd skonkretyzowanych informacji o inwestowaniu nielegalnych bądź legalnych środków finansowych w fundusze inwestycyjne w celu finansowania terroryzmu w sektorze innych instytucji finansowych. Stopień skomplikowania rynku Forex oraz rynku papierów wartościowych powoduje stosunkowo niską atrakcyjność tej formy finansowania działalności terrorystycznej.

Uśredniony poziom zagrożenia sektora innych instytucji finansowych – ML – 2,2 i FT – 1

Uśredniony poziom podatności sektora innych instytucji finansowych – ML – 2,0 i FT – 2

Oszacowany poziom prawdopodobieństwa dla sektora – ML – 2,08 i FT - 1,60

Poziom ryzyka jest ostatecznie określany przez kombinację zagrożenia i podatności. Macierz ryzyka określająca ten poziom ryzyka opiera się na wadze 40% (zagrożenie) + 60% (podatność) – przy założeniu, że komponent podatności ma większą zdolność określania poziomu ryzyka. Zakłada się, że poziom podatności może zwiększyć atrakcyjność, a tym samym zamiary przestępców/terrorystów, aby użyć danego modus operandi – wpływając w ten sposób ostatecznie na poziom zagrożenia. Poziom ryzyka sektora, z uwzględniem prawdopobieństwa i konsekwencji (współczynnik 2,5 dla PP i 1,5 dla FT), jest ustalany zgodnie z metodyką krajowej oceny ryzyka – aneks nr 1.

Ryzyko FT sektora innych instytucji finansowych – 1,56	
1 – 1,5	Niskie
1,6 – 2,5	Średnie
2,6 – 3,5	Wysokie

3,6 – 4	Bardzo wysokie
Ryzyko ML sektora innych instytucji finansowych – 2,25	
1 – 1,5	Niskie
1,6 – 2,5	Średnie
2,6 – 3,5	Wysokie
3,6 – 4	Bardzo wysokie

WNIOSEK 1: Poziom ryzyka wykorzystania sektora innych instytucji finansowych do finansowania terroryzmu w Polsce znajduje się na poziomie niskim.

WNIOSEK 2: Poziom ryzyka wykorzystania sektora innych instytucji finansowych do prania pieniędzy w Polsce znajduje się na poziomie średnim.

Mitygacja zidentyfikowanych ryzyk:

W celu ograniczenia prawdopodobieństwa wykorzystania sektora innych instytucji finansowych do prania pieniędzy lub finansowania terroryzmu, zasadne jest podjęcie odpowiednich działań. Stosowanie zaproponowanych działań mitygujących powinno następować z uwzględnieniem rozpoznanego przez danę instytucję obowiązaną ryzyka.

Podmioty sektora innych instytucji finansowych powinny doskonalić podejmowane działania związane z odpowiednią oceną stosunków gospodarczych klienta oraz uzyskiwaniem informacji na temat ich celu i zamierzonego charakteru, a także powinny utrzymywać bieżący monitoring stosunków gospodarczych.

W sektorze innych instytucji finansowych powinny być podejmowane działania podnoszące świadomość narażenia na przestępstwo prania pieniędzy oraz finansowania terroryzmu, jak również podnoszące poziom wyszkolenia pracowników tego sektora w analizie sygnałów ostrzegawczych wynikających z transakcji podejrzanych.

Kontynuowane powinny być szkolenia dla instytucji obowiązanych z sektora innych instytucji finansowych, podczas których będą przekazywane teoretyczne i praktyczne wskazówki dotyczące ustalania beneficjenta rzeczywistego oraz struktury własności i kontroli klientów a także raportowania rozbieżności do organu właściwego w sprawie CRBR. Zalecane jest

uczestnictwo przedstawicieli instytucji obowiązanych w szkoleniach podnoszących świadomość AML/CTF, organizowanych zarówno przez GIIF, jak i przez UKNF w ramach Programu CEDUR.

Instytucje obowiązane z sektora innych instytucji finansowych powinny zwracać szczególną uwagę na transfery środków do jurysdykcji charakteryzujących się wyższym ryzykiem prania pieniędzy oraz finansowania terroryzmu. Instytucje obowiązane powinny położyć szczególny nacisk na ustalenie danych dotyczących źródła pochodzenia transferowanych wartości majątkowych, jak również dokumentów wskazujących na uzasadnienie przeprowadzenia danej transakcji.

Instytucje obowiązane powinny przykładać szczególną wagę do czynników geograficznych mogących wskazywać na wyższe ryzyko prania pieniędzy czy też finansowania terroryzmu, takich jak niestabilna sytuacja polityczna czy konflikt zbrojny, czego najdobitniejszym przykładem w ostatnich latach jest wojna prowadzona przez Rosję przeciwko Ukrainie. Z uwagi na wysokie ryzyko transferowania środków pochodzących z nielegalnego handlu, przemytu ludzi, handlu bronią, czy też działań zmierzających do omijania sankcji gospodarczych, szczególnie istotne jest analizowanie przez instytucje obowiązane nie tylko danych dotyczących samych stron transakcji, ale również beneficjentów rzeczywistych, czy też faktycznych celów przeprowadzania danych transakcji.

Podmioty świadczące usługi faktoringu powinny zwracać szczególną uwagę na weryfikację źródła pochodzenia wartości majątkowych, co w przypadku usługi faktoringu powinno obejmować weryfikację podstawy wystawienia faktur przez klienta instytucji obowiązanej. Bieżące monitorowanie stosunków gospodarczych oraz weryfikacja źródła pochodzenia wartości majątkowych, może również obejmować analizę stosunków gospodarczych pomiędzy klientem a jego kontrahentami.

Z uwagi na charakter działalności prowadzonej przez instytucje obowiązane z sektora innych instytucji finansowych, kluczowe jest uzyskiwanie wiedzy na temat charakteru stosunków gospodarczych prowadzonych przez klientów, a także źródła pochodzenia wartości majątkowych, będących w dyspozycji klienta.

5. Obszar – wymiana walut

Opis sektora – zawarty jest w podrozdziale 2.1.2. KOR „Sektory rynku finansowego” oraz w podrozdziale 7.2.1 „Podatność rynku finansowego”.

Scenariusze wystąpienia ryzyka (tj. możliwe przykłady wystąpienia ryzyka) zarówno w przypadku prania pieniędzy, jak i finansowania terroryzmu - dotyczyły wykorzystania do

prania pieniędzy i finansowania terroryzmu produktów finansowych w postaci gotówkowej wymiany walut, wymiany pieniędzy w ramach jednej waluty oraz usługi podmiotów oferujących bezgotówkową wymianę walut. Ich opis znajduje się poniżej.

Pranie pieniędzy

Tabela 26

Rodzaj wykorzystanych usług, produktów finansowych	Gotówkowa wymiana walut
Ogólny opis ryzyka	Wymiana waluty w celu utrudnienia identyfikacji pieniędzy pochodzących z przestępstwa
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Korzystanie przez przestępców z gotówkowej wymiany walut w kantorach w celu utrudnienia organom ścigania odtworzenia ścieżki transferu wartości majątkowych. Korzystanie z "zaufanych" kantorów, nieraportujących transakcji podejrzanych do jednostki analityki finansowej. 2. Wymiana w kantorach zgromadzonych pieniędzy pochodzących z nielegalnych źródeł na wysokie nominały w innych walutach (powszechnie wymienianych na całym świecie, np. EUR), celem łatwiejszego ich transportowania przez granice państwowe.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Dostęp do tego typu usług jest relatywnie łatwy. Istnieją możliwości ukrycia danych identyfikacyjnych klientów (podmioty oferujące tego typu usługi dokonują głównie transakcji na okaziciela. Identyfikacja klienta i jego weryfikacja w lokalu ma miejsce w każdym przypadku stosowania środków bezpieczeństwa finansowego – transakcji o równowartości 15 000 euro i większej). Organy administracji publicznej posiadają podstawową wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwości gromadzenia i analizowania informacji dot. tego typu usług, jednak pochodzących od podmiotów będących IO albo udostępnionych przez zagraniczną jednostkę analityki finansowej. Istnieje prawdopodobieństwo, że przypadek prania pieniędzy w zakresie analizowanych scenariuszy nie zostanie wykryty. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają częściowo zakresowi analizowanego ryzyka.
Poziom zagrożenia	3
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie mechanizmu wymiany waluty w celu utrudnienia identyfikacji pieniędzy pochodzących z przestępstwa jest jedną z częściej używanych metod prania pieniędzy. Jest to sposób łatwy, szeroko dostępny, jego zastosowanie niewiele kosztuje i jest postrzegany przez sprawców raczej jako atrakcyjny. Transakcje wymiany walut poniżej progu rejestracji nie wzbudzają podejrzeń, zwłaszcza gdy pracownicy np. kantoru współpracują z przestępcami. Wysoki wolumen obrotów kantoru pozwala ukryć wymianę nielegalnych środków wśród legalnych transakcji. GIIF otrzymywał informacje o wykorzystaniu tej metody do prania pieniędzy, zwłaszcza w powiązaniu z innymi metodami. WNIOSEK: Wykorzystanie mechanizmu wymiany waluty w celu utrudnienia identyfikacji pieniędzy pochodzących z przestępstwa stwarza wysokie zagrożenie prania pieniędzy.

Tabela 27

Rodzaj wykorzystanych usług, produktów finansowych	Wymiana pieniędzy w ramach jednej waluty
Ogólny opis ryzyka	Wymiana pieniędzy o niskich nominałach na banknoty o wyższej wartości
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia	Wymiana banknotów EUR o niskich nominałach na banknoty o nominale 500 EUR lub 200 EUR w celu zmniejszenia objętości przenoszonych środków

ryzyka)	pieniężnych[34].
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Dostęp do tego typu usług wymiany walut jest utrudniony i uzależniony od posiadania przez IO banknotów o takim nominale. Łatwe jest ukrycie danych identyfikacyjnych dokonującego transakcji, zwłaszcza jeśli poszczególne transakcje są przeprowadzane w relatywnie niewielkich kwotach. Brak możliwości realizacji transakcji o charakterze międzynarodowym. Wszystkie podmioty oferujące te usługi są IO. Posiadają one świadomość swoich obowiązków z zakresu PPP/PFT. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek prania pieniędzy w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają zakresowi analizowanego ryzyka.
Poziom zagrożenia	3
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie mechanizmu wymiany pieniędzy o niskich nominałach na banknoty o wyższej wartości jest jedną z często używanych metod prania pieniędzy. Dokonuje się tego typu operacji w bankach, kantorach, ale także na poczcie. Jest to sposób szeroko dostępny, jego zastosowanie niewiele kosztuje i jest postrzegany przez sprawców jako atrakcyjny. Jednakże bezpieczeństwo tej metody wymaga zaplanowania, przestrzegania reguły dokonywania niskich kwotowo operacji. Bowiem wymiana pogniecionych, często brudnych banknotów o niskich nominałach może łatwo zwrócić uwagę. Najczęściej metoda ta wymaga współpracy pracowników zatrudnionych w instytucjach zajmujących się tego typu usługami. GIIF otrzymywał informacje o wykorzystaniu tej metody do prania pieniędzy. WNIOSEK: Wykorzystanie mechanizmu wymiany pieniędzy o niskich nominałach na banknoty o wyższej wartości stwarza wysokie zagrożenie prania pieniędzy.

Tabela 28

Rodzaj wykorzystanych usług, produktów finansowych	Usługi podmiotów oferujących bezgotówkową wymianę walut
Ogólny opis ryzyka	Bezgotówkowa wymiana waluty połączona z transferem środków
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Korzystanie przez przestępców z bezgotówkowej wymiany walut w tzw. kantorach internetowych w celu utrudnienia organom ścigania odtworzenia ścieżki transferu wartości majątkowych. Przykładowo - środki w PLN są transferowane na rzecz tzw. kantoru internetowego z rachunku bankowego prowadzonego w jednej instytucji ze zleceniem ich wymiany na USD i przekazania na rachunek prowadzony w innym banku, należący w rzeczywistości do innego podmiotu niż zleceniodawca. 2. Przelew środków pieniężnych (pochodzących z przestępstwa) do kantoru internetowego z konta osoby fizycznej będącej ofiarą nieautoryzowanego dostępu do jej rachunku.
Poziom podatności	3

[34] Europejski Bank Centralny zakończył emisję banknotu 500 EUR w dniu 27.04.2019r. Głównym powodem zakończenia emisji ww. banknotu były obawy, że banknoty te są często wykorzystywane w działalności przestępczej. Banknot 500 EUR, tak jak reszta nominałów, bezterminowo zachował swoją wartość i bez ograniczeń podlega wymianie w krajowych bankach centralnych.

Uzasadnienie dla poziomu podatności	Dostęp do usług wymiany walut jest bardzo łatwy. Łatwe jest ukrycie danych identyfikacyjnych dokonującego transakcji, zwłaszcza jeśli poszczególne transakcje są przeprowadzane w relatywnie niewielkich kwotach. Istnieje możliwość realizacji transakcji o charakterze międzynarodowym w przypadku realizacji takich transakcji przynajmniej częściowo w formie bezgotówkowej. Występują też problemy z weryfikacją zagranicznych klientów w centralnych rejestrach beneficjentów rzeczywistych państw UE, zwłaszcza dotyczy to podmiotów o skomplikowanej strukturze kapitałowej. Wszystkie podmioty oferujące te usługi są IO. Posiadają one pewną świadomość swoich obowiązków z zakresu PPP/PFT. Relatywnie mało informacji o podejrzanych transakcjach/podejrzanej działalności przekazywanych jest przez podmioty zajmujące się wymianą walut. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek prania pieniędzy w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w części zakresowi analizowanego ryzyka.
Poziom zagrożenia	4
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie mechanizmu bezgotówkowej wymiany walut w tzw. kantorach internetowych połączonej z transferem środków dla utrudnienia organom ścigania odtworzenia ścieżki transferu wartości majątkowych jest zidentyfikowaną metodą umożliwiającą pranie pieniędzy. Obecnie kantory internetowe nie są regulowane prawnie. Nie podlegają żadnej ustawie ani jednemu organowi, które by ustanowiły ich zakres działania. Działalność w zakresie internetowej wymiany walut nie podlega nadzorowi KNF. Nadzorowi KNF podlegać może świadczenie usług płatniczych w związku z taką działalnością, co wymaga uzyskania stosownych uprawnień. Według szacunków raportu firmy Accenture[35] w 2019 roku wielkość obrotów na rynku walutowym (z pominięciem transakcji międzybankowych oraz transakcji terminowych) w Polsce szacowało się na niecały 1 bln PLN. W ciągu trzech kolejnych lat, prognozowany był wzrost o około 86 mld PLN. Wyraźny spadek dynamiki wzrostu wynika z kryzysu gospodarczego, zapoczątkowanego przez wybuch pandemii COVID-19. Bezgotówkowa wymiana waluty połączona z transferem środków stosunkowo niewiele kosztuje i jako *modus operandi* może być postrzegana przez sprawców jako atrakcyjny i szeroko dostępny sposób dla prania pieniędzy. W warunkach dynamicznego wzrostu obrotu gospodarczego prowadzonego przez przedsiębiorstwa, zajmujące się eksportem bądź importem, transakcje wymiany bezgotówkowej w kantorach internetowych mogą być relatywnie niewidoczne dla nadzoru (zwłaszcza przy braku jasnych uregulowań prawnych). GIIF otrzymywał bardzo nieliczne informacje o możliwości wykorzystania tej metody do prania pieniędzy. Zastosowanie tego *modus operandi* wymaga planowania, wiedzy i umiejętności raczej na niskim poziomie zaawansowania. Może on być postrzegany przez sprawców jako dość atrakcyjny i bezpieczny. GIIF otrzymywał informacje o wykorzystaniu tej metody do prania pieniędzy. WNIOSEK: Wykorzystanie mechanizmu bezgotówkowej wymiany walut w tzw. kantorach internetowych połączonej z transferem środków stwarza bardzo wysokie zagrożenie prania pieniędzy.

Finansowanie terroryzmu

[35] Raport RYNEK WYMIANY WALUT W POLSCE https://www.accenture.com › _acnmedia › PDF-125

Tabela 29

Rodzaj wykorzystanych usług, produktów finansowych	Gotówkowa wymiana walut
Ogólny opis ryzyka	Wymiana waluty w celu utrudnienia identyfikacji przestępstwa finansowania terroryzmu
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Korzystanie przez osoby powiązane z organizacjami terrorystycznymi z wymiany walut w kantorach (np. wymiana z USD na EUR) w celu utrudnienia organom ścigania odtworzenia ścieżki transferu wartości majątkowych. Korzystanie z "zaufanych" kantorów, nieraportujących transakcji podejrzanych do właściwej jednostki analityki finansowej. 2. Wymiana zgromadzonych pieniędzy (np. zebranych od zwolenników) na wysokie nominały w innych walutach (powszechnie wymienianych na całym świecie, np. EUR) w kantorach, celem łatwiejszego ich transportowania przez granice państwowe.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Dostęp do usług wymiany walut jest bardzo łatwy. Łatwe jest ukrycie danych identyfikacyjnych dokonującego transakcji, zwłaszcza jeśli poszczególne transakcje są przeprowadzane w relatywnie niewielkich kwotach. W wielu wypadkach utrudniona jest prawidłowa identyfikacja i weryfikacja tożsamości uchodźców z Ukrainy. Wszystkie podmioty oferujące te usługi są IO. Posiadają one świadomość swoich obowiązków z zakresu PPP/PFT. Relatywnie mało informacji o podejrzanych transakcjach/podejrzanej działalności przekazywanych jest przez podmioty zajmujące się wymianą walut[36]. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają zakresowi analizowanego ryzyka.
Poziom zagrożenia	2
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie mechanizmu wymiany waluty w celu utrudnienia identyfikacji przestępstwa finansowania terroryzmu jest sposobem stosunkowo łatwym do realizacji i szeroko dostępnym. Jego zastosowanie niewiele kosztuje i jest postrzegany przez sprawców raczej jako atrakcyjny, zwłaszcza że środki mogą pochodzić z zupełnie legalnych źródeł. Transakcje wymiany walut poniżej progu rejestracji z reguły nie wzbudzają podejrzeń. Wysoki wolumen obrotów kantoru pozwala ukryć wymianę nielegalnych bądź legalnych środków wśród zupełnie legalnych jednostkowych transakcji. Brak jest informacji o prowadzeniu kantorów przez podmioty powiązane z osobami podejrzanymi o terroryzm bądź FTF. GIIF otrzymywał bardzo nieliczne informacje o możliwości wykorzystania tej metody do finansowania działalności terrorystycznej. WNIOSEK: Wykorzystanie mechanizmu wymiany waluty w celu utrudnienia identyfikacji przestępstwa finansowania terroryzmu stwarza średnie zagrożenie finansowaniem terroryzmu..

Tabela 30

Rodzaj wykorzystanych usług, produktów finansowych	Wymiana pieniędzy w ramach jednej waluty

[36] Nie biorąc pod uwagę banków, świadczących usługę wymiany walut, również online.

Ogólny opis ryzyka	Wymiana pieniędzy o niskich nominałach na banknoty o wyższej wartości
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	Wymiana banknotów EUR o niskich nominałach na banknoty o nominale 200 EUR w celu zmniejszenia objętości przenoszonych środków pieniężnych.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Dostęp do usług wymiany walut jest bardzo łatwy. Stosunkowo łatwe jest ukrycie danych identyfikacyjnych dokonującego transakcji, zwłaszcza jeśli poszczególne transakcje są przeprowadzane w relatywnie niewielkich kwotach. W wielu wypadkach utrudniona jest prawidłowa identyfikacja i weryfikacja tożsamości uchodźców z Ukrainy. Istnieje możliwość realizacji transakcji o charakterze międzynarodowym w przypadku realizacji takich transakcji przynajmniej częściowo w formie bezgotówkowej. Wszystkie podmioty oferujące te usługi są IO. Posiadają one świadomość swoich obowiązków z zakresu PPP/PFT. Relatywnie mało informacji o podejrzanych transakcjach/podejrzanej działalności przekazywanych jest przez podmioty zajmujące się wymianą walut[37]. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają zakresowi analizowanego ryzyka.
Poziom zagrożenia	2
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie mechanizmu wymiany pieniędzy o niskich nominałach na banknoty o wyższej wartości w celu finansowania terroryzmu jest sposobem szeroko dostępnym, a jego zastosowanie niewiele kosztuje. Może być on postrzegany przez sprawców jako atrakcyjny. Fizyczne przenoszenie banknotów przeznaczonych na cele finansowania terroryzmu nie powinno zwracać uwagi, a zmniejszenie objętości przewożonej gotówki zmniejsza zagrożenie jej wykrycia bądź przypadkowej utraty. Pomimo ogłoszenia decyzji o wycofaniu banknotu 500 euro (od maja 2019 r. obowiązuje zakaz drukowania tych banknotów przez kraje strefy EURO), nie odnotowano w państwach członkowskich UE większego popytu na te banknoty ze strony grup terrorystycznych, które preferują banknoty o niskich nominałach. Jednakże bezpieczeństwo tej metody wymaga zaplanowania, przestrzegania reguły dokonywania niskich kwotowo operacji. Bowiem wymiana pogniecionych, często brudnych banknotów o niskich nominałach może łatwo zwrócić uwagę. Najczęściej metoda ta wymaga współpracy pracowników zatrudnionych w instytucjach typu bank bądź kantor. GIIF otrzymywał bardzo nieliczne informacje o możliwości wykorzystania tej metody do finansowania działalności terrorystycznej. WNIOSEK: Wykorzystanie mechanizmu wymiany pieniędzy o niskich nominałach na banknoty o wyższej wartości stwarza średnie zagrożenie finansowaniem terroryzmu.

Tabela 31

Rodzaj wykorzystanych usług, produktów finansowych	Usługi podmiotów oferujących bezgotówkową wymianę walut
Ogólny opis ryzyka	Bezgotówkowa wymiana waluty połączona z transferem środków

[37] Nie biorąc pod uwagę banków, świadczących usługę wymiany walut, również online.

Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	Korzystanie przez osoby powiązane z organizacjami terrorystycznymi z bezgotówkowej wymiany walut w tzw. kantorach internetowych w celu utrudnienia organom ścigania odtworzenia ścieżki transferu wartości majątkowych. Przykładowo - środki w PLN są transferowane na rzecz tzw. kantoru internetowego z rachunku bankowego prowadzonego w jednej instytucji ze zleceniem ich wymiany na USD i przekazania na rachunek prowadzony w innym banku, należącego w rzeczywistości do innego podmiotu niż zleceniodawca.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Dostęp do usług wymiany walut jest bardzo łatwy. Łatwe jest ukrycie danych identyfikacyjnych dokonującego transakcji, zwłaszcza jeśli poszczególne transakcje są przeprowadzane w relatywnie niewielkich kwotach. Istnieje możliwość realizacji transakcji o charakterze międzynarodowym w przypadku realizacji takich transakcji przynajmniej częściowo w formie bezgotówkowej. Występują też problemy z weryfikacją zagranicznych klientów w centralnych rejestrach beneficjentów rzeczywistych państw UE, zwłaszcza dotyczy to podmiotów o skomplikowanej strukturze kapitałowej. Wszystkie podmioty oferujące te usługi są IO. Posiadają one pewną świadomość swoich obowiązków z zakresu PPP/PFT. Relatywnie mało informacji o podejrzanych transakcjach/podejrzanej działalności przekazywanych jest przez podmioty zajmujące się wymianą walut. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w części zakresowi analizowanego ryzyka[38].
Poziom zagrożenia	2

[38] Trwają prace nad projektem ustawy o zmianie *ustawy - Prawo dewizowe* oraz niektórych innych ustaw, w zakresie objęcia nadzorem podmioty wymieniające waluty bezgotówkowo. Zgodnie z jego założeniami „transakcje bezgotówkowej wymiany walut, dokonywane przez kantory internetowe oraz transakcje gotówkowo-bezgotówkowej wymiany walut" mają podlegać przepisom *ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych*. Jednak już teraz część podmiotów oferujących jednocześnie bezgotówkową wymianę walut i usługi płatnicze podlega nadzorowi KNF.

Uzasadnienie dla poziomu zagrożenia	Wykorzystanie mechanizmu bezgotówkowej wymiany walut w tzw. kantorach internetowych połączonej z transferem środków dla utrudnienia organom ścigania odtworzenia ścieżki transferu wartości majątkowych jest zidentyfikowaną metodą umożliwiającą finansowanie terroryzmu. Obecnie kantory internetowe nie są regulowane prawnie. Nie podlegają żadnej ustawie ani jednemu organowi, które by ustanowiły ich zakres działania. Działalność w zakresie internetowej wymiany walut nie podlega nadzorowi KNF. Nadzorowi KNF podlegać może świadczenie usług płatniczych w związku z taką działalnością, co wymaga uzyskania stosownych uprawnień. Według szacunków raportu firmy Accenture[39] w 2019 roku wielkość obrotów na rynku walutowym (z pominięciem transakcji międzybankowych oraz transakcji terminowych) w Polsce szacowało się na niecały 1 bln PLN. W ciągu trzech kolejnych lat, prognozowany był wzrost o około 86 mld PLN. Wyraźny spadek dynamiki wzrostu wynika z kryzysu gospodarczego, zapoczątkowanego przez wybuch pandemii COVID-19. Bezgotówkowa wymiana waluty połączona z transferem środków stosunkowo niewiele kosztuje i jako *modus operandi* może być postrzegana przez sprawców jako atrakcyjny i szeroko dostępny sposób dla finansowania terroryzmu. W warunkach dynamicznego wzrostu obrotu gospodarczego prowadzonego przez przedsiębiorstwa, zajmujące się eksportem bądź importem, transakcje wymiany bezgotówkowej w kantorach internetowych mogą być relatywnie niewidoczne dla nadzoru (zwłaszcza przy braku jasnych uregulowań prawnych). GIIF otrzymywał bardzo nieliczne informacje o możliwości wykorzystania tej metody do finansowania działalności terrorystycznej. WNIOSEK: Wykorzystanie mechanizmu bezgotówkowej wymiany walut w tzw. kantorach internetowych połączonej z transferem środków stwarza średnie zagrożenie finansowaniem terroryzmu.

Usługi wymiany walut oferowane są w Polsce przede wszystkim przez stacjonarne kantory wymiany walut, prowadzące działalność regulowaną w rozumieniu przepisów *ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców*, wpisane do rejestru działalności kantorowej prowadzonego przez Prezesa Narodowego Banku Polskiego. Działalność kantorowa jest regulowaną działalnością gospodarczą polegającą na kupnie i sprzedaży wartości dewizowych oraz pośrednictwie w ich kupnie i sprzedaży. Z uwagi jednak na rozwój technologii internetowych do kantorów stacjonarnych w usłudze wymiany walut dołączyły kantory internetowe, które zaczęły zdobywać popularność dzięki innowacyjnym rozwiązaniom, oferując swoim klientom bezgotówkową i natychmiastową wymianę walut. W podobnym kierunku podążyły banki, które rozwinęły własne, przyjazne dla użytkowników platformy walutowe. Z prawnego punktu widzenia jednak działalność polegająca na świadczeniu usług wymiany walut na odległość, z wykorzystaniem Internetu do zawierania umów, zaś przelewów bankowych do przyjmowania od klientów i dostarczania klientom środków pieniężnych, nie stanowi działalności kantorowej w rozumieniu *ustawy z dnia 27 lipca 2002 r. – Prawo dewizowe.* W ostatnim czasie coraz większą popularność zyskują jednak fintechy, które charakteryzują się nowoczesnym podejściem do wymiany walut, oferując swoim klientom wygodne w użyciu aplikacje i rozwiązania. Oprócz wymiany walut wraz z dodatkowymi usługami ofertę fintechów uzupełniają wielowalutowe karty pre-paid. Według posiadanych danych w 2020 r. obroty na rynku wymiany walut wyniosły szacunkowo niemal bilion[40] złotych rocznie, a wartość tych obrotów cały czas rośnie.

[39] Raport RYNEK WYMIANY WALUT W POLSCE https://www.accenture.com › _acnmedia › PDF-125

[40] https://www.accenture.com › acnmedia › PDF-125 RYNEK WYMIANY WALUT W POLSCE – Accenture dostęp w dniu 14.01.2023 r.

Podatność sektora

Wszystkie podmioty oferujące usługi wymiany walut oferowane w Polsce – kantory stacjonarne, internetowe i banki są instytucjami obowiązanymi (IO). Podmioty te są zobowiązane ustawowo do stosowania środków bezpieczeństwa finansowego. Wymienione w ustawie środki bezpieczeństwa finansowego obejmują przede wszystkim takie czynności jak identyfikacja klienta i weryfikacja jego tożsamości; identyfikacja beneficjenta rzeczywistego; uzyskanie informacji dotyczących celu relacji klienta z jednostką obowiązaną; bieżące monitorowanie stosunków gospodarczych z klientem. Dla działalności kantorowej istotne są przede wszystkim sytuacje przeprowadzania transakcji okazjonalnej o wartości 15000 euro lub większej, bez względu na to czy jest to pojedyncza transakcja czy kilka transakcji wydających się ze sobą powiązanych, lub transferze środków pieniężnych o wartości przekraczającej kwotę 1000 euro. Inną ważną z punktu widzenia środków bezpieczeństwa finansowego jest sytuacja wystąpienia wątpliwości co do prawdziwości lub kompletności do tej pory uzyskanych danych identyfikacyjnych klienta, a także wypadek podejrzenia prania pieniędzy lub finansowania terroryzmu.

Działalność kantorową (regulowaną działalność wykonywaną na podstawie przepisów *ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców*) może wykonywać osoba fizyczna, ktora nie została prawomocnie skazana za przestępstwo skarbowe albo za przestępstwo popełnione w celu osiągnięcia korzyści majątkowej lub osobistej, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, w której wspólnicy, którym powierzono prowadzenie spraw spółki lub uprawnieni do reprezentacji spółki, lub członkowie organów zarządzających nie zostali skazani za ww. przestępstwa. Wymóg niekaralności dotyczy również osób kierujących wykonywaniem czynności związanych z prowadzeniem działalności kantorowej oraz do beneficjenta rzeczywistego podmiotu prowadzącego działalność kantorową oraz osób wykonujących bezpośrednio czynności kantorowe. Ponadto osoby wykonujące bezpośrednio czynności kantorowe muszą posiadać udokumentowane fachowe przygotowanie do wykonywania tych czynności tj. ukończony kurs obejmujący zagadnienia dotyczące działalności kantorowej lub pracę w banku, co najmniej 1 rok na stanowisku w zakresie obsługi transakcji walutowych. Istnieją również przedmiotowe ograniczenia w wykonywaniu działalności kantorowej, dotyczące niezbędnego wyposażenia lokalu przeznaczonego do wykonywania działalności kantorowej oraz sposobu prowadzenia ewidencji i wydawania dowodów kupna i sprzedaży wartości dewizowych. Są one określone rozporządzeniem Ministra Finansów z dnia 24 września 2004 r. Ponadto każdy przedsiębiorca wykonujący działalność kantorową jest obowiązany, na potrzeby kontroli skarbowej oraz kontroli wykonywanej przez Prezesa Narodowego Banku Polskiego (działalność regulowana), przechowywać dokumenty związane z tą działalnością przez okres 5 lat, licząc od końca roku kalendarzowego, w którym wykonywał działalność kantorową. Przedmiotowe wymogi nie dotyczą kantorów internetowych, których działalność nie jest działalnością opartą o wpis do rejestru, prowadzonego przez Prezesa Narodowego Banku Polskiego.

Podmioty sektora wymiany walut posiadają pewną świadomość swoich obowiązków z zakresu PPP/PFT[41]. Relatywnie mało powiadomień o transakcjach podejrzanych, przekazywanych do Generalnego Inspektora Informacji Finansowej (GIIF), pochodzi właśnie od podmiotów

[41] W 2021 r. przeprowadzono kontrole obejmujące łącznie 842 kantory. Nieprawidłowości w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu stwierdzono w 100 spośród skontrolowanych kantorów.

zajmujących się wymianą walut. Z danych GIIF dotyczących wszczętych przez GIIF w latach 2019-2021 postępowań analitycznych wynika, że w 2019 r. było to ok. 0,5% wszystkich postępowań dotyczących podejrzenia prania pieniędzy lub finansowania terroryzmu w związku z wykorzystaniem do podejrzanych usług wymiany walut lub wymiany banknotów, w 2020 r. było to ok. 0,9%, a w 2021 r. ok 0,8%.

Pracownicy kantorów stacjonarnych powinni mieć stosunkowo wysoką świadomość narażenia działalności kantoru na podejrzane transakcje związane z praniem pieniędzy bądź finansowaniem terroryzmu. Mają oni bowiem obowiązek ukończenia odpowiednich kursów dla pracowników kantoru, które obejmują zagadnienia praktyczne i prawne przy prowadzeniu takiej działalności. Kurs musi być udokumentowany otrzymanym świadectwem lub certyfikatem. Powinni więc być oni wyszkoleni w analizie sygnałów ostrzegawczych wynikających z transakcji podejrzanych. Ponieważ większość kantorów wymiany walut w Polsce należy do sektora małych i średnich przedsiębiorstw, to tylko nieliczne z nich dysponują zaawansowanymi narzędziami i systemami informatycznymi, wspomagającymi realizację celów przeciwdziałania praniu pieniędzy oraz finansowania terroryzmu. NBP prowadzi od 2019 r. spotkania z przedsiębiorcami prowadzącymi działalność kantorową mające na celu szerzenie wiedzy z zakresu działalności kantorowej oraz z zakresu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu. GIIF prowadził szkolenia dla instytucji obowiązanych i jednostek współpracujących, podczas których są przekazywane teoretyczne i praktyczne wskazówki dotyczące ustalania beneficjenta rzeczywistego oraz struktury własności i kontroli klientów, a także raportowania rozbieżności do organu właściwego w sprawie CRBR. Prowadzone były też szkolenia podnoszące świadomość AML/CTF w instytucjach obowiązanych.

Stosunkowo duża ilość przeprowadzanych w Polsce transakcji wymiany walut to transakcje okazjonalne, tj. nieprzeprowadzane w ramach stosunków gospodarczych. Klienci indywidualni deklarują, że 44% ich pieniędzy[42] zostało wymienionych w kantorach stacjonarnych. Na popularność takiej wymiany walut wpływa przede wszystkim anonimowość transakcji okazjonalnych, realizowanych często poniżej progu równowartości 15 000 EUR oraz gotówkowy charakter oferowanych usług.

Z uwagi na trwający konflikt zbrojny na Ukrainie utrudnione jest też pozyskanie szerszego spektrum dokumentów potwierdzających tożsamość lub wiarygodność klienta. Występują poważne problemy z identyfikacją i weryfikacją osób. Występująca bariera językowa i kulturowa w istotny sposób wpływa na prawidłowe rozpoznanie czynników zwiększonego ryzyka. Bariera ta utrudnia prawidłową ocenę odpowiedzi klientów-uchodźców w kwestiach problematycznych, które wymagają dodatkowych informacji czy dokumentów. Biorąc jednak pod uwagę rosnącą aktywność gospodarczą należy też zdawać sobie sprawę, że wymiana walut w małych i średnich firmach jest czymś naturalnym i powszechnym. 54% z nich dokonuje jej co najmniej kilka razy w tygodniu, a aż trzy na cztery przedsiębiorstwa tego typu operacje przeprowadza raz w tygodniu lub częściej. Z punktu widzenia kantoru wymiany walut występują jednak problemy z weryfikacją np. zagranicznych klientów w centralnych rejestrach beneficjentów rzeczywistych państw UE, zwłaszcza dotyczy to podmiotów o skomplikowanej strukturze kapitałowej.

[42] https://www.accenture.com › acnmedia › PDF-125 RYNEK WYMIANY WALUT W POLSCE – Accenture dostęp w dniu 14.01.2023 r.

Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie.

Istniejące przepisy prawne odpowiadają w dużej mierze zakresowi analizowanego ryzyka.

Zagrożenia w sektorze

Sektor wymiany walut pod względem oceny zagrożenia praniem pieniędzy, ale też zagrożenia finansowania terroryzmu, jest jednym z najczęściej wykorzystywanych sektorów. Sprawcy przestępstwa prania pieniędzy czy finansowania terroryzmu muszą dokonać w niektórych sytuacjach konwersji posiadanych środków finansowych pomiędzy różnymi walutami. Same środki finansowane mogą pochodzić ze źródeł legalnych bądź nielegalnych. Szczególnie istotny jest ten modus operandi w przypadku finansowania terroryzmu, gdy środki zbierane są na rzecz podróży w rejon konfliktu przez bojowników tzw. foreign fighters czy też w celu przekazania środków finansowych na rzecz konkretnych organizacji terrorystycznych czy celów ideologicznych, związanych z konfliktem w innym rejonie kontynentu czy globu.

Wśród zidentyfikowanych zagrożeń w obszarze wymiany walut zwraca uwagę przede wszystkim możliwość infiltracji kantorów wymiany walut przez grupy przestępcze. Zwłaszcza gdy dotyczy to kantorów zlokalizowanych w strefach przygranicznych, w miastach z dużą ilością turystów, dysponujących różnymi walutami. Czynnikiem zwiększającym zagrożenie wykorzystania kantoru wymiany walut do prania pieniędzy jest także korzystanie z jego usług przez osoby zajmujące stanowiska PEP-ów. Na zwiększone zagrożenie zarówno prania pieniędzy, jak i finansowania terroryzmu, wpływa użycie gotówki w transakcji. Może to mieć potencjalnie duże znaczenie w stosunkowo niskokwotowych transakcjach wymiany walut. Oprócz gotówkowej formy wymiany walut do głównych zidentyfikowanych obecnie zagrożeń należą: anonimowość transakcji, bliskość regionów przygranicznych, obecność na terytorium kraju społeczności imigranckich (migranci ekonomiczni, uchodźcy, pracownicy transgraniczni, osoby ubiegające się o azyl, turyści).

Wśród innych czynników zagrożenia w obszarze wymiany walut można wymienić zagrożenia związane z przedsiębiorcą prowadzącym działalność kantorową. Dotyczy to możliwości mieszania zysków pochodzących z legalnych i nielegalnych źródeł; relatywnie dużego obrotu jedną walutą bez uzasadnienia ekonomicznego; niedopełnienia przez pracowników kantoru należytej staranności przy wypełnianiu obowiązków dotyczących stosowania środków bezpieczeństwa finansowego; nawiązywania relacji bez fizycznej obecności klienta; przekazania środków na rachunki walutowe osób trzecich bez możliwości ustalenia beneficjenta rzeczywistego transakcji; możliwość posługiwania się banknotami o wysokich nominałach (np. 200 i 500 euro), wykorzystywanymi m.in. do transferowania i przechowywania zysków z nielegalnej działalności; zagrożenie produktowe – kupno/sprzedaż wartości dewizowych w kantorze oraz transakcje przez rachunki lub z wykorzystaniem automatycznych urządzeń do wymiany walut – walutomatów. Przeprowadzenie transakcji za pomocą walutomatu umożliwia zachowanie anonimowości. Ponadto należy zwrócić uwagę na zagrożenia związane z wystąpieniem powiązań osobowych przedsiębiorców prowadzących działalność kantorową z państwami wysokiego ryzyka poprzez kontakty z podmiotami mającymi siedzibę lub powiązania biznesowe w krajach podwyższonego ryzyka prania pieniędzy lub finansowania terroryzmu wskazanymi w *Rozporządzeniu delegowanym Komisji UE 2016/1675 z dnia 14 lipca 2016 r.* oraz na listach

FATF. Należy też zwracać uwagę na kantory, które krótki okres funkcjonowania na rynku łączą z dużymi obrotami.

Zagrożenia są również związane z klientami kantorów. Do tych zagrożeń należy zagrożenie związane z rozproszeniem transakcji. W celu ominięcia obowiązku informowania GIIF o transakcjach powyżej 15 000 euro, przeprowadza się transakcje o nieco mniejszej wartości, rozłożone w czasie. Zagrożenie zwiększa się w przypadku dużej liczby kantorów usytuowanych blisko siebie, np. na jednej ulicy. Zagrożenie przy wymianie walut związane z obsługą klientów dotyczy też klientów przeprowadzających anonimowe transakcje na okaziciela, w przypadku których na potwierdzenie przeprowadzonej transakcji wystawiany jest dowód kupna/sprzedaży niezawierający danych identyfikacyjnych klienta. Na ryzyko wpływa przede wszystkim anonimowość transakcji okazjonalnych, zwłaszcza jeżeli są realizowane poniżej progu równowartości 15 000 euro.

Zagrożeniem aktualnie wydaje się zdalna identyfikacja i weryfikacja tożsamości klientów, która staje się standardem. Wiąże się to z utrudnioną możliwością weryfikacji autentyczności okazywanych dokumentów oraz trudnością w ocenie zachowania klienta.

Uśredniony poziom zagrożenia sektora wymiany walut – ML – 3,33 i FT – 2,0

Uśredniony poziom podatności sektora wymiany walut – ML – 2,33 i FT – 2,0

Oszacowany poziom prawdopodobieństwa dla sektora – ML – 2,73 i FT - 2,00

Poziom ryzyka jest ostatecznie określany przez kombinację zagrożenia i podatności. Macierz ryzyka określająca ten poziom ryzyka opiera się na wadze 40% (zagrożenie) + 60% (podatność) – przy założeniu, że komponent podatności ma większą zdolność określania poziomu ryzyka. Zakłada się, że poziom podatności może zwiększyć atrakcyjność, a tym samym zamiary przestępców/terrorystów, aby użyć danego modus operandi – wpływając w ten sposób ostatecznie na poziom zagrożenia. Poziom ryzyka sektora, z uwzględniem prawdopobieństwa i konsekwencji (współczynnik 2,5 dla PP i 1,5 dla FT), jest ustalany zgodnie z metodyką krajowej oceny ryzyka – aneks nr 1.

Ryzyko FT sektora wymiany walut – 1.80	
1 – 1,5	Niskie
1,6 – 2,5	Średnie
2,6 – 3,5	Wysokie
3,6 – 4	Bardzo wysokie
Ryzyko ML sektora wymiany walut – 2,64	
1 – 1,5	Niskie
1,6 – 2,5	Średnie

2,6 – 3,5	Wysokie
3,6 – 4	Bardzo wysokie

WNIOSEK 1: Poziom ryzyka wykorzystania sektora wymiany walut do finansowania terroryzmu w Polsce znajduje się na poziomie średnim.

WNIOSEK 2: Poziom ryzyka wykorzystania sektora wymiany walut do prania pieniędzy w Polsce znajduje się na poziomie wysokim.

Mitygacja zidentyfikowanych ryzyk:

W celu ograniczenia prawdopodobieństwa wykorzystania sektora wymiany walut do prania pieniędzy lub finansowania terroryzmu, zasadne jest podjęcie odpowiednich działań. Stosowanie zaproponowanych działań mitygujących powinno następować z uwzględnieniem rozpoznanego przez danę instytucję obowiązaną ryzyka.

W sektorze wymiany walut powinny być podejmowane działania gwarantujące utrzymanie wysokiej świadomości narażenia na przestępstwo prania pieniędzy oraz finansowania terroryzmu, jak również utrzymujące poziom wyszkolenia pracowników tego sektora w analizie sygnałów ostrzegawczych wynikających z transakcji podejrzanych.

Podmioty sektora wymiany walut powinny doskonalić podejmowane działania związane z odpowiednią oceną przeprowadzanych transakcji wymiany walut, a także powinny utrzymywać bieżący monitoring stosunków gospodarczych.

W sektorze wymiany walut powinny być podejmowane działania podnoszące świadomość narażenia na przestępstwo prania pieniędzy oraz finansowania terroryzmu, jak również podnoszące poziom wyszkolenia pracowników tego sektora w analizie sygnałów ostrzegawczych wynikających z transakcji podejrzanych.

Ponieważ tylko nieliczne z kantorów wymiany walut dysponują zaawansowanymi narzędziami i systemami informatycznymi, wspomagającymi realizację celów przeciwdziałania praniu pieniędzy oraz finansowania terroryzmu, zasadnym jest rozwijanie przez instytucje sektora wymiany walut swoich możliwości w tym zakresie.

Kontynuowane powinny być szkolenia dla instytucji obowiązanych z sektora wymiany walut, podczas których będą przekazywane teoretyczne i praktyczne wskazówki dotyczące ustalania beneficjenta rzeczywistego oraz struktury własności i kontroli klientów a także raportowania rozbieżności do organu właściwego w sprawie CRBR. Zalecane jest uczestnictwo przedstawicieli instytucji obowiązanych w szkoleniach podnoszących świadomość AML/CTF, organizowanych zarówno przez GIIF, jak i przez UKNF w ramach Programu CEDUR.

Instytucje obowiązane z sektora wymiany walut powinny zwracać szczególną uwagę na transakcje wymiany walut związane z jurysdykcjami charakteryzujących się wyższym ryzykiem prania pieniędzy oraz finansowania terroryzmu. Instytucje obowiązane powinny położyć szczególny nacisk na ustalenie danych dotyczących źródła pochodzenia transferowanych wartości majątkowych, jak również dokumentów wskazujących na uzasadnienie przeprowadzenia danej transakcji. W przypadku wymiany większej ilości

gotówki przez nierezydentów UE, instytucje obowiązane powinny rozważyć zwrócenie się do klienta o przedstawienie informacji na temat źródła pochodzenia wartości majątkowych, np. poprzez weryfikację deklaracji dewizowych klientów z państw spoza UE.

Instytucje obowiązane przyjmujące płatności albo wpłaty gotówkowe w walutach obcych, powinny weryfikować źródło pochodzenia wartości majątkowych, w tym zasadnym może się okazać pozyskanie od klienta informacji potwierdzających dokonanie wymiany waluty, czy też potwierdzających złożenie deklaracji dewizowych.

Instytucje obowiązane powinny przykładać szczególną wagę do czynników geograficznych mogących wskazywać na wyższe ryzyko prania pieniędzy czy też finansowania terroryzmu, takich jak niestabilna sytuacja polityczna czy konflikt zbrojny, czego najdobitniejszym przykładem w ostatnich latach jest wojna prowadzona przez Rosję przeciwko Ukrainie. Z uwagi na wysokie ryzyko transferowania środków pochodzących z nielegalnego handlu, przemytu ludzi, handlu bronią, czy też działań zmierzających do omijania sankcji gospodarczych, szczególnie istotne jest analizowanie przez instytucje obowiązane nie tylko danych dotyczących samych stron transakcji, ale również beneficjentów rzeczywistych, czy też faktycznych celów przeprowadzania danych transakcji. Podmioty z sektora wymiany walut powinny zwracać szczególną uwagę na wysokokwotowe transakcje przeprowadzane z rezydentami jurysdykcji objętych konfliktami, jak również na transakcje wskazujące, na wykorzystanie pośrednika do wymiany waluty.

6. Obszar – waluty wirtualne

Opis sektora – zawarty jest w podrozdziałach KOR 2.1.2 - „Sektory rynku finansowego", podrozdziale 4.5. „Rejestr działalności na rzecz spółek lub trustów i rejestr działalności w zakresie walut wirtualnych" oraz w podrozdziale 7.2.1 - „Podatność rynku finansowego", a także w rozdziale 6.3. „Najczęstsze metody stosowane w celu finansowania terroryzmu".

Scenariusze wystąpienia ryzyka (tj. możliwe przykłady wystąpienia ryzyka) zarówno w przypadku prania pieniędzy, jak i finansowania terroryzmu - dotyczyły wykorzystania do prania pieniędzy i finansowania terroryzmu produktów i usług finansowych w postaci zdecentralizowanych i wymienialnych walut wirtualnych (tzw. kryptowalut). Ich opis znajduje się poniżej.

Pranie pieniędzy

Tabela 32

Rodzaj wykorzystanych usług, produktów finansowych	Zdecentralizowane i wymienialne waluty wirtualne (tzw. kryptowaluty)
Ogólny opis ryzyka	Wykorzystanie kryptowalut do transferowania wartości pochodzących z nielegalnych źródeł
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Wykorzystywanie kryptowalut do uzyskiwania zysków z różnego rodzaju przestępstw, w tym wymuszeń (np. jako zapłata za odszyfrowanie shakowanych danych na komputerze), porwań (jako okup za uwolnienie porwanej osoby). 2. Wykorzystanie kryptowalut do dokonywania zapłaty za narkotyki, kupione za pośrednictwem platform handlowych w Darknecie. 3. Wykorzystywanie kryptowalut do zaciemnienia źródła pochodzenia nielegalnych zysków, np. pieniądze wytransferowane w wyniku nieautoryzowanego dostępu do rachunku bankowego ofiary są przekazywane na rachunek podmiotu prowadzące platformę wymiany walut wirtualnych celem zakupu jednostek kryptowalut. Zakupione jednostki kryptowaluty są następnie przekazywane na anonimowy portfel *offline*. 4. Przyjmowanie na rachunek w banku polskim środków mogących pochodzić z różnych przestępstw i następnie transferowanie ich do podmiotów zajmujących się obrotem kryptowalutami (utrudnione/niemożliwe śledzenie dalszej ścieżki przepływu środków). 5. Świadczenie usług pośrednictwa finansowego m.in. w zakresie inwestycji w kryptowaluty przez podmioty nieposiadające odpowiednich zezwoleń. 6. Użycie tzw. BTM (Bitcoin ATMs) do realizacji wypłat gotówkowych w różnych walutach. Gotówkowa forma dokonywanych transakcji umożliwia legalizację środków pochodzących z przestępstwa. 7. Używanie przez przestępców tzw. zdecentralizowanych finansów tzw. DeFi [43]. zbiorczy termin dla usług finansowych opartych na publicznych łańcuchach bloków (głównie *Ethereum*). Za pomocą DeFi można wykonywać takie same operacje, jak te obsługiwane przez banki np. zaciągać pożyczki i ich udzielać, kupować ubezpieczenia, handlować instrumentami pochodnymi, obracać aktywami bez udziału osób trzecich.
Poziom podatności	3
Uzasadnienie dla poziomu podatności	Dostęp do tego typu usług jest relatywnie łatwy. Istnieją możliwości ukrycia danych identyfikacyjnych klientów (podmioty oferujące tego typu usługi dokonują identyfikacji klientów na odległość). Występują transakcje o charakterze międzynarodowym. Podmioty oferujące usługi w zakresie wymiany walut wirtualnych (w tym kryptowalut) czy udostępniania tzw. „hot wallets" są IO. Jakkolwiek w Internecie są dostępne oferty podmiotów zarejestrowanych poza granicami

[43] DeFi ma charakter globalny, *peer-to-peer* (czyli bezpośrednio pomiędzy dwoma osobami, a nie poprzez scentralizowany system), zapewnia anonimowość i globalną dostępność.

	kraju, a także UE, które nie podlegają obowiązkom w zakresie przeciwdziałania PP/FT. Ponadto, transakcje przy użyciu kryptowalut mogą być dokonywane bez pośrednictwa podmiotów trzecich. Organy administracji publicznej posiadają podstawową wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwości gromadzenia i analizowania informacji dot. tego typu usług, jednak pochodzących od podmiotów będących IO albo udostępnionych przez zagraniczną jednostkę analityki finansowej. Istnieje prawdopodobieństwo, że przypadek prania pieniędzy w zakresie analizowanych scenariuszy nie zostanie wykryty. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają częściowo zakresowi analizowanego ryzyka.
Poziom zagrożenia	3
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie kryptowalut do transferowania wartości majątkowych pochodzących z nielegalnych źródeł może być jedną z metod prania pieniędzy. Powodem jest to, że naturalne cechy kryptowalut dają możliwość stosunkowo łatwego ukrycia danych stron transakcji, mogą wystąpić kłopoty ze śledzeniem ścieżki transferów[44] oraz ich ewentualnym zatrzymaniem. Sprzyja to możliwości ich użycia przez zorganizowane grupy przestępcze, zwłaszcza że transakcje takie są trudne do wykrycia dla organów ścigania i organów podatkowych. Żeby jednak zastosować powyższy *modus operandi* do prania pieniędzy potrzebne jest odpowiednie planowanie, a także wiedza do jego zastosowania. GIIF posiada niezbyt liczne informacje o możliwości wykorzystywania kryptowalut do transferowania wartości majątkowych pochodzących z nielegalnych źródeł. WNIOSEK: Na obecnym etapie wykorzystanie kryptowalut do transferowania wartości majątkowych pochodzących z nielegalnych źródeł z uwagi na stopień skomplikowania stwarza wysokie zagrożenie dla prania pieniędzy.

Tabela 33

Rodzaj wykorzystanych usług, produktów finansowych	Scentralizowane waluty wirtualne
Ogólny opis ryzyka	Wykorzystanie scentralizowanych walut wirtualnych do transferowania wartości pochodzących z nielegalnych źródeł
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	Przestępcy wymieniają pieniądze pochodzące z nielegalnych źródeł na jednostki scentralizowanych walut wirtualnych w jednym z internetowych punktów obrotu kryptowalutami realizujących tego typu transakcje. Następnie jednostki tych walut lokują na koncie założonym u zagranicznego dostarczyciela usług ww. zakresie transferów wartości (podobnego typu jak usługi płatnicze). Jednostki tych walut są przekazywane na inne konta założone w ramach tego samego systemu transakcyjnego, a następnie po ich wymianie przekazywane są na zagraniczny rachunek bankowy.
Poziom podatności	3

[44] Zwłaszcza w przypadku wykorzystania narzędzi do mieszania, plątania transakcji w celu skomplikowania powiązań pomiędzy nimi i ich użytkownikami (tzw. *anomizers*).

Uzasadnienie dla poziomu podatności	Dostęp do tego typu usług jest relatywnie łatwy - jakkolwiek niewiele podmiotów oferuje tego typu waluty. Istnieją możliwości ukrycia danych identyfikacyjnych klientów (podmioty oferujące tego typu usługi dokonują identyfikacji klientów na odległość). Występują transakcje o charakterze międzynarodowym. Podmioty oferujące te usługi są IO. Jakkolwiek w Internecie są dostępne oferty podmiotów zarejestrowanych poza granicami kraju, a także UE, które nie podlegają obowiązkom w zakresie przeciwdziałania PP/FT. Organy administracji publicznej posiadają podstawową wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma ograniczone możliwości gromadzenia i analizowania informacji dot. tego typu usług. Istnieje prawdopodobieństwo, że przypadek prania pieniędzy w zakresie analizowanych scenariuszy nie zostanie wykryty. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają częściowo zakresowi analizowanego ryzyka
Poziom zagrożenia	3
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie scentralizowanych walut wirtualnych do transferowania wartości majątkowych pochodzących z nielegalnych źródeł również może być jedną z metod prania pieniędzy. Globalny charakter rynków finansowych i kapitałowych powoduje, że powstaje możliwość stosunkowo łatwej zamiany pieniędzy pochodzących z nielegalnych źródeł na jednostki scentralizowanych walut wirtualnych oraz (w wyniku szeregu transakcji) w drugą stronę (z wykorzystaniem anonimizacji stron transakcji i cech utrudniających śledzenie transferów, jak ich zatrzymanie). Żeby jednak zastosować powyższy *modus operandi* do prania pieniędzy potrzebne jest odpowiednie planowanie, a także wiedza do jego zastosowania. GIIF posiada informacje o możliwości wykorzystywania scentralizowanych walut wirtualnych do transferowania wartości majątkowych pochodzących z nielegalnych źródeł. WNIOSEK: Na obecnym etapie wykorzystanie scentralizowanych walut wirtualnych do transferowania wartości majątkowych pochodzących z nielegalnych źródeł stwarza wysokie zagrożenie dla prania pieniędzy.

Finansowanie terroryzmu

Tabela 34

Rodzaj wykorzystanych usług, produktów finansowych	Zdecentralizowane i wymienialne waluty wirtualne (tzw. kryptowaluty)
Ogólny opis ryzyka	Wykorzystanie kryptowalut do transferowania wartości majątkowych na cele działalności terrorystycznej
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Upowszechnianie informacji o adresach kryptowalut, na które zwolennicy organizacji terrorystycznych transferują wartości majątkowe w zdecentralizowanych i wymienialnych walutach wirtualnych. 2. Gromadzenie środków od sympatyków organizacji terrorystycznych lub nieświadomych inwestorów pod pretekstem finansowania przygotowań emisji nowej kryptowaluty, która to emisja albo nie następuje, albo kończy się deprecjacją wyemitowanej waluty. Zgromadzone środki przekazywane są organizacji terrorystycznej. Dodatkowo może funkcjonować system poleceń mający służyć skutecznej rekrutacji nowych jej członków. 3. Darowizny wirtualnych walut dokonywane przez krewnych bojowników organizacji terrorystycznych za pośrednictwem aplikacji OTT (Over the Top). Aplikacja over-the-top (OTT) to dowolna aplikacja lub usługa, która dostarcza produkt przez Internet i omija tradycyjną dystrybucję.
Poziom podatności	3

Uzasadnienie dla poziomu podatności	Dostęp do tego typu usług jest relatywnie łatwy. Istnieją możliwości ukrycia danych identyfikacyjnych klientów (podmioty oferujące tego typu usługi dokonują identyfikacji klientów na odległość). Występują transakcje o charakterze międzynarodowym. Podmioty oferujące usługi w zakresie wymiany walut wirtualnych (w tym kryptowalut) czy udostępniania tzw. „hot wallets" są IO. Jakkolwiek w Internecie są dostępne oferty podmiotów zarejestrowanych poza granicami kraju, a także UE, które nie podlegają obowiązkom w zakresie przeciwdziałania PP/FT. Ponadto transakcje przy użyciu kryptowalut mogą być dokonywane bez pośrednictwa podmiotów trzecich. Organy administracji publicznej posiadają podstawową wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwości gromadzenia i analizowania informacji dot. tego typu usług, jednak pochodzących od podmiotów będących IO albo udostępnionych przez zagraniczną jednostkę analityki finansowej. Istnieje prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy nie zostanie wykryty. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają częściowo zakresowi analizowanego ryzyka.
Poziom zagrożenia	3
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie walut wirtualnych do transferowania wartości majątkowych na cele działalności terrorystycznej z uwagi na ich cechy sprzyjające anonimizacji stron transakcji i utrudniające zarówno śledzenie transferów, jak ich zatrzymanie, może być jedną z metod finansowego wspierania terroryzmu. Same waluty wirtualne zyskały na popularności ze względu na swoje cechy, takie jak dostępność globalna, łatwość dostępu, rzetelne i nieodwracalne transakcje, niski koszt i szybkość międzynarodowego transferu. Wydaje się jednak, że ich wykorzystanie w Europie wśród organizacji terrorystycznych wydaje się być stosunkowo słabe w stosunku do rozwoju ich popularności w ponadnarodowych grupach przestępczości zorganizowanej, zwłaszcza tych związanych z cyberprzestępczością. Raport Europolu TE-SAT za 2020 r. konkluduje, że liczba spraw związanych z wykorzystaniem kryptowalut dla celów finansowania terroryzmu w 2020 r. pozostawała na niskim poziomie. Zostały zidentyfikowane przez zagraniczne służby przypadki wykorzystania walut wirtualnych do realizacji w Europie transakcji mających związek z finansowaniem terroryzmu, jakkolwiek ich liczba pozostaje relatywnie niewielka. Użycie walut wirtualnych jest trudne do zastosowania, wymaga specjalistycznej wiedzy. WNIOSEK: Wykorzystanie walut wirtualnych do transferowania wartości majątkowych na cele działalności terrorystycznej stwarza średnie zagrożenie finansowaniem terroryzmu.

Rynek kryptoaktywów ma charakter ponadnarodowy, wymykający się terytorialnemu charakterowi działalności regulowanej. Również w Polsce rynek kryptowalut nie jest rynkiem regulowanym ani nadzorowanym. KNF nie licencjonuje, nie nadzoruje ani też nie wykonuje żadnych innych uprawnień władczych w odniesieniu do działalności w zakresie obrotu kryptowalutami[45]. Niektóre z podmiotów działających na rynku krytptowalut upoważnione są do świadczenia usług płatniczych, służących w szczególności rozliczeniom płatności dokonywanych prawnym środkiem płatniczym (FIAT) za nabywane lub sprzedawane kryptowaluty. W tym zakresie działalność tych podmiotów podlega nadzorowi KNF. Podkreślić jednak należy, że nadzór ten dotyczy wyłącznie prawidłowości świadczenia usług

[45] https://www.knf.gov.pl/komunikacja/komunikaty?articleId=70400&p_id=18, Ostrzeżenie przed oszustami powołującymi się na nadzór KNF w zakresie transakcji wymiany kryptowalut, dostęp w dniu 20.01.2023 r.

płatniczych i nie obejmuje kwestii wywiązywania się tych podmiotów lub osób przez nie reprezentowanych z zobowiązań z tytułu kupna lub sprzedaży kryptowalut.

Prowadzenie działalności gospodarczej w zakresie walut wirtualnych od października 2021 r. ma status działalności regulowanej, tzn. zostało ono uzależnione od wcześniejszego wpisu do rejestru działalności w zakresie walut wirtualnych, prowadzonego przez Dyrektora Izby Administracji Skarbowej w Katowicach (według stanu na 29.06.2023 r. było 815 wpisów).

W art. 2 ust. 2 pkt 26) *ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* zawarta jest legalna definicja walut wirtualnych. Zgodnie z treścią tego przepisu przez „walutę wirtualną" należy rozumieć cyfrowe odwzorowanie wartości, które nie jest:

a) prawnym środkiem płatniczym emitowanym przez NBP, zagraniczne banki centralne lub inne organy administracji publicznej,

b) międzynarodową jednostką rozrachunkową ustanawianą przez organizację międzynarodową i akceptowaną przez poszczególne kraje należące do tej organizacji lub z nią współpracujące,

c) pieniądzem elektronicznym w rozumieniu *ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych*,

d) instrumentem finansowym w rozumieniu *ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi*,

e) wekslem lub czekiem

oraz jest wymienialne w obrocie gospodarczym na prawne środki płatnicze i akceptowane jako środek wymiany, a także może być elektronicznie przechowywane lub przeniesione albo może być przedmiotem handlu elektronicznego.

Ze względu na szybko ewoluujące technologie i produkty rynku kryptowalut Unia Europejska zdecydowała się objąć ramami regulacyjnymi kryptoaktywa, emitentów kryptoaktywów i dostawców usług kryptoaktywowych (platformy obrotu kryptoaktywami i portfele kryptoaktywowe). Ma to zapewnić większą przejrzystość w Unii Europejskiej, bowiem tylko niektóre państwa członkowskie miały krajowe przepisy dotyczące kryptoaktywów, natomiast na szczeblu unijnym nie istniały żadne konkretne ramy regulacyjne. W tym celu zostało wydane unijne *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1114 z dnia 31 maja 2023 r. w sprawie rynków kryptoaktywów oraz zmiany rozporządzeń (UE) nr 1093/2010 i (UE) nr 1095/2010 oraz dyrektyw 2013/36/UE i (UE) 2019/1937* (MiCA - Markets in Crypto Assets). W projekcie rozporządzenia pojawiły się wymagania dla podmiotów, które chcą zajmować się działalnością w zakresie handlu kryptowalutami. Został np. wprowadzony obowiązek uzyskania zezwolenia czy opublikowania odpowiedniego dokumentu informacyjnego, który ma być zatwierdzany przez odpowiednie organy krajowe. Dodatkowo zmienią się wymogi organizacyjne oraz wymogi w zakresie zabezpieczenia ostrożnościowego. *Rozporządzenie w sprawie rynków kryptoaktywów* dzieli kryptoaktywa na 3 kategorie – tokeny powiązane z aktywami; tokeny będące pieniądzem elektronicznym (e-pieniądzem); kryptoaktywa inne niż tokeny. W kategorii tokenów powiązanych z aktywami oraz tokenów będących pieniądzem elektronicznym obowiązkowe będzie uzyskanie formalnego zezwolenia, którego otrzymanie będzie obwarowane spełnieniem wielu warunków. Wśród tych warunków trzeba będzie

posiadać odpowiednie procedury, polityki czy odpowiednich pracowników, posiadających wiedzę i doświadczenie. Ustanowiono też wymogi podmiotowe w zakresie osób zarządzających, w szczególności w zakresie nieskazitelności charakteru. Zasadniczo więc firmy świadczące usługi w zakresie kryptowalut muszą być bardzo transparentne dla organów kontrolujących ich działalność na terytorium Polski. W rozporządzeniu przewidziano też nową kategorię podmiotów „świadczących usługi doradcze w zakresie kryptowalut". Chodzi o różnego typu doradców nakłaniających do inwestycji w obszarze aktywów cyfrowych. Tego typu podmioty również będą musiały spełnić pewne wymogi przejrzystości. O wydanie zezwolenia będą mogły ubiegać się jedynie osoby prawne posiadające siedzibę statutową w państwie członkowskim Unii Europejskiej. Zezwolenie mogą uzyskać emitenci kryptowalut, którzy dokonują oferty publicznej tokenów powiązanych z aktywami w Unii lub ubiegają się o dopuszczenie takich aktywów do obrotu na platformie obrotu kryptoaktywami. Zezwolenie udzielone przez właściwy organ jest ważne w całej Unii i umożliwia emitentowi oferowanie tokenów powiązanych z aktywami, w odniesieniu do których uzyskał zezwolenie, w całej Unii oraz ubieganie się o dopuszczenie takich tokenów powiązanych z aktywami do obrotu na platformie obrotu kryptoaktywami. Przepisy rozporządzenia będą obowiązywać od 30 grudnia 2024 r., z wyjątkiem przepisów dotyczących tokenów powiązanych z aktywami oraz tokenów będących pieniądzem elektronicznym, które będą obowiązywać od 30 czerwca 2024 r.

Kolejnym aktem prawnym z obszaru kryptoaktywów jest *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1113 z dnia 31 maja 2023 r. w sprawie informacji towarzyszących transferom środków pieniężnych i niektórych kryptoaktywów oraz zmiany dyrektywy (UE) 2015/849*. Rozporządzenie stanowi część pakietu zmian w unijnych przepisach dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu[46]. Nowelizacja przepisów dotyczy objęcia transferów kryptoaktywów zbliżonymi wymogami co do informacji, które muszą być przesyłane wraz z transferami kryptoaktywów, do wymogów stosowanych do transferów środków pieniężnych. Dostawcy usług w zakresie kryptoaktywów będą zobowiązani do gromadzenia i udostępniania informacji identyfikujących nadawcę i odbiorcę dokonywanych transferów kryptoaktywów. Informacje te będą musiały być przekazywane wraz z transferem kryptoaktywów. Znowelizowane przepisy pozwolą śledzić transfery kryptoaktywów. Rozporządzenie będzie obowiązywać od 30 grudnia 2024 r.

Jednocześnie z pracami nad rozporządzeniem w sprawie rynków kryptoaktywów Komisja Europejska, w dniu 8 grudnia 2022 r. opublikowała propozycję dyrektywy w sprawie współpracy administracyjnej obejmującej sprawozdawczość podatkową dotyczącą kryptowalut („DAC8"). Komisja zaproponowała […] ujednolicenie przepisów związanych z sprawozdawczością dla usługodawców harmonizujących transakcje w walutach cyfrowych,

[46] Na pakiet ten składają się, poza aktem prawnym omówionym w niniejszym materiale, następujące projekty: propozycja Rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego Urząd ds. Przeciwdziałania Praniu Pieniędzy i Finansowaniu Terroryzmu i zmieniającego rozporządzenia (UE) nr 1093/2010, (UE) nr 1094/2010 i (UE) nr 1095/2010 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0421), propozycja Rozporządzenia Parlamentu Europejskiego i Rady w sprawie przeciwdziałania korzystaniu z systemu finansowego w celu prania pieniędzy lub finansowania terroryzmu (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0420), propozycja Dyrektywy Parlamentu Europejskiego i Rady w sprawie mechanizmów, które państwa członkowskie powinny wprowadzić, mających na celu zapobieganie wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz uchylająca dyrektywę (UE) 2015/849 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0423).

a w tym roczne raporty z giełd i rynków kryptowalut[47]. Poprawi to przejrzystość w zakresie zobowiązań podatkowych, pomagając w identyfikacji dochodów i zysków podlegających opodatkowaniu. Co do zasady dostawcy usług związanych z kryptowalutami, niezależnie od ich wielkości lub lokalizacji, będą musieli zgłaszać transakcje klientów zamieszkałych w UE, bez względu na to, czy są to transakcje krajowe czy transgraniczne. Nowa dyrektywa poprawi zdolność państw członkowskich do wykrywania i przeciwdziałania oszustwom podatkowym, uchylaniu się od opodatkowania oraz unikaniu opodatkowania. Rozszerzy też ona zakres sprawozdawczości i wymiany informacji między organami podatkowymi w UE poprzez objęcie jej zakresem dochodów i przychodów generowanych przez użytkowników zamieszkałych w UE podczas prowadzenia działalności z wykorzystaniem kryptowalut. Przedmiotowa dyrektywa może stanowić koniec okresu, kiedy właściciele portfeli kryptograficznych mogli pozostawać anonimowi. Kwestia ustalenia danych osobowych właścicieli aktywów jest bowiem kluczowa dla efektywnego weryfikowania osób fizycznych i prawnych, które mogą uchylać się od opodatkowania. Dyrektywa przewiduje też szerokie obowiązki dotyczące raportowania. Transakcje podlegające zgłoszeniu to transakcje wymiany i transfery związane z aktywami kryptograficznymi. Zakresem dyrektywy objęte są zarówno transakcje krajowe, jak i transgraniczne.

W sektorze związanym z podmiotami prowadzącymi działalność gospodarczą polegającą na świadczeniu usług w zakresie walut wirtualnych coraz większe zagrożenie związane z praniem pieniędzy oraz finansowaniem terroryzmu odgrywają niewymienialne tokeny NFT (ang. non-fungible token). Są to unikalne cyfrowe certyfikaty oparte na technologii blockchain, które reprezentują różnie definiowane prawo do zarówno fizycznych jak i cyfrowych aktywów. Poprzez przystępną i wiarygodną ewidencję uprawnień oraz możliwość zarabiania tantiem od pierwotnej sprzedaży zasobu cyfrowego – rynek NFT staje się jednym z najszybciej rozwijających się sektorów globalnej gospodarki cyfrowej. Sektor NFT jest to sektor rynku niewymagający dokładnych informacji o klientach i transakcjach. Brak regulacji AML na rynku NFT powoduje większe ryzyko dla uczestników rynku, a w szerszym ujęciu dla ogólnej stabilności finansowej. NFT są oparte na tej samej technologii blockchain co waluty wirtualne, różnią się tym, że są niewymienialne. NFT to tokeny kryptograficzne oparte o technologie powstałe w ramach blockchain powiązane z określonym obiektem cyfrowym. Najczęściej to cyfrowe powiązanie reprezentuje podstawowe prawo do cyfrowego lub fizycznego zasobu, w tym obrazów, filmów, plików audio lub innych cyfrowych „przedmiotów". Funkcje NFT są zarządzane za pomocą inteligentnych kontraktów i portfeli cyfrowych, a ogólnie działania te są publicznie weryfikowalne, ponieważ są rejestrowane w blockchainie.

W chwili obecnej transakcje NFT pozostają zasadniczo nieuregulowane. FATF zauważa jednak, że transakcje NFT mogą mieścić się w definicji aktywów wirtualnych, jeśli w praktyce wykorzystywane są do celów płatniczych lub inwestycyjnych. W warunkach polskich podmiot, który oferuje NFT spełniający kryteria waluty wirtualnej, w rozumieniu *ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*, będzie instytucją obowiązaną. Instytucje obowiązane, które mają stosunki gospodarcze z takim podmiotem (np. banki, które prowadzą dla takiego podmiotu rachunek bankowy), powinny uwzględnić ten fakt w ocenie stosunków gospodarczych z podmiotem. W szczególności pod uwagę powinien wzięty zostać fakt, że kupno i sprzedaż NFT są dokonywane z wykorzystaniem walut

[47] https://kryptoprawo.pl/dac8-transakcje-kryptowalutowe-beda-raportowane-do-skarbowki/ dostęp w dniu 22.01.2023 r.

wirtualnych. Na gruncie polskich przepisów nie jest jednak dopuszczalne dokonywanie transakcji wymiany walut wirtualnych zapewniających anonimowość na NFT.

Podatność sektora

Podmioty oferujące usługi w zakresie wymiany walut wirtualnych (w tym kryptowalut) czy udostępniania tzw. „hot wallets" są instytucjami obowiązanymi. W Internecie jednakże są dostępne oferty podmiotów zarejestrowanych poza granicami Polski, a także UE, które nie podlegają obowiązkom w zakresie przeciwdziałania PP/FT. Należy też zwrócić uwagę na fakt, że transakcje przy użyciu kryptowalut mogą być dokonywane bez pośrednictwa podmiotów trzecich. Podmioty te jako instytucje obowiązane stosują środki bezpieczeństwa finansowego, określone w ustawie z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

Wymienione w ustawie środki bezpieczeństwa finansowego obejmują przede wszystkim prawidłową identyfikację klienta i beneficjenta rzeczywistego, monitorowanie rozbieżności występujących między CRBR a ustaleniami instytucji obowiązanej, właściwe ustalenie struktury własności i kontroli w przypadku klienta będącego osobą prawną albo jednostką organizacyjną nieposiadającą osobowości prawnej. Należy tu też bieżące monitorowanie stosunków gospodarczych klienta, uzyskiwanie informacji na temat ich celu i zamierzonego charakteru. Stosowanie środków bezpieczeństwa finansowego odnosi się do transakcji okazjonalnych równych 1 000 euro lub przewyższających tę wartość.

Jednakże, jak wynika z posiadanych informacji, działalność podmiotów (instytucji obowiązanych, zwłaszcza mniejszych, obejmujących punkty obrotu kryptowalutami, giełdy kryptowalutowe, podmioty dostarczające portfele kryptowalutowe) oferujących usługi w zakresie wymiany walut wirtualnych wiąże się z trudnościami z rzeczywistym monitorowaniem transakcji swoich klientów. Podmioty sektora walut wirtualnych posiadają zróżnicowaną świadomość swoich obowiązków z zakresu PPP/PFT.

W zakresie sektora walut wirtualnych w latach 2019-2021 GIIF otrzymał i zrealizował łącznie 45 spraw analitycznych, gdzie transakcjami podejrzanymi były transakcje z udziałem walut wirtualnych. W 2019 r. było to ok. 1,8% wszystkich postępowań dotyczących podejrzenia prania pieniędzy lub finansowania terroryzmu w związku z wykorzystaniem do podejrzanych transakcji walut wirtualnych, w 2020 r. ok. 2,0%, a w 2021 r. ok 4,6%.

Odnośnie transakcji w sektorze walut wirtualnych wykorzystywany jest przez podmioty oszukańcze atrybut wiarygodności organów publicznych. Dotyczy to oferowania kupna lub sprzedaży kryptowalut, z jednoczesnym wskazaniem, że transakcje te są nadzorowane przez Komisję Nadzoru Finansowego. Potencjalni klienci często są informowani o tym, że podczas transakcji spełnione zostaną „wymagania KNF dotyczące nagrywania procesu transakcji", co ma polegać przykładowo, na udostępnieniu pulpitu komputera. Częstym przekazem jest, że w operacji wymiany walut wirtualnych będzie uczestniczył pracownik UKNF w celu monitorowania przebiegu transakcji.

Centralne Biuro Zwalczania Cyberprzestępczości zauważa, że wyróżniającym się trendem przestępczości w cyberprzestrzeni oraz pośród przestępstw popełnianych z wykorzystaniem najnowszych technologii, jest wykorzystywanie kryptowalut do ukrywania źródeł dochodów uzyskiwanych z działalności przestępczej. Mowa tu o walutach wirtualnych obejmujących kryptowaluty oraz niektóre inne umowne jednostki dające się wymienić na pieniądze

fiducjarne, które mogą być wykorzystane do przenoszenia wartości majątkowych również na cele działalności terrorystycznej. Sprzyja temu anonimizacja stron transakcji utrudniająca zarówno śledzenie transferów, jak też ich zatrzymanie.

Z praktyki prowadzenia spraw karnych przez prokuraturę wynika, że sprawy dotyczące walut wirtualnych są bardzo skomplikowane[48]. Wynika to między innymi z tego, że sprawowanie kontroli nad podmiotami oferującymi usługi w zakresie wymiany walut wirtualnych i samymi transakcjami jest mniej efektywne, aniżeli nad „tradycyjnym" przepływem pieniądza bezgotówkowego. Doświadczenie pokazuje, że działalność większości VASP (Virtual Asset Service Providers) bardziej lub mniej „zahacza" o szarą strefę dotyczącą aktywności przestępców, a nierozpoznana do końca natura cyfrowych żetonów zwiększa ryzyko malwersacji. Sprzyja temu brak spójnego, globalnego nadzoru nad podmiotami świadczącymi usługi, odmienne regulacje prawne, a nawet miejsca, gdzie brak skutecznych procedur AML/CTF i implementacji standardów KYC. Występują też stosunkowo niskie koszty alternatywne wynikające z utraty reputacji: ujawnienie przez bank zdarzenia związanego z „praniem" spotka się najprawdopodobniej z negatywnym odbiorem społecznym nawet, jeśli zadziałały reguły AML. W przypadku giełd i punktów obrotu kryptowalutami możliwość wyprania pieniędzy powoduje często reakcję odwrotną: przestępcy chętnie wykorzystują „podejrzane" platformy, co zwiększa zyski ich administratorów.

Z badań, przeprowadzonych przez P. Opitka[49] na podstawie spraw prowadzonych we wszystkich prokuraturach w Polsce na przestrzeni kilku ostatnich lat (do roku 2020), dotyczących przestępczości kryptowalutowej wynika, że to bitcoin jest najczęściej zaangażowany do popełniania przestępstw i wbrew spotykanym opiniom, o wiele rzadziej wykorzystywane są systemy zapewniające jeszcze większą anonimowość (Z–Cash, Monero). Wynika to przede wszystkim z faktu, że rynek BTC jest stosunkowo głęboki, skalowalny i w miarę stabilny.

Według raportu firmy Chainalysis, zajmującej się analizą blockchain, wartość nielegalnych transakcji na rynku kryptowalut w 2022 r.[50] wyniosła 20,1 mld dol. Jest to głównie efekt ich wykorzystywania przez firmy objęte sankcjami USA. W 2022 r. nastąpiło czasowe załamanie rynku kryptowalut, co było efektem upadku giełd i zmniejszenia poziomu akceptacji ryzyka. Inwestorzy ponieśli duże straty, a firmy regulacyjne zintensyfikowały wezwania do zwiększenia ochrony konsumentów. Jednak, jak stwierdza raport firmy Chainalysis, nawet gdy ogólny wolumen transakcji spadł, wartość transakcji kryptowalutami związanych z nielegalną działalnością biznesową lub wręcz działaniami kryminalnymi wzrosła drugi rok z rzędu. Przyczyną były transakcje związane z podmiotami objętymi sankcjami. W 2022 r. stanowiły 44% nielegalnej działalności na rynku kryptowalut. Przykładem może być rosyjska giełda kryptowalut Garantex, objęta sankcjami Departamentu Skarbu USA w kwietniu 2022 r. Jej działania według raportu stanowiły „znaczną część nielegalnego wolumenu transakcyjnego w 2022 r.", przy czym większość została wygenerowana przez „rosyjskich użytkowników działających na moskiewskiej giełdzie". Prawdopodobnie poprzez kryptowaluty wyprowadzano w ten sposób z Rosji pieniądze. Ponieważ firma objęta jest sankcjami, wszystkie te transakcje oznaczano jako nielegalne. W 2022 r. spadł wolumen transakcji

[48] P. Opitek – Przeciwdziałanie praniu pieniędzy z wykorzystaniem walut wirtualnych, Prokuratura i Prawo 12, 2020
[49] Tamże
[50] https://isbiznes.pl/2023/01/13/przestepcy-lubia-kryptowaluty/ dostęp w dniu 19.01.2023 r.

kryptowalutami związanych z oszustwami, oprogramowaniem ransomware, finansowaniem terroryzmu i handlem ludźmi. Za to transakcje skradzionymi kryptowalutami wzrosły o 7%.

W odniesieniu do Polski raport firmy Chainalysis określił (dane od września 2021 r. do września 2022 r.) łączną wartość otrzymanych przez Polskę w tym czasie środków na 63,62 mld USD, co stanowi -0,22% wzrostu w stosunku do poprzedniego roku. Chainalysis zidentyfikowała wartość 384,0 milionów dolarów nielegalnych obrotów i 749,0 dolarów podejrzanej działalności w ww. okresie.

Największą kategorią działalności w Polsce była wymiana scentralizowana, na którą w okresie od września 2021 r. do września 2022 r wpłynęło 74,9% całej działalności. Drugą co do wielkości kategorią w Polsce było DeFi, które otrzymało 22,3%.

W Polsce najczęściej stosowaną platformą pod względem ruchu w sieci jest giełda Binance.com, która otrzymała 30,7 mln odwiedzin od września 2021 r. do września 2022 r. Drugą co do wielkości platformą był hostowany portfel o nazwie eToro.com, który w tym samym okresie odnotował 12,25 mln odwiedzin.

Nielegalna działalność w zakresie obrotu walutami wirtualnymi zidentyfikowana w Polsce od września 2021 r. do września 2022 r zmieniała się. Największe źródło nielegalnej działalności pochodziło z kategorii sankcji. W tej kategorii w ww. okresie wpłynęła kryptowaluta o wartości 75,47 mln USD. Najszybciej rozwijającą się kategorią przestępczości były skradzione fundusze, które wzrosły o 7,3% w stosunku do poprzednich 12 miesięcy, osiągając 26,58 mln USD łącznej wartości.

Z uwagi na to, że technologia NFT zyskuje na popularności, zaleca się podmiotom prowadzącym działalność gospodarczą polegającą na świadczeniu usług w zakresie walut wirtualnych zwracanie szczególnej uwagi na podejrzane portfele i transakcje NFT. Instytucje te mogą świadczyć swoje usługi w zakresie wymiany walut wirtualnych na NFT jedynie wtedy, gdy dokonują tego z wykorzystaniem transparentnych walut wirtualnych. GIIF podkreśla, że niedopuszczalne jest wykorzystywanie do tej wymiany tzw. AEC (ang, Anonymity enhanced cryptocurrencies), czyli kryptowalut zapewniających anonimowość. Stosowanie tych anonimizujących kryptowalut powoduje brak możliwości udowodnienia, że dana instytucja obowiązana wywiązała się z obowiązku stosowania właściwych środków bezpieczeństwa finansowego. Należy jednak podkreślić, że rynek NFT ewoluuje w rynek wtórny, przez co konieczne mogą okazać się konkretne regulacje, aby zapobiec wzrostowi ryzyka prania pieniędzy i finansowania terroryzmu na omawianym rynku.

Tokeny NFT mają szczególną podatność na pranie pieniędzy i finansowanie terroryzmu przez wzgląd na podobieństwo do dzieł sztuki oraz stosowaną technologię blockchain.

Podatność NFT w tym zakresie związana jest ze specyfiką handlu dziełami sztuki w szerszej domenie NFT. Na słabo regulowanym rynku NFT ta specyfika charakteryzuje się: wysokim poziomem anonimowości, ograniczonymi informacjami o nabywcach, samoregulującymi się rynkami, nieprzejrzystymi cenami i transakcjami o wysokiej wartości między nieznanymi stronami. Rynek NFT jest podatny na oszukańcze praktyki, a działania organów ścigania w przypadku oszustw z udziałem NFT są znacznie utrudnione.

Inną przyczyną podatności jest łatwość przenoszenia prawa do NFT, nierozerwalnie związana z podstawową technologią blockchain. Podobnie jak waluty wirtualne, przeniesienie prawa do

NFT nie jest ograniczone granicami geograficznymi i odbywa się bez potencjalnej interwencji regulacyjnej lub ponoszenia kosztów. Prawo do NFT może zatem szybko zmieniać uprawnionego i być przenoszone między różnymi portfelami i ostatecznymi beneficjentami. To sprawia, że rejestracja aktywów przez organy podatkowe lub inne jest bardzo trudna, ponieważ status jurysdykcyjny NFT nie jest jasny.

Następna podatność polega na ukrywaniu podstawowych danych dotyczących transakcji walut wirtualnych. Chociaż można prześledzić zmianę własności NFT między portfelami, zmiana adresu portfela nie odzwierciedla zmiany właściciela. Ponieważ większość głównych platform NFT nie wymaga identyfikacji klienta ani nie stosuje środków bezpieczeństwa finansowego wobec klienta, portfele ostatecznych właścicieli muszą być mapowane za pomocą bloków transakcyjnych, aby zobaczyć łańcuch portfeli, przez który przeszła waluta. Proces ten staje się bardziej skomplikowany przez „miksery" lub „tumblery" walut wirtualnych.

Zwiększona podatność NFT związana jest z łatwością ukrycia posiadania portfela. Po zlokalizowaniu portfeli beneficjentów należy je przypisać do osoby prawnej lub fizycznej. Portfele walut wirtualnych są w wielu jurysdykcjach pseudo-anonimowe, a zidentyfikowanie odpowiedzialnej osoby może wymagać zidentyfikowania odpowiedniego adresu IP, zastosowanego sprzętu i innych czynników, które mogą dotyczyć różnych jurysdykcji.

Jak wynika z posiadanych przez GIIF informacji instytucje sektora walut wirtualnych powinny analizować dane dotyczące przeprowadzanych transakcji i posiadać narzędzia do oceny dzienników zdarzeń. Z uwagi na koszty posiadania zaawansowanych, dedykowanych narzędzi informatycznych, nie wszystkie instytucje tego sektora dysponują takimi zaawansowanymi, automatycznymi narzędziami i systemami informatycznymi, wspomagającymi realizację celów przeciwdziałania praniu pieniędzy oraz finansowania terroryzmu.

W celu podnoszenia świadomości AML/CTF w instytucjach obowiązanych – w tym w sektorze walut wirtualnych, GIIF prowadził szkolenia dla instytucji obowiązanych i jednostek współpracujących, podczas których były przekazywane teoretyczne i praktyczne wskazówki dotyczące zagadnień przeciwdziałania praniu pieniędzy oraz finansowania terroryzmu. Dotyczyło to m.in. ustalania beneficjenta rzeczywistego oraz struktury własności i kontroli klientów, a także raportowania rozbieżności do organu właściwego w sprawie CRBR. Sam poziom świadomości AML/CTF w instytucjach obowiązanych przedmiotowego sektora walut wirtualnych znacznie się poprawił.

Z uwagi na trwający konflikt zbrojny na Ukrainie również w sektorze walut wirtualnych utrudnione jest pozyskanie szerszego spektrum dokumentów potwierdzających tożsamość lub wiarygodność klienta. I tu występują problemy z identyfikacją i weryfikacją osób, a występująca bariera językowa i kulturowa w istotny sposób wpływa na prawidłowe rozpoznanie czynników zwiększonego ryzyka. Występują również problemy z weryfikacją zagranicznych klientów w centralnych rejestrach beneficjentów rzeczywistych państw UE, zwłaszcza dotyczy to podmiotów o skomplikowanej strukturze kapitałowej.

Dostęp do usług oferowanych przez podmioty sektora walut wirtualnych jest relatywnie łatwy. Istnieją możliwości ukrycia danych identyfikacyjnych klientów (podmioty oferujące tego typu usługi mogą dokonywać identyfikacji klientów na odległość). Występują transakcje o złożonym i transgranicznym charakterze.

Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji dot. tego typu usług, jednak pochodzących od podmiotów będących IO albo udostępnionych przez zagraniczną jednostkę analityki finansowej. Istnieje prawdopodobieństwo, że przypadek ML czy FT w zakresie analizowanych scenariuszy nie zostanie wykryty.

Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie.

Istniejące przepisy prawne odpowiadają w częściowo zakresowi analizowanego ryzyka.

Zagrożenia w sektorze

Właściwie z każdym rokiem wzrasta wolumen obrotów na rynku kryptowalut, zarówno pod względem przetwarzanych transakcji, jak i liczby klientów firm, działających na tym rynku. Najistotniejszym czynnikiem zagrożenia na tym rynku wydaje się brak wystarczającej transparentności dokonywanych transakcji oraz kłopoty z ustaleniem tożsamości klientów końcowych zaangażowanych w dokonywanie transakcji na tym rynku. Może to ułatwiać pranie pieniędzy czy finansowanie terroryzmu.

Chociaż w warunkach polskich to bitcoin jest najczęściej używaną walutą wirtualną do popełniania przestępstw, to w warunkach europejskich widoczne są trendy zmiany w kierunku kryptowalut o zwiększonej anonimowości, które zapewniają większą anonimowość dokonywania transakcji. Kryptowaluty o zwiększonej anonimowości są jednak trudniejsze do zdobycia na rynku i zawierania nimi transakcji niż bitcoin.

W sektorze walut wirtualnych jako obszar działalności szczególnie narażony na ryzyko prania pieniędzy oraz finansowania terroryzmu został zidentyfikowany obszar działalności giełd/punktów obrotu kryptowalutami działających jako pośrednicy wymiany obsługiwanych przez instytucje finansowe oraz wykorzystywanie wirtualnych aktywów do transferowania wartości pochodzących z nielegalnych źródeł. GIIF zidentyfikował znaczący wzrost liczby osób fizycznych, występujących w charakterze tzw. partnerów innych instytucji obowiązanych, zajmujących się wymianą kryptowalut, prowadzący do trudności ze zbadaniem źródła pochodzenia środków. Ponadto zidentyfikowano przypadki, w których podmioty prowadzące działalność giełd/punktów obrotu kryptowalutami nie posiadały odpowiednich narzędzi/oprogramowań służących do bieżącego monitorowania transakcji klientów oraz identyfikacji transakcji podejrzanych. Nie badano z tego powodu źródła pochodzenia środków pieniężnych, nie dokonywano analiz adresów kryptowalutowych pod kątem źródła pochodzenia i legalności jednostek kryptowalut będących przedmiotem transakcji, nie dokonywano analiz przeprowadzanych transakcji, które są niezgodne z wiedzą o kliencie, a generują bardzo wysokie ryzyko prania pieniędzy i finansowania terroryzmu nie tylko na poziomie giełdy/punktu obrotu kryptowalutami, ale także na poziomie instytucji finansowej, która prowadzi rachunki na rzecz ww. podmiotów. W związku z powyższym ponieważ transakcje realizowane za pośrednictwem tego typu podmiotów są trudne do prześledzenia ze względu na specyfikę stosowanej technologii, to instytucje obowiązane powinny wnikliwie badać źródło pochodzenia środków obsługiwanych giełd/punktów obrotu kryptowalutami.

Zagrożeniem może być również możliwość szybkiego przeprowadzania transakcji pomiędzy różnymi jurysdykcjami, w których to jurysdykcjach obowiązki informacyjne związane z transferami wirtualnych aktywów nie zostały jeszcze w pełni wprowadzone.

W jurysdykcjach tych może też nie występować konieczność ujawniania tożsamości podmiotu dokonującego transakcji walutami wirtualnymi.

Sektor walut wirtualnych pod względem oceny zagrożenia praniem pieniędzy, ale też zagrożenia finansowania terroryzmu, jest potencjalnie sektorem wykorzystywanym w związku z przestępstwami źródłowymi dla prania pieniędzy oraz finansowania terroryzmu: przestępstwami skarbowymi, handlu narkotykami, przestępstwami przeciwko mieniu oraz przeciwko obrotowi gospodarczemu, korupcji, handlu ludźmi czy oszustwami.

Ponieważ wymiana aktywów wirtualnych staje się coraz bardziej uregulowana w przepisach dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, wiele zagrożeń powiązanych z nimi przeniosło się na rynek NFT. Duża skala zagrożenia wynika z nieprecyzyjnych regulacji prawnych dotyczących NFT. Ponieważ każdy NFT jest niepowtarzalny przez wzgląd na powiązane aktywa lub funkcje, może być wykorzystywany na wielu segmentach rynku: od obrotu dziełami sztuki po usługi finansowe. Ten brak przejrzystości w regulacjach powoduje luki w systemie monitoringu i zwalczaniu przestępstw prania pieniędzy i finansowania terroryzmu.

Same transakcje NFT powodują zagrożenie, obejmujące tradycyjne oszustwa, takie jak fałszowanie transakcji NFT i wprowadzanie w błąd nabywców. Zagrożenie to jest szczególnie istotne na rynkach NFT, które działają przy użyciu automatycznych inteligentnych kontraktów, przy minimalnych wymaganiach KYC i rzadko posiadają jakiekolwiek mechanizmy monitorowania. Jednak transakcje NFT również wykazują wiele zagrożeń związanych z ich podobieństwem do rynku sztuki. Obejmują one anonimowość, nierejestrowaną sprzedaż i zaangażowanie w transakcje podmiotów z jurysdykcji wysokiego ryzyka. Wyraźne zwiększenie zagrożenia transakcji występuje wtedy, gdy handel NFT następuje bez pośredników.

Jednym z podstawowych źródeł i sposobów finansowania ISIL, Al-Kaidy oraz stowarzyszonych z nimi organizacji terrorystycznych są darowizny kryptowalut za pośrednictwem aplikacji OTT (Over the Top). Sposób ten jest o tyle atrakcyjny, ponieważ użyte waluty wirtualne umożliwiają szybkie przeprowadzanie transakcji bez konieczności ujawniania tożsamości „właściciela". Transakcje dokonywane przez Internet mają ten walor, że pozwalają na interakcję z obszarami wysokiego ryzyka lub klientami wysokiego ryzyka, których nie można łatwo zidentyfikować, nawet jeśli transakcje pozostawiają w sieci identyfikowalne cyfrowe ślady. Kryptowaluty są atrakcyjne dla celów finansowania terroryzmu z uwagi na brak jasnych przepisów dotyczących walut wirtualnych w wielu jurysdykcjach, co powoduje też potencjalne możliwości bezpiecznego przeprowadzenia transakcji wymiany między kryptowalutami a walutami fiducjarnymi. Jak wskazuje ostatnia *ponadnarodowa ocena ryzyka* (SNRA) grupy terrorystyczne mogą być zainteresowane wykorzystaniem kryptowalut do finansowania działalności terrorystycznej. Zgłoszono ograniczoną, ale rosnącą liczbę przypadków związanych z kryptowalutami. Grupa Egmont natomiast wykryła przypadki grup terrorystycznych wykorzystujących kryptowaluty. W tym przypadku wiadomo, że grupy te przekazały instrukcje w Internecie (w tym za pośrednictwem Twittera) dotyczące korzystania z kryptowalut. Tymczasem Raport Europolu TE-SAT za 2020 r. zauważa jednak, że liczba spraw związanych z wykorzystaniem kryptowalut dla celów finansowania terroryzmu w 2020 r. pozostawała raczej na niskim poziomie. Nie zmieniło się to w roku 2021. Grupy terrorystyczne i ekstremistyczne coraz częściej używały natomiast metod finansowania

społecznościowego w połączeniu z wykorzystaniem kryptowalut, co miało zapewnić wyższy poziom anonimowości darczyńców i biorców. Przypadki te miały miejsce przede wszystkim w wypadku terroryzmu dżihadystycznego oraz w przypadku ekstremistycznych organizacji prawicowych.

Liczba sygnałów w Polsce o możliwości wykorzystania walut wirtualnych do finansowania terroryzmu jest niewielka.

Uśredniony poziom zagrożenia sektora walut wirtualnych – ML –3,0 i FT – 3,0

Uśredniony poziom podatności sektora walut wirtualnych – ML – 3,0 i FT – 3,0

Oszacowany poziom prawdopodobieństwa dla sektora – ML – 3,00 i FT - 3,00

Poziom ryzyka jest ostatecznie określany przez kombinację zagrożenia i podatności. Macierz ryzyka określająca ten poziom ryzyka opiera się na wadze 40% (zagrożenie) + 60% (podatność) – przy założeniu, że komponent podatności ma większą zdolność określania poziomu ryzyka. Zakłada się, że poziom podatności może zwiększyć atrakcyjność, a tym samym zamiary przestępców/terrorystów, aby użyć danego modus operandi – wpływając w ten sposób ostatecznie na poziom zagrożenia. Poziom ryzyka sektora, z uwzględniem prawdopobieństwa i konsekwencji (współczynnik 2,5 dla PP i 1,5 dla FT), jest ustalany zgodnie z metodyką krajowej oceny ryzyka – aneks nr 1.

Ryzyko FT sektora walut wirtualnych –2,40	
1 – 1,5	Niskie
1,6 – 2,5	Średnie
2,6 – 3,5	Wysokie
3,6 – 4	Bardzo wysokie
Ryzyko ML sektora walut wirtualnych – 2,80	
1 – 1,5	Niskie
1,6 – 2,5	Średnie
2,6 – 3,5	Wysokie
3,6 – 4	Bardzo wysokie

WNIOSEK 1: Poziom ryzyka wykorzystania sektora walut wirtualnych do finansowania terroryzmu w Polsce znajduje się na poziomie średnim.

WNIOSEK 2: Poziom ryzyka wykorzystania sektora walut wirtualnych do prania pieniędzy w Polsce znajduje się na poziomie wysokim.

Mitygacja zidentyfikowanych ryzyk:

W celu ograniczenia prawdopodobieństwa wykorzystania sektora walut wirtualnych do prania pieniędzy lub finansowania terroryzmu, zasadne jest podjęcie odpowiednich działań. Stosowanie zaproponowanych działań mitygujących powinno następować z uwzględnieniem rozpoznanego przez danę instytucję obowiązaną ryzyka.

Przedsiębiorcy zajmujący się sprzedażą walut wirtualnych za gotówkę, w przypadku zapłaty z wykorzystaniem większej ilości gotówki przez nierezydentów UE, zasadnym byłoby pozyskiwanie informacji na temat źródła pochodzenia wartości majątkowych, np. poprzez weryfikację deklaracji dewizowych klientów z państw spoza UE.

Podmioty sektora walut wirtualnych powinny wzmocnić działania związane z odpowiednią oceną stosunków gospodarczych klienta oraz uzyskiwaniem informacji na temat ich celu i zamierzonego charakteru, a także powinny podejmować działania zmierzające do usprawnienia bieżącego monitoringu stosunków gospodarczych. Instytucje obowiązane z sektora walut wirtualnych powinny zwracać uwagę na źródło pochodzenia wartości majątkowych klientów, przeprowadzających transakcje wymiany pomiędzy walutami wirtualnymi, gdy wymienianą walutą wirtualną jest waluta charakteryzująca się wyższym poziomem anonimowości.

W sektorze walut wirtualnych powinny być podejmowane działania podnoszące świadomość narażenia na przestępstwo prania pieniędzy oraz finansowania terroryzmu, jak również gwarantujące odpowiednie szkolenia pracowników tego sektora w analizie sygnałów ostrzegawczych wynikających z transakcji podejrzanych.

Z uwagi na szerokie spektrum działania podmiotów z sektora walut wirtualnych, podmioty te powinny dopilnować, aby ocena ryzyka podmiotu i była dostosowana do ich profilu działalności i uwzględniała czynniki i ryzyko charakterystyczne dla działalności firmy.

Zalecane jest rozwijanie przez instytucje sektora walut wirtualnych zaawansowanych narzędzi i systemów informatycznych, wspomagających realizację celów przeciwdziałania praniu pieniędzy oraz finansowania terroryzmu.

Organizowane powinny być szkolenia dla instytucji obowiązanych z sektora walut wirtualnych, podczas których będą przekazywane teoretyczne i praktyczne wskazówki dotyczące ustalania beneficjenta rzeczywistego oraz struktury własności i kontroli klientów, a także raportowania rozbieżności do organu właściwego w sprawie CRBR. Zalecane jest uczestnictwo przedstawicieli instytucji obowiązanych w szkoleniach podnoszących świadomość AML/CTF, organizowanych zarówno przez GIIF, jak i przez UKNF w ramach Programu CEDUR.

Instytucje obowiązane powinny położyć szczególny nacisk na ustalenie danych dotyczących źródła pochodzenia transferowanych wartości majątkowych.

Instytucje obowiązane powinny przykładać szczególną wagę do czynników geograficznych mogących wskazywać na wyższe ryzyko prania pieniędzy czy też finansowania terroryzmu, takich jak niestabilna sytuacja polityczna czy konflikt zbrojny, czego najdobitniejszym przykładem w ostatnich latach jest wojna prowadzona przez Rosję przeciwko Ukrainie. Z uwagi na wysokie ryzyko transferowania środków pochodzących z nielegalnego handlu,

przemytu ludzi, handlu bronią, czy też działań zmierzających do omijania sankcji gospodarczych, szczególnie istotne jest analizowanie przez instytucje obowiązane nie tylko danych dotyczących samych stron transakcji, ale również beneficjentów rzeczywistych, czy też faktycznych celów przeprowadzania danych transakcji.

Istotnym czynnikiem ograniczającym ryzyka związane z sektorem walut wirtualnych, na poziomie systemowym, powinno być przyjęcie i wdrożenie rozwiązań przewidzianych w *Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2023/1114 z dnia 31 maja 2023 r. w sprawie rynków kryptoaktywów oraz zmiany rozporządzeń (UE) nr 1093/2010 i (UE) nr 1095/2010* oraz *dyrektyw 2013/36/UE i (UE) 2019/1937* oraz *Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2023/1113 z dnia 31 maja 2023 r. w sprawie informacji towarzyszących transferom środków pieniężnych i niektórych kryptoaktywów oraz zmiany dyrektywy (UE) 2015/849*. Ujednolicenie na poziomie UE podejścia do obowiązków podmiotów z sektora walut wirtualnych powinno ograniczyć obserwowane obecnie działania sprowadzające się do migracji podmiotów z sektora walut wirtualnych pomiędzy poszczególnymi jurysdykcjami z obszaru UE, celem wyboru jurysdykcji o pasujących dla danego podmiotu wymaganiach (w domyśle – najmniej rygorystycznych), z jednoczesnym zachowaniem uprawnienia do świadczenia usług na terenie całej wspólnoty.

7. Obszar – usługi telekomunikacyjne powiązane z płatnościami mobilnymi

Opis sektora – zawarty jest w podrozdziale 7.2.1 - „Podatność rynku finansowego".

Scenariusze wystąpienia ryzyka (tj. możliwe przykłady wystąpienia ryzyka) dotyczyły wykorzystania do prania pieniędzy usługi telekomunikacyjnej dotyczącej numerów o podwyższonej płatności, a do finansowania terroryzmu produktów i usług finansowych w postaci płatności dokonywanych za pomocą telefonu komórkowego. Opis scenariuszy znajduje się poniżej.

Pranie pieniędzy

Tabela 35

Rodzaj wykorzystanych usług, produktów finansowych	Usługi telekomunikacyjne dot. numerów o podwyższonej płatności
Ogólny opis ryzyka	Wykorzystanie usług telekomunikacyjnych w zakresie numerów o podwyższonej płatności do legitymizowania środków z przestępczej działalności
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	Zawarcie umowy na świadczenie usług telekomunikacyjnych dot. rejestrowanych numerów o podwyższonej płatności (typu Premium) na rzecz osób podstawionych (tzw. słupów), celem zapewnienia anonimowości sprawców. Następnie za pomocą odpowiednich kodów wykonywanie są określone połączenia przez przestępców lub osoby z nimi powiązane, za które pobierane są wysokie opłaty. Część uzyskanego zysku stanowi zapłata dla "słupa", a pozostała większość jest wykorzystywana przez przestępców jako "wyprane" pieniądze.
Poziom podatności	4
Uzasadnienie dla poziomu podatności	Możliwość świadczenia tego typu usług, a także dostęp do nich jest relatywnie łatwy. Istnieje możliwość ukrycia danych identyfikacyjnych klientów (przy wykorzystaniu słupów lub ewentualnie zagranicznych numerów telefonów). Mogą występować transakcje o charakterze międzynarodowym. Podmioty oferujące te usługi nie są IO. Organy administracji publicznej posiadają podstawową wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF nie ma możliwości gromadzenia i analizowania informacji dot. tego typu usług. Istnieje prawdopodobieństwo, że przypadek prania pieniędzy w zakresie analizowanych scenariuszy nie zostanie wykryty. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne nie odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	2
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie usług telekomunikacyjnych w zakresie numerów o podwyższonej płatności do legitymizowania środków z przestępczej działalności może być jedną z metod prania pieniędzy. GIIF otrzymywał nieliczne informacje o wykorzystywaniu takiego *modus operandi* do przestępstwa prania pieniędzy, ale ten sposób jest postrzegany jako mało atrakcyjny i stosunkowo niebezpieczny. Podmiot realizujący usługi telekomunikacyjne w zakresie numerów o podwyższonej płatności zobowiązany jest przekazywać wymagane przepisami ustawy informacje do prowadzonego przez Prezesa Urzędu Komunikacji Elektronicznej rejestru[51]. Potrzebne jest planowanie, wiedza i umiejętności do zastosowania tego *modus operandi*. Nie jest to też sposób tani. WNIOSEK: wykorzystanie usług telekomunikacyjnych w zakresie numerów o podwyższonej płatności do legitymizowania środków z przestępczej działalności stwarza średnie zagrożenie dla prania pieniędzy.

[51] https://bip.uke.gov.pl/zgloszenia-do-rejestru-premium/zgloszenia-do-rejestru-premium-rate,1.html

Finansowanie terroryzmu

Tabela 36

Rodzaj wykorzystanych usług, produktów finansowych	Płatności dokonywane za pomocą telefonu komórkowego
Ogólny opis ryzyka	Nabywanie lub doładowanie kart SIM w celu przekazywania środków
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	Korzystanie z mobilnych płatności, niestosujących w odpowiednim zakresie środków bezpieczeństwa finansowego, w celu finansowania terroryzmu w sposób utrudniający identyfikacje zleceniodawcy i beneficjenta transakcji, np.: zwolennicy organizacji terrorystycznej przekazują płatności mobilne (w debet swoich rachunków telefonicznych) na rzecz jednej osoby, która następnie wypłaca otrzymane pieniądze w gotówce w bankomacie, aby przekazać je na cele organizacji terrorystycznej.
Poziom podatności	4
Uzasadnienie dla poziomu podatności	Możliwość świadczenia tego typu usług, a także dostęp do nich jest relatywnie łatwy. Istnieje możliwość ukrycia danych identyfikacyjnych klientów (przy wykorzystaniu słupów lub ewentualnie zagranicznych numerów tel.). Mogą występować transakcje o charakterze międzynarodowym. Podmioty oferujące te usługi nie są IO. Organy administracji publicznej posiadają podstawową wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF nie ma możliwość gromadzenia i analizowania informacji dot. tego typu usług. Istnieje prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy nie zostanie wykryty. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne nie odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	1
Uzasadnienie dla poziomu zagrożenia	Nabywanie lub doładowanie kart SIM w celu przekazywania środków jest jednym z bezpieczniejszych i szybkich sposobów finansowania działań o charakterze terrorystycznym. Korzystanie z mobilnych systemów płatności, w których nie stosuje się w odpowiednim zakresie środków bezpieczeństwa finansowego, jest tanie i atrakcyjne. Wystarczy w aplikacji mobilnej uruchomić opcję transferów na numer telefonu lub przekazać środki beneficjentowi do wypłaty w bankomacie. W Polsce jednak brak jest jednoznacznej informacji o wykorzystywaniu tego *modus operandi* dla celów finansowania działalności terrorystycznej. Ograniczeniem anonimowości jest wprowadzony w Polsce w 2017 r. obowiązek rejestracji numerów prepaid tak, aby każdy numer telefonu miał swojego jasno określonego użytkownika. WNIOSEK: Wykorzystanie nabywania lub doładowania kart SIM w celu przekazywania/gromadzenia środków na działalność terrorystyczną stwarza niskie zagrożenie finansowaniem terroryzmu.

Tabela 37

Rodzaj wykorzystanych usług, produktów finansowych	Usługi telekomunikacyjne dot. numerów o podwyższonej płatności
Ogólny opis ryzyka	Wykorzystanie usług telekomunikacyjnych w zakresie numerów o podwyższonej płatności do gromadzenia środków na działalność terrorystyczną
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	Zawarcie umowy na świadczenie usług telekomunikacyjnych dot. rejestrowanych numerów o podwyższonej płatności (typu *Premium*) na rzecz osób podstawionych (tzw. słupów) celem zapewnienia anonimowości sprawców. Następnie za pomocą odpowiednich kodów wykonywane są określone połączenia przez zwolenników organizacji terrorystycznej, za które pobierane są wysokie opłaty. Część uzyskanego zysku stanowi zapłata dla "słupa", a pozostała większość jest przekazywana na cele działalności terrorystycznej.

Poziom podatności	4
Uzasadnienie dla poziomu podatności	Możliwość świadczenia tego typu usług, a także dostęp do nich jest relatywnie łatwy. Istnieje możliwość ukrycia danych identyfikacyjnych klientów (przy wykorzystaniu słupów lub ewentualnie zagranicznych numerów tel.). Mogą występować transakcje o charakterze międzynarodowym. Podmioty oferujące te usługi nie są IO. Organy administracji publicznej posiadają podstawową wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF nie ma możliwości gromadzenia i analizowania informacji dot. tego typu usług. Istnieje prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy nie zostanie wykryty. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne nie odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	2
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie usług telekomunikacyjnych w zakresie numerów o podwyższonej płatności (usługi typu PREMIUM) do gromadzenia środków na działalność terrorystyczną jest jedną ze zidentyfikowanych metod finansowania terroryzmu. Chociaż w Polsce brak jest jednoznacznej informacji o wykorzystywaniu tego *modus operandi*, to ABW odnotowała w przeszłości przypadki angażowania się cudzoziemców z państw podwyższonego ryzyka w oszustwa telekomunikacyjne z użyciem numerów typu PREMIUM, z których dochody najprawdopodobniej przeznaczane były na działalność ugrupowań terrorystycznych. Dla celów finansowania działalności terrorystycznej sposób jest postrzegany jako stosunkowo atrakcyjny, rozproszone grono zwolenników lub osób popierających działania terrorystyczne może w łatwy sposób wspomagać/zasilać nisko kwotowo podmiot prowadzący usługi telekomunikacyjne w zakresie numerów o podwyższonej płatności. Zyski z takiej działalności przeznaczane są na działalność terrorystyczną. Potrzebne jest planowanie, wiedza i umiejętności do zastosowania tego *modus operandi*. Nie jest to jednak sposób tani. WNIOSEK: Wykorzystanie usług telekomunikacyjnych w zakresie numerów o podwyższonej płatności (usługi typu PREMIUM) do gromadzenia środków na działalność terrorystyczną stwarza średnie zagrożenie finansowaniem terroryzmu.

Płatności mobilne są to płatności bezgotówkowe dokonywane za pomocą urządzenia mobilnego[52] (np. smartfonu lub tabletu) i technologii mobilnych (np. NFC, SMS, USSD, WAP). Urządzenia mobilne muszą mieć możliwość połączenia się z siecią telekomunikacyjną (komórkową lub Internetem), a dokonywanie płatności odbywa się zazwyczaj w aplikacji bankowej lub płatniczej. Płatności mobilne można podzielić na:

- zbliżeniowe – wykorzystujące technologię NFC i stosowane przede wszystkim w płatnościach w terminalach POS, maszynach vendingowych, parkomatach czy bramkach na autostradach;
- zdalne – wykorzystujące połączenie internetowe lub technologię GSM i stosowane przede wszystkim w sklepach internetowych, pomiędzy użytkownikami (płatność mobilna typu *Peer-to-Peer* – P2P), przy opłatach za parkowanie i transport miejski, a także w mniejszym zakresie w terminalach POS.

Dostępne obecnie rozwiązania mobilne umożliwiają także realizowanie wypłat gotówkowych (z bankomatów oraz w kasach sklepowych w formie usługi *cash back*), zarówno zbliżeniowo, jak i zdalnie. Większość rozwiązań mobilnych w Polsce funkcjonuje w oparciu o karty płatnicze (np. Google Wallet, Apple Pay), co pozwala na korzystanie z możliwości oferowanych przez schematy kart płatniczych. Przykładowo, w przypadku ewentualnego

[52] https://www.nbp.pl/home.aspx?f=/edukacja/zasoby/broszury/platnosci-mobilne.html dostęp 23.01.2023 r.

oszustwa poszkodowani klienci mogą ubiegać się o zwrot utraconych środków w ramach procedury *chargeback*. Z kolei system BLIK funkcjonuje w oparciu o mobilny dostęp do środków zgromadzonych bezpośrednio na rachunku bankowym. Nowoczesne płatności mobilne należą do najbezpieczniejszych form dokonywania płatności. W przypadku rozwiązań mobilnych opartych na kartach płatniczych stosuje się tokenizację[53] oraz zabezpieczenia biometryczne (np. używanie odcisku palca, biometrii tęczówki oka lub twarzy do potwierdzania transakcji przez użytkownika). Od drugiej połowy 2021 r. możliwa jest także zbliżeniowa płatność BLIKIEM, generowany jest na ekranie telefonu użytkownika jednorazowy, 6-cyfrowy kod, który jest ważny jedynie przez 2 minuty.

Wśród mobilnych płatności zbliżeniowych - w zależności od posiadanego urządzenia - możemy wyróżnić:

- płatności telefonem - możliwe są zarówno zbliżeniowo, w technologii NFC (np. Apple Pay, Google Pay, Blik zbliżeniowy, HCE), jak i bez niej (Blik z kodem);
- płatności zegarkiem - do tej grupy należą Garmin Pay i Fitbit Pay, SwatchPay! i Xiaomi Pay.

W badaniu przeprowadzonym przez firmę Blue Media „Finanse Polaków w czasach postpandemicznych 2022”[54] (badanie przeprowadzone w czerwcu 2022 r.) - niemal połowa Polaków (46 %) płaci za zakupy w Internecie BLIKiem. To obecnie najczęściej wybierana forma płatności, której popularność od kilku lat sukcesywnie rośnie. W 2022 roku BLIK wdrożył dodatkową funkcjonalność polegającą tylko na zbliżeniu telefonu do czytnika kart płatniczych.

Wśród głównych barier w korzystaniu z płatności mobilnych są:

- brak świadomości na temat możliwości tego typu płatności. Potencjalni użytkownicy mogą nie być świadomi korzyści takiego rozwiązania;
- bariera użytkowa, w wyniku której użytkownicy nie rozumieją działania technologii i nie umieją jej obsługiwać;
- brak świadomości zagrożeń, jakie stwarza korzystanie z technologii;
- bariery psychologiczne, takie jak przywiązanie do tradycyjnych metod płatności i niekorzystny odbiór nowinek technologicznych, szczególnie wśród starszych odbiorców.

Te czynniki powodują pewne zniechęcenie wobec płatności mobilnych.

Dynamiczny rozwój płatności mobilnych ma duży związek z obawami społeczeństwa dotyczącymi zdrowia i bezpieczeństwa sanitarnego. Podczas pandemii COVID-19 Światowa Organizacja Zdrowia zwróciła się do konsumentów o szersze korzystanie z cyfrowych metod płatności zbliżeniowych w swoich działaniach finansowych. WHO twierdziła, że koronawirusy na banknotach i monetach mogą przeżyć nawet do 3 dni. Takie m.in. informacje były powodem zwiększenia limitów w transakcjach bezgotówkowych na terenie większości krajów świata, aby

[53] Tokenizacja - dane karty płatniczej oraz konkretnej transakcji są zastępowane innym ciągiem cyfr, tj. tokenem, przez co dane te są niedostępne dla osób trzecich, np. dla sprzedawców.

[54] https://bluemedia.pl/baza-wiedzy/badania-i-raporty/blik-metoda-platnosci-deklasuje-inne-220709, dostęp 23.01.2023 r.

klienci mogli dokonywać większych zakupów bez ograniczeń i bez konieczności operowania pieniędzmi fizycznymi.

Badania statystyczne mówią, że w 2020 r. niemal połowa konsumentów w wieku 18-54 lat korzystała z portfeli mobilnych. Najliczniej reprezentowaną grupą byli millenialsi (24-39 lat). Z kolei, według badania Cornerstone Advisors[55], w grudniu 2020 r. prawie 80 % właścicieli smartfonów miało na swoim smartfonie co najmniej jedną aplikację do płatności mobilnych, przy czym aplikacja PayPal była zainstalowana na 65 % wszystkich smartfonów.

W 2021 roku globalna wartość rynku płatności mobilnych[56] wyniosła prawie 2 biliony dolarów (2000000000000$). Szacuje się, że korzysta z nich już ćwierć populacji świata, a do 2024 roku udział wykorzystania płatności wzrośnie o kolejne 30 %

Najwięcej użytkowników mobilnych płatności odnotowały Chiny, w których już 87 % obywateli używało m-płatności. Na drugim miejscu była Korea Południowa, która mogła pochwalić się wynikiem prawie 46 % Trzecie były Stany Zjednoczone z wynikiem 43%, później Indie z 40% Co ciekawe, Japończycy, którzy odpowiadają za pierwsze wdrożenia tych technologii byli dopiero na piątym miejscu, z wynikiem 35% użytkowników mobilnych płatności.

Najwięcej na świecie użytkowników miały chińskie aplikacje[57] do płatności mobilnych. AliPay jest największą usługą tego typu na świecie. O jej wadze możemy się przekonać, gdy zauważymy, że w 2019 r. przetworzyła wolumen transakcji o łącznej wartości 17 bilionów dolarów. WeChat Pay z kolei jest domyślną usługą płatniczą dla WeChat, czyli największego chińskiego serwisu społecznościowego. Poza Chinami na świecie najpopularniejsze jest Apple Pay, które ma największy wolumen transakcji.

Podatność sektora

Możliwość wykorzystania płatności mobilnych oraz usług telekomunikacyjnych w zakresie numerów o podwyższonej płatności do legitymizowania środków z przestępczej działalności, a także dostęp do nich jest relatywnie łatwy. Istnieje natomiast możliwość ukrycia danych identyfikacyjnych klientów (przy wykorzystaniu słupów lub ewentualnie zagranicznych numerów telefonów). Mogą też występować transakcje o charakterze międzynarodowym. Podmioty oferujące usługi w przedmiotowym sektorze nie są instytucjami obowiązanymi.

Płatności mobilne umożliwiają nie tylko bezgotówkowy zakup różnych przedmiotów i usług, ale także przekazywanie środków między rachunkami. Te płatności bezgotówkowe, dokonywane są przy wykorzystaniu urządzenia mobilnego (smartfon, tablet, smartwatch) za pomocą technologii mobilnych, takich jak np. SMS, NFC, USSD, WAP. Konieczna jest też łączność z siecią telekomunikacyjną (GSM czy Internet).

Usługi telekomunikacyjne stanowią wszystkie usługi, dotyczące transmisji, emisji i odbioru sygnałów, tekstów, obrazów i dźwięków lub wszelkiego rodzaju informacji drogą kablową, radiową, optyczną lub za pośrednictwem innych systemów elektromagnetycznych. Samo świadczenie usług telekomunikacyjnych stanowi działalność telekomunikacyjną, z której prowadzeniem wiąże się obowiązek dokonania wpisu do rejestru przedsiębiorców

[55] https://mobiletrends.pl/stan-platnosci-mobilnych-kiedys-i-dzis/ dostęp 23.01.2023 r.
[56] Tamże
[57] Tamże

telekomunikacyjnych, prowadzonego przez Urząd Komunikacji Elektronicznej – i to bez względu na ich publiczny albo niepubliczny charakter.

W trakcie pandemii COVID-19 nastąpił wzrost zainteresowania płatnościami mobilnymi. Nastąpił też wzrost wartości transakcji mobilnych na rynku wywołany zamykaniem oddziałów i biur instytucji finansowych (lub ich działaniem w ograniczonym wymiarze czasowym). Spowodowało to jednocześnie zainteresowanie sektorem płatności mobilnych zarówno przez przestępców, jak i zorganizowane grupy przestępcze.

Firmy zajmujące się technologią finansową (FinTech) wykorzystują technologię do oferowania usług finansowych w połączeniu z wykorzystaniem usług telekomunikacyjnych, na przykład bankowości internetowej i aplikacji do płatności mobilnych. Jak wynika z raportu „Digital 2021[58]", na przełomie 2020 i 2021 roku liczba ludzi na całym świecie wyniosła 7,83 miliarda. Ponad połowa, bo 5,22 miliarda, to użytkownicy telefonów komórkowych (niekoniecznie jednak smartfonów). Nieco mniej – 4,66 miliarda, co daje 59,5% populacji – korzystało z Internetu. Potencjalnie każdy z użytkowników smartfonów może korzystać z aplikacji pozwalających na płatności mobilne. Płatności mobilne są już wykorzystywane np. przez wielu emigrantów i pracowników sezonowych, którzy chcą wysłać część swoich zarobków do domu, aby wesprzeć swoje rodziny. Przekazy płatności mobilnych zastępują korzystanie z tradycyjnych banków i firm świadczących usługi pieniężne, które pobierały wysokie opłaty za małe przelewy. Jednocześnie płatności mobilne zachęciły niektórych użytkowników do omijania korzystania z podziemnych systemów przekazów pieniężnych, takich jak hawala.

W działalności podmiotów przedmiotowego sektora mogą występować kłopoty związane z pozyskaniem od klientów szerszego spektrum dokumentów potwierdzających tożsamość lub wiarygodność klienta. W Polsce każda karta SIM sprzedawana w Polsce musi być zarejestrowana pod prawdziwym imieniem i nazwiskiem nabywcy. Rejestracja karty SIM wymaga podania numeru PESEL, a w przypadku telefonów firmowych numeru REGON lub NIP. Karty prepaid bez potwierdzonej tożsamości właściciela utraciły ważność 1 lutego 2017. Jednakże nie we wszystkich krajach, nawet sąsiednich, istnieje obowiązek rejestracji kart SIM. W sieci Internet można znaleźć zarówno pojedyncze ogłoszenia, jak i wyspecjalizowane e-sklepy powstałe wyłącznie w celu sprzedaży takich kart. W jednym z nich znajdziemy karty np. czeskich operatorów, które będą działały bez rejestracji.

W związku z konfliktem na Ukrainie i obecnością w Polsce dużej liczby uchodźców występują poważne problemy z identyfikacją i weryfikacją osób. Występująca bariera językowa i kulturowa w istotny sposób wpływa na prawidłowe rozpoznanie czynników zwiększonego ryzyka. Każdy uchodźca może potencjalnie nabyć telefon komórkowy i dokonywać płatności mobilnych.

Płatności mobilne stwarzają duże możliwości wykorzystania ich w celu finansowania terroryzmu. Rozwój technologii telekomunikacyjnych, zmniejszenie wykluczenia telekomunikacyjnego i informacyjnego (Internet), szybkie rozprzestrzenianie się aplikacji pozwalających na płatności mobilne, przyczyniło się do dynamicznego rozwoju usług finansowych, nawet w krajach wydawałoby słabo rozwiniętych gospodarczo. Również w krajach, które są krajami podwyższonego ryzyka terrorystycznego czy w krajach będących strefami konfliktów czy leżących obok takich stref. W wielu z takich krajów usługi finansowe

[58] https://datareportal.com/reports/digital-2021-global-overview-report dostęp 23.01.2023 r.

są obecnie oferowane właśnie za pośrednictwem telefonów komórkowych. Posiadacze telefonów mogą płacić rachunki, przesyłać pieniądze, otrzymywać kredyty, otwierać konta i sprawdzać salda. Telefonem można nawet przesyłać pracownikom wynagrodzenie, nie wspominając o możliwości płatności telefonem za usługi i towary. Ponieważ fundusze wykorzystywane do finansowania terroryzmu mogą pochodzić zarówno z legalnych, jak i nielegalnych źródeł, potencjalnie środki finansowe można przekazać właśnie w formie płatności mobilnych. Ma to istotne znaczenie np. przy wyjazdach osób w strefy konfliktu (np. Foreign Terrorist Fighters). Bojownicy mogą przed wyjazdem wpłacić pieniądze, a następnie wypłacić je po przybyciu na miejsce bądź w krajach sąsiednich. Takie postępowanie jest o wiele efektywniejsze w porównaniu z noszeniem znacznej ilości gotówki. Płatności mobilne pozwalają omijać zarówno tradycyjne banki, jak i bankomaty. Wykorzystanie aplikacji pozwalających na płatności mobilne potencjalnie zapewnia wirtualny bankomat lub wirtualny portfel każdemu, kto zdecydowałby się na finansowanie terroryzmu z wykorzystaniem telefonu komórkowego. Ponadto mogą wystąpić praktyczne problemy z określeniem miejsca popełnienia przestępstwa i jurysdykcji karnej w przypadkach transakcji transgranicznych i przy udziale obcokrajowców, a także mogą być kwestionowane kompetencje organów ścigania do prowadzenia konkretnych postepowań karnych. W wielu przypadkach wystąpią problemy w zakresie możliwości śledzenia płatności mobilnych dokonywanych przez telefon.

Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w zakresie przedmiotowego sektora. GIIF nie ma możliwości gromadzenia i analizowania informacji dotyczących tego typu usług. Istnieje prawdopodobieństwo, że przypadek dotyczący prania pieniędzy czy finansowania terroryzmu nie zostanie wykryty.

Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie.

Istniejące przepisy prawne nie odpowiadają w dużej części zakresowi analizowanego ryzyka.

Zagrożenia w sektorze

Sektor płatności mobilnych pod względem oceny zagrożenia praniem pieniędzy, ale też zagrożenia finansowania terroryzmu, jest sektorem potencjalnie mogącym być wykorzystanym w związku z przestępstwami źródłowymi dla prania pieniędzy oraz finansowania terroryzmu. Nowe sposoby płatności generują swego rodzaju nowe typy wyłudzeń i oszustw. Najwięcej dotyczy wciąż kradzieży tożsamości (phishing) – aż 71 % sprzedających identyfikuje takie oszustwa[59] – przejęta przez przestępców może być karta kredytowa, urządzenie mobilne (w tym karta SIM), lub program lojalnościowy, z którego punkty mogą służyć do dokonywania płatności. Kolejnym oszustwem jest pharming (66 %), polegający na przekierowaniu użytkownika na fałszywą stronę www i przejęcie jego hasła, danych rachunku lub karty kredytowej. Przedmiotem tych działań są zarówno użytkownicy serwisów zakupowych jak i sami dostawcy poprzez atakowanie ich przez hackerskie oprogramowanie. Przybiera to coraz częściej formę wymiany fałszywych informacji między serwisem a jego niczego nieświadomymi użytkownikami. Mogą wystąpić też tzw. wyłudzenia „przyjacielskie". Przestępcy informują firmę, że karta, którą dokonano transakcji została ukradziona i proszą o zwrot pieniędzy – korzyścią nie jest tylko przejęcie zamówionych towarów lub usług. Do

[59] https://fintek.pl/oszustwa-podazaja-rozwojem-platnosci-mobilnych/ dostęp 23.01.2023 r.

dokonania tej transakcji potrzebne są dane pośrednika, który otrzymuje zamówione przedmioty, wyłudzającym chodzi natomiast o pieniądze.

Usługi płatności mobilnych mogą być wykorzystywane do prania pieniędzy czy finansowania terroryzmu nawet bez nawiązywania bezpośrednich relacji biznesowych. Same relacje biznesowe na linii dostawca – użytkownik usług płatności mobilnych mogą być ustanowione poprzez agentów, online lub poprzez system płatności mobilnych. Takie zagrożone anonimizacją usługi płatności mobilnych mogą umożliwiać istniejące na rynku, przede wszystkim w innych jurysdykcjach, zanonimizowane produkty – zwłaszcza karty przedpłacone, które mogą być podłączone do usług płatności mobilnych. Zweryfikowanie tożsamości klienta może być w takim przypadku utrudnione. O ile same mechanizmy monitorowania i raportowania transakcji podejrzanych mogą działać skutecznie, to brak skutecznej identyfikacji użytkownika płatności mobilnych może stwarzać problem. Jednakże to konkretne instytucje finansowe decydują, czy ich karty będą działać z produktami płatności mobilnych, jak np. Google Pay czy Apple Pay. Konkretna instytucja finansowa może ograniczyć możliwość dokonywania płatności mobilnych w przypadku części lub wszystkich kart.

Zagrożenie w kontekście prania pieniędzy czy finansowania terroryzmu może wypływać również ze względu na techniczny sposób przeprowadzania płatności mobilnych. Większość usług płatności mobilnych opartych jest na modelu bankowym, czyli podłączeniu środków finansowych z rachunku bankowego lub karty płatniczej. Jednakże niektóre usługi płatności mobilnych nie wykorzystują modelu bankowego, a naładowanie wirtualnej portmonetki może nastąpić innymi metodami, np. *online*, nawet od niezidentyfikowanego kontrahenta. Takie możliwości finansowania wirtualnej portmonetki zaciemniają pochodzenie funduszy, tworząc wyższe ryzyko prania pieniędzy i finansowania terroryzmu. Należy również uwzględnić fakt, że użytkownicy płatności mobilnych mają dostęp do środków pieniężnych za pośrednictwem międzynarodowych sieci bankomatów. Dostęp do gotówki poprzez bankomaty istotnie zwiększa poziom ryzyka prania pieniędzy i finansowania terroryzmu, ponieważ pozwala na przekazanie środków pieniężnych w jednym kraju i ich wypłatę w innym.

Innym zagrożeniem w kontekście prania pieniędzy czy finansowania terroryzmu może być cyfrowy smurfing. Użytkownikom aplikacji obsługujących płatności mobilne można mianowicie dać brudne pieniądze i skierować je do załadowania ich telefonów komórkowych cyfrową wartością – zgodnie z wszelkimi obowiązującymi limitami prawnymi lub sprawozdawczymi. Następnie użytkownicy aplikacji obsługujących płatności mobilne dokonują wielokrotnych transakcji przekazywania wartości na konta kontrolowane przez przestępczość zorganizowaną. W wyniku zastosowania takich form prania pieniędzy przestępcy są w stanie uniknąć takich niedogodności jak transport wielkich ilości posiadanej gotówki oraz uniknąć wymogów sprawozdawczości finansowej.

Większość jednostek analityki finansowej, w tym GIIF, nie otrzymuje informacji o przepływach dotyczących płatności mobilnych. Brak jest właściwego modelowania analitycznego takich transakcji, co praktycznie uniemożliwia ich przetwarzanie i analizowanie. Brak jest też praktycznych możliwości śledzenia i monitorowania płatności mobilnych, a zniszczenie dowodu w postaci telefonu, trudność odtworzenia lub ustalenia informacji, które znajdowały się w telefonie, znacznie utrudnia dochodzenia organów ścigania.

Uśredniony poziom zagrożenia sektora usług telekomunikacyjnych powiązanych z płatnościami mobilnymi – ML – 2,0 i FT – 1

Uśredniony poziom podatności sektora usług telekomunikacyjnych powiązanych z płatnościami mobilnymi – ML – 4,0 i FT – 4

Oszacowany poziom prawdopodobieństwa dla sektora – ML – 3,20 i FT - 2,80

Poziom ryzyka jest ostatecznie określany przez kombinację zagrożenia i podatności. Macierz ryzyka określająca ten poziom ryzyka opiera się na wadze 40% (zagrożenie) + 60% (podatność) – przy założeniu, że komponent podatności ma większą zdolność określania poziomu ryzyka. Zakłada się, że poziom podatności może zwiększyć atrakcyjność, a tym samym zamiary przestępców/terrorystów, aby użyć danego modus operandi – wpływając w ten sposób ostatecznie na poziom zagrożenia. Poziom ryzyka sektora, z uwzględniem prawdopobieństwa i konsekwencji (współczynnik 2,5 dla PP i 1,5 dla FT), jest ustalany zgodnie z metodyką krajowej oceny ryzyka – aneks nr 1.

Ryzyko FT sektora usług telekomunikacyjnych powiązanych z płatnościami mobilnymi – 2,28	
1 – 1,5	Niskie
1,6 – 2,5	Średnie
2,6 – 3,5	Wysokie
3,6 – 4	Bardzo wysokie
Ryzyko ML sektora usług telekomunikacyjnych powiązanych z płatnościami mobilnymi – 2,92	
1 – 1,5	Niskie
1,6 – 2,5	Średnie
2,6 – 3,5	Wysokie
3,6 – 4	Bardzo wysokie

WNIOSEK 1: Poziom ryzyka wykorzystania sektora usług telekomunikacyjnych powiązanych z płatnościami mobilnymi do finansowania terroryzmu w Polsce znajduje się na poziomie średnim.

WNIOSEK 2: Poziom ryzyka wykorzystania sektora usług telekomunikacyjnych powiązanych z płatnościami mobilnymi do prania pieniędzy w Polsce znajduje się na poziomie wysokim.

Mitygacja zidentyfikowanych ryzyk:

W celu ograniczenia prawdopodobieństwa wykorzystania usług telekomunikacyjnych powiązanych z płatnościami mobilnymi do prania pieniędzy lub finansowania terroryzmu, zasadne jest podjęcie odpowiednich działań. Stosowanie zaproponowanych działań mitygujących powinno następować z uwzględnieniem rozpoznanego przez danę instytucję obowiązaną ryzyka.

Instytucje obowiązane powinny skrupulatnie podchodzić do kwestii oceny ryzyka klienta świadczącego usługi telekomunikacyjne powiązane z płatnościami mobilnymi, podejmując odpowiednie środki ograniczające, dostosowując zakres stosowanych środków bezpieczeństwa finansowego do profilu działalności klienta. Jednocześnie w przypadkach mogących budzić wątpliwości, takich jak duże różnice w wolumenie płatności pomiędzy badanymi okresami, zasadne jest pozyskiwanie od klienta instytucji obowiązanej informacji na temat źródła pochodzenia wartości majątkowych.

W przypadku korzystania przez klienta instytucji obowiązanej z rozwiązań umożliwiających płatności przez terminale płatnicze czy też z aplikacji służących realizowaniu płatności, czynnikiem branym pod uwagę przez instytucje obowiązane powinny być okoliczności wskazujące na nieproporcjonalnie dużą wartość transakcji w odniesieniu do profilu działalności gospodarczej klienta czy też dotychczas zgromadzonych informacji o kliencie.

8. Fizyczny przewóz wartości majątkowych przez granicę

Opis sektora – zawarty jest w podrozdziale 7.2.2 - „Podatność rynku pozainansowego”, a także w rozdziale 5.3. „Najczęściej wykorzystywane metody prania pieniędzy”.

Scenariusze wystąpienia ryzyka obejmowały możliwość wykorzystania osób fizycznych do transportu środków pieniężnych, lub innych nośników wartości majątkowych (metali lokacyjnych, kamieni szlachetnych, kart płatniczych, czeków itp.).

Pranie pieniędzy

Tabela 38

Rodzaj wykorzystanych usług, produktów finansowych	Kurierzy wartości majątkowych (tzw. z ang. *cash couriers*)
Ogólny opis ryzyka	Wykorzystanie osób fizycznych do przewozu pieniędzy pochodzących z nielegalnych źródeł poprzez granice państwowe
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Osoby fizyczne (czasami wynajmowane jedynie w celu jednorazowego przewozu wartości majątkowych) transportują te wartości przez granice w różny sposób: • przewożąc jednorazowo środki pieniężne poniżej progu wymagającego ich deklaracji, • deklarując przywóz/wywóz środków pieniężnych o wartości pow. progu i wskazując fikcyjny cel ich przeznaczenia, • transportując/przemycając środki pieniężne, ukryte w bagażu, w środku transportu, pod ubraniem. 2. Oprócz gotówki przewozowi mogą podlegać takie wartości majątkowe, jak kamienie i metale szlachetne, dzieła sztuki, karty płatnicze, karty prepaid, czeki itd. 3. Przewóz znacznych sum pieniędzy przez granice z jednoczesnym zgłoszeniem do deklaracji przywozu/wywozu kwoty pieniędzy trochę powyżej progu wymaganego przy deklaracjach dewizowych, która nie wzbudzi podejrzeń. Sprawcy liczą, że funkcjonariusze służby celnej lub straży granicznej poprzestaną na dopełnieniu obowiązku z przyjęciem deklaracji i nie będą szukać innych środków pieniężnych, przewożonych przez sprawców w o wiele większej kwocie.
Poziom podatności	4
Uzasadnienie dla poziomu podatności	Dostęp do usług przewozu wartości majątkowych jest bardzo łatwy - każdy może być takim kurierem. Podczas kontroli na granicach zewnętrznych UE nie jest możliwe ukrycie danych identyfikacyjnych kuriera. Jakkolwiek sam przewóz wartości majątkowych, a tym samym dane identyfikacyjne kuriera mogą nie zostać rozpoznane przez organy administracji publicznej na granicy. W dobie konfliktu zbrojnego na Ukrainie i przyjmowania przez Polskę uchodźców ze stref konfliktu przekraczanie granicy na odcinku ukraińskim jest niezwykle ułatwione. W tym potencjalnie możliwe jest ukrycie danych identyfikacyjnych kuriera. Podmioty oferujące te usługi nie są IO. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji (informacje przekazywane przez KAS i SG, system CIS (System Informacji Celnej). Istnieje duże prawdopodobieństwo, że przypadek prania pieniędzy w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	4

Uzasadnienie dla poziomu zagrożenia	Wykorzystanie osób fizycznych do przewozu pieniędzy poprzez granice państwowe jest jedną z najczęściej spotykanych metod prania pieniędzy. Przewóz pieniędzy albo innych wartości majątkowych poprzez granice państwowe jest sposobem szeroko dostępnym, a jego zastosowanie relatywnie niewiele kosztuje i jest postrzegane przez sprawców jako atrakcyjne i stosunkowo bezpieczne. Zwłaszcza gdy przewożone sumy są poniżej progu obowiązkowej deklaracji przywozu. Wykorzystanie osób fizycznych do przewozu pieniędzy poprzez granice państwowe nie wymaga posiadania specjalistycznej wiedzy o systemie bankowym ani specjalistycznych umiejętności, a zapewnia anonimowość dla grupy/organizacji, która organizuje proceder. GIIF otrzymywał informacje o możliwości wykorzystania tej metody do prania pieniędzy. Polskie służby odnotowały przypadki wykorzystania tej metody do transferu środków pieniężnych pomiędzy uczestnikami procederu prania pieniędzy. WNIOSEK: Wykorzystanie osób fizycznych do przewozu pieniędzy pochodzących z nielegalnych źródeł poprzez granice państwowe stwarza bardzo wysokie zagrożenie prania pieniędzy.

Tabela 39

Rodzaj wykorzystanych usług, produktów finansowych	Paczki kurierskie, pocztowe, przewozy cargo
Ogólny opis ryzyka	Wykorzystanie usług kurierskich i pocztowych do przekazywania pieniędzy pochodzących z nielegalnych źródeł
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	Przestępca przekazuje środki pochodzące z nielegalnych źródeł w paczkach nadawanych na poczcie do osób fizycznych, przebywających w innych krajach. Odbiorcy środków następnie wprowadzają te pieniądze do systemu finansowego (np. lokując je na rachunkach bankowych) celem ich zainwestowania lub wykorzystania do zakupu dóbr, które są następnie udostępniane przestępcom.
Poziom podatności	3
Uzasadnienie dla poziomu podatności	Dostęp do usług kurierskich i pocztowych oraz przewozów cargo jest relatywnie łatwy. Istnieją możliwości ukrycia danych identyfikacyjnych zlecających i odbierających przesyłki. Paczki kurierskie, pocztowe oraz towary w ramach usług cargo są przekazywane pomiędzy osobami i podmiotami z różnych krajów. W dobie konfliktu zbrojnego na Ukrainie istnieje potencjalna możliwość wykorzystania danych identyfikacyjnych osób z tych miejsc konfliktu, które zostały zajęte przez wroga lub zniszczone w działaniach wojennych. Tylko część podmiotów oferujących te usługi jest IO. Nie są nimi przewoźnicy oraz firmy spedycyjne. Organy administracji publicznej posiadają ograniczoną wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji (jedynie w ograniczonym zakresie. Istnieje duże prawdopodobieństwo, że przypadek prania pieniędzy w zakresie analizowanych scenariuszy nie zostanie wykryty. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne tylko częściowo odpowiadają zakresowi analizowanego ryzyka.
Poziom zagrożenia	3

Uzasadnienie dla poziomu zagrożenia	Wykorzystanie usług kurierskich i pocztowych do przekazywania pieniędzy pochodzących z nielegalnych źródeł jest sposobem prania pieniędzy stosunkowo łatwym, szeroko dostępnym, a jego zastosowanie niewiele kosztuje. Jest postrzegany przez sprawców raczej jako atrakcyjny. Wykorzystanie usług kurierskich bądź pocztowych z reguły nie wzbudza podejrzeń. Wysoki wolumen obrotów - jeśli chodzi o przesyłki międzynarodowe - pozwala ukryć wykorzystanie tych usług do prania pieniędzy. W celu ukrycia beneficjenta rzeczywistego częstokroć wykorzystywane są „słupy". W dobie konfliktu zbrojnego na Ukrainie jest to o tyle łatwe, że wobec pewnej części uchodźców występują problemy z identyfikacją i weryfikacją tych osób, Osoby te przekraczając granicę albo w ogóle nie miały żadnych dokumentów, albo miały dokumenty w rodzaju paszportu wewnętrznego pisanego cyrylicą. Zastosowanie tego *modus operandi* wymaga jednak zaplanowania, wiedzy o systemie przesyłek i umiejętności logistycznych. GIIF otrzymywał informacje o wykorzystaniu tej metody do prania pieniędzy, zwłaszcza w powiązaniu z innymi metodami. WNIOSEK: Wykorzystanie usług kurierskich i pocztowych do przekazywania pieniędzy pochodzących z nielegalnych źródeł stwarza wysokie zagrożenie prania pieniędzy.

Finansowanie terroryzmu

Tabela 40

Rodzaj wykorzystanych usług, produktów finansowych	Kurierzy wartości majątkowych (tzw. z ang. cash couriers)
Ogólny opis ryzyka	Wykorzystanie osób fizycznych do przewozu pieniędzy poprzez granice państwowe
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Osoby fizyczne (czasami wynajmowane jedynie w celu jednorazowego przewozu wartości majątkowych) transportują te wartości przez granice w różny sposób: – przewożąc jednorazowo środki pieniężne poniżej progu wymagającego ich deklaracji, – deklarując przywóz/wywóz środki pieniężne o wartości powyżej ww. progu i wskazując fikcyjny cel ich przeznaczenia, – transportując/przemycając środki pieniężne o wartości znacznie powyżej progu wymagającego ich deklarację, ukryte w bagażu, w środku transportu, pod ubraniem. 2. Oprócz gotówki przewozowi mogą podlegać takie wartości majątkowe, jak kamienie i metale szlachetne, dzieła sztuki, karty płatnicze, karty prepaid, czeki itd. 3. Przewóz znacznych sum pieniędzy przez granice z jednoczesnym zgłoszeniem do deklaracji przywozu/wywozu kwoty pieniędzy trochę powyżej progu wymaganego przy deklaracjach dewizowych, która nie wzbudzi podejrzeń. Sprawcy liczą, że funkcjonariusze służby celnej lub straży granicznej poprzestaną na dopełnieniu obowiązku z przyjęciem deklaracji i nie będą szukać innych środków pieniężnych, przewożonych przez sprawców w o wiele większej kwocie.
Poziom podatności	4

Uzasadnienie dla poziomu podatności	Dostęp do usług przewozu wartości majątkowych jest bardzo łatwy - każdy może być takim kurierem. Podczas kontroli na granicach zewnętrznych UE nie jest możliwe ukrycie danych identyfikacyjnych kuriera. Jakkolwiek sam przewóz wartości majątkowych, a tym samym dane identyfikacyjne kuriera mogą nie zostać rozpoznane przez organy administracji publicznej na granicy. W dobie konfliktu zbrojnego na Ukrainie i przyjmowania przez Polskę uchodźców ze stref konfliktu przekraczanie granicy na odcinku ukraińskim jest niezwykle ułatwione. W tym potencjalnie możliwe jest ukrycie danych identyfikacyjnych kuriera. Podmioty oferujące te usługi nie są IO. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji (informacje przekazywane przez KAS i SG, system CIS. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	4
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie osób fizycznych do przewozu pieniędzy poprzez granice państwowe jest jedną z najczęściej spotykanych metod finansowania działalności terrorystycznej. Przewóz pieniędzy albo innych wartości majątkowych poprzez granice państwowe jest sposobem szeroko dostępnym, a jego zastosowanie relatywnie niewiele kosztuje i jest postrzegane przez sprawców jako atrakcyjne i stosunkowo bezpieczne. Zwłaszcza gdy przewożone sumy są poniżej progu obowiązkowej deklaracji przywozu. Wykorzystanie osób fizycznych do przewozu pieniędzy poprzez granice państwowe nie wymaga posiadania specjalistycznej wiedzy o systemie bankowym ani specjalistycznych umiejętności, a zapewnia anonimowość dla grupy/organizacji, która organizuje proceder. GIIF otrzymywał nieliczne informacje o możliwości wykorzystania tej metody do finansowania działalności terrorystycznej. Polskie służby odnotowały przypadki wykorzystania tej metody do transferu środków przeznaczonych na działalność terrorystyczną. WNIOSEK: Wykorzystanie osób fizycznych do przewozu pieniędzy poprzez granice państwowe stwarza bardzo wysokie zagrożenie finansowaniem terroryzmu.

Tabela 41

Rodzaj wykorzystanych usług, produktów finansowych	Paczki kurierskie, pocztowe, przewozy cargo
Ogólny opis ryzyka	Wykorzystanie usług kurierskich i pocztowych
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	Zwolennik organizacji terrorystycznej przekazuje zgromadzone na jej cele środki pieniężne w paczkach nadawanych na poczcie do osoby fizycznej, zamieszkałej w jednym z krajów sąsiadujących z rejonem działalności organizacji terrorystycznych, która następnie przekazuje otrzymane środki członkom tej organizacji.
Poziom podatności	4
Uzasadnienie dla poziomu podatności	Dostęp do usług kurierskich i pocztowych oraz przewozów cargo jest relatywnie łatwy. Istnieją możliwości ukrycia danych identyfikacyjnych zlecających i odbierających przesyłki. Paczki kurierskie, pocztowe oraz towary w ramach usług cargo są przekazywane pomiędzy osobami i podmiotami z różnych krajów. W dobie konfliktu zbrojnego na Ukrainie istnieje potencjalna możliwość wykorzystania danych identyfikacyjnych osób z tych miejsc konfliktu, które zostały zajęte przez wroga lub zniszczone w działaniach wojennych. Tylko część podmiotów oferujących te usługi jest IO. Nie są nimi przewoźnicy oraz firmy spedycyjne. Organy administracji publicznej posiadają ograniczoną wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji

	(jedynie w ograniczonym zakresie). Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy nie zostanie wykryty. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne tylko częściowo odpowiadają zakresowi analizowanego ryzyka.
Poziom zagrożenia	3
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie usług kurierskich i pocztowych do przekazywania organizacjom terrorystycznym pieniędzy na cele działalności terrorystycznej jest jedną ze zidentyfikowanych metod finansowania terroryzmu. Jest to sposób stosunkowo łatwy, szeroko dostępny, jego zastosowanie niewiele kosztuje i jest postrzegany przez sprawców raczej jako atrakcyjny. Wykorzystanie usług kurierskich bądź pocztowych z reguły nie wzbudza podejrzeń. Wysoki wolumen obrotów - jeśli chodzi o przesyłki międzynarodowe - pozwala ukryć wykorzystanie tych usług do przekazywania pieniędzy na cele działalności terrorystycznej. Zwłaszcza gdy nie są to jednorazowo sumy zbyt wysokie. W celu ukrycia beneficjenta rzeczywistego częstokroć wykorzystywane są „słupy". W dobie konfliktu zbrojnego na Ukrainie jest to o tyle łatwe, że wobec pewnej części uchodźców występują problemy z identyfikacją i weryfikacją tych osób, Osoby te przekraczając granicę albo w ogóle nie miały żadnych dokumentów, albo miały dokumenty w rodzaju paszportu wewnętrznego pisanego cyrylicą. Zastosowanie tego *modus operandi* wymaga jednak zaplanowania, wiedzy o systemie przesyłek i umiejętności logistycznych. GIIF otrzymywał bardzo nieliczne informacje o możliwości wykorzystania tej metody do finansowania działalności terrorystycznej. WNIOSEK: Wykorzystanie usług kurierskich i pocztowych do przekazywania organizacjom terrorystycznym pieniędzy na cele działalności terrorystycznej stwarza wysokie zagrożenie finansowaniem terroryzmu.

Transport takich środków może dotyczyć wywozu wartości pochodzących z działalności nielegalnej, w celu ich ukrycia, lub też ich przywóz na teren kraju w celu ich lokowania albo finansowania działalności nielegalnej. W zakresie finansowania terroryzmu rozważyć można możliwość przywozu na teren kraju środków mogących posłużyć do sfinansowania ataków, lub wywóz takich środków zebranych od sympatyków na terenie kraju dla sfinansowania działalności terrorystycznej na terenie innych państw. Możliwe ryzyko obejmuje również możliwość wykorzystania terytorium kraju do tranzytu takich wartości.

W aneksie nr 1 do dokumentu SNRA z 2022 r. wskazano, że szczególnie istotny jest nadzór nad środkami pieniężnymi wyprowadzanymi poza terytorium UE, które mogą służyć do finansowania działań terrorystycznych i zbrojnych w krajach trzecich. W szczególności dotyczy to bojowników udających się do strefy walk, które przy okazji zabierają ze sobą środki na własne utrzymanie i sfinansowanie działalności organizacji. Kwoty takie często nie przekraczają określonych prawem limitów przewozu. Zaznaczono również, że najwygodniejszym sposobem z punktu widzenia sprawców jest wykorzystanie poczty lub usług kurierskich, co obniża prawdopodobieństwo zatrzymania kuriera.

W zakresie prania pieniędzy transport gotówki jest uznanym sposobem logistyki nielegalnie zdobytego majątku z uwagi na gotówkowy charakter rozliczeń za znaczną cześć czynności związanych z działalnością nielegalną. Szczególnie istotne jest tu wykorzystanie banknotów o dużych nominałach. Przestępcy wykorzystujący obrót gotówkowy muszą dokonywać relokacji zgormadzonych środków do lokalizacji gdzie są one bezpieczne, lub mogą być (ze względu na istniejący system kontroli lub uwarunkowania rynku) łatwiej wprowadzone do legalnego obrotu. Użycie kurierów jest o tyle istotne, że są oni wykorzystywani nawet

w przestępstwach nie generujących znacznego obrotu gotówkowego, np. oszustwach bankomatowych lub oszustwach BLIK, gdzie podstawione osoby odbierają gotówkę zdobytą w trakcie cyberprzestępstwa. Obrót gotówkowy z tytułu nielegalnej działalności szacuje się na nawet bilion dolarów rocznie.

Zasady przewozu przez granicę państwową Polski wartości dewizowych lub krajowych środków płatniczych określają przepisy *ustawy z dnia 27 lipca 2002 r. – Prawo dewizowe*. Zgłoszeniu podlega przewóz środków w kwocie powyżej 10 000 EUR, niezależnie czy dotyczy wwozu czy też wywozu. Za środki pieniężne uznane zostały zarówno banknoty i monety obiegowe, zbywalne papiery na okaziciela, w tym czeki, czeki podróżne weksle itp., towary używane jako wysoce płynny środek przechowywania wartości, karty przedpłacone, banknoty i monety nie będące oficjalnymi środkami płatniczymi na terenie kraju, ale mogą być wymienione na walutę obiegową oraz złoto i platyna dewizowa. Powyższe zasady nie dotyczą środków pieniężnych przewożonych przez granice wewnętrzne Strefy Schengen[60].

Podatność

W Aneksie nr 1 do Supra-National Risk Assessment działalność kurierów gotówkowych została wskazana jako jedno z głównych zagrożeń sektorowych. O skali problemu świadczy fakt, iż w trakcie przeprowadzonej w okresie od września do listopada 2022 r. wspólnej akcji organów ścigania z 25 krajów świat, wspieranych przez Europol, Interpol, Eurojust oraz Europejską Federację Bankową zatrzymanych zostało 2 469 kurierów (org.: money mule) oraz 222 osoby rekrutujące. Akcja skutkowała zidentyfikowaniem 4 089 nielegalnych transakcji oraz przechwyceniem 17,5 mln Euro[61].

W trakcie trwania pandemii COVID-19 oraz związanym z nią ograniczeniu przemieszczania zjawisko zostało znacznie ograniczone. Przywrócenie kontroli na wewnętrznych granicach Schengen oraz długie okresy lockdownów utrudniły, lub wręcz uniemożliwiły dowolny i nieograniczony transport fizycznych wartości pieniężnych. Ustąpienie kryzysu oraz zniesienie obostrzeń umożliwiły ponowne wykorzystanie takiego sposobu przekazywania środków. Ponadto, wywołany przez wybuch wojny na Ukrainie napływ uchodźców spowodowała podwyższenie ryzyka napływu nielegalnych środków. Część osób przekraczających granicę nie przeszła pełnej kontroli celnej, pomimo iż niejednokrotnie wwozili ze sobą znaczną ilość majątku osobistego. W połączeniu z utrudnionym procesem weryfikacji danych osobowych zwiększyło to możliwość napływu nierejestrowanych środków pieniężnych oraz innych wartości majątkowych, tym bardziej że Polska przyjęła największą liczbę uchodźców.

Odpowiednie organy władzy państwowej niewątpliwie posiadają odpowiednią wiedzę oraz świadomość istnienia zagrożenia. GIIF otrzymuje informacje o stwierdzonych próbach przewozu środków pieniężnych przez granicę. W przypadku wykrycia przewozu istnieje wysokie prawdopodobieństwo skazania bezpośredniego sprawcy. Ujemną cechą procederu jest jednak fakt, że ukaranie faktycznego organizatora lub zleceniodawcy przewozu jest mniej prawdopodobne niż ukaranie samego kuriera.

Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie.

[60] https://granica.gov.pl/j/index.php/535; dostęp: 16.12.2022 r.,
[61] 2 469 money mules arrested in worldwide crackdown against money laundering | Europol (europa.eu); dostęp 15.12.2022 r.

Istniejące przepisy prawne odpowiadają w dużej mierze zakresowi analizowanego ryzyka.

Zagrożenia w sektorze.

Poważnym zagrożeniem jest fakt, że fizyczny przewóz gotówki jest rynkiem usług kompletnie nieuregulowanym, gdzie większość zaangażowanych to osoby fizyczne nie działające jako podmiot gospodarki. Wynika to z samego założenia istnienia takiej działalności, która ma służyć do przewożenia środków zdobytych nielegalnie. Transport dokonywany jest w sposób ukryty, a ewentualne wykrycie procederu zależy wyłącznie od sprawności służb policyjnych i granicznych. Brak jest zatem innych narzędzi do obserwacji i kontroli zjawiska niż działania operacyjno-kontrolne.

Z punktu widzenia AML/CTF przewóz gotówki lub środków będących nośnikiem wartości jest jednym z najpoważniejszych źródeł ryzyka, ponieważ jest zasadniczą częścią obrotu gotówkowego oraz procesem bez którego nie byłby in możliwy. Można przyjąć, że każdy rodzaj działalności nielegalnej, w której używana jest gotówka, spowoduje wcześniej czy później konieczność jej przewozu.

W zakresie finansowania terroryzmu zauważyć należy, że w Polsce były przykłady wspierania zagranicznych grup bojowników. Na terenie kraju istnieją zorganizowane grupy stronników różnych organizacji zagranicznych, często odwołujących się do stosowania przemocy. Istnieje faktyczne ryzyko wykorzystania tego zaplecza do finansowania działalności terrorystycznej poza terytorium kraju[62]. Niewątpliwie mogą zostać w tym celu wykorzystani kurierzy wywożący środki majątkowe poza granicę.

Możliwość przewozu w ramach Strefy Schengen nierejestrowanych wartości majątkowych stwarza również możliwość wykorzystania do celów prania pieniędzy istniejących lub nierozpoznanych jeszcze luk w polskim systemie finansowym.

Zagadnieniem technicznym jest logistyka związana z procesem gromadzenia i przekazywania środków, która zakładać musi z jednej strony zebranie pieniędzy lub wartości majątkowych z ich źródeł, a następnie skoordynowane przekazanie ich do osób bądź podmiotów odpowiedzialnych za proces legalizacji na terenie Unii Europejskiej lub wyprowadzenie do kraju trzeciego. Budowa odpowiedniej struktury do takiego celu jest utrudniona z uwagi szczególnie w przypadku rozległych i dochodowych rodzajów działalności nielegalnej np. handlu narkotykami lub prostytucji. Jednakże w większości przypadków transport nie dotyczy dużych ilości gotówki i jest potencjalnie łatwy do zorganizowania. Do zorganizowania transportu nie jest konieczna wiedza specjalistyczna.

Uśredniony poziom zagrożenia sektora fizycznego przewozu wartości majątkowych przez granicę – AML – 3,5 i FT – 3,5

Uśredniony poziom podatności sektora fizycznego przewozu wartości majątkowych przez granicę – AML – 3,5 i FT – 4,0

Oszacowany poziom prawdopodobieństwa dla sektora – ML – 3,50 i FT - 3,80

Poziom ryzyka jest ostatecznie określany przez kombinację zagrożenia i podatności. Macierz ryzyka określająca ten poziom ryzyka opiera się na wadze 40% (zagrożenie) + 60% (podatność) – przy założeniu, że komponent podatności ma większą zdolność określania poziomu ryzyka.

[62] Oskarżeni o wspieranie terroryzmu Czeczeni nie pomagali Państwu Islamskiemu - mówił przed białostockim sądem biegły ekspert (radio.bialystok.pl), dostęp: 19.12.2022 r.

Zakłada się, że poziom podatności może zwiększyć atrakcyjność, a tym samym zamiary przestępców/terrorystów, aby użyć danego modus operandi – wpływając w ten sposób ostatecznie na poziom zagrożenia. Poziom ryzyka sektora, z uwzględniem prawdopobieństwa i konsekwencji (współczynnik 2,5 dla PP i 1,5 dla FT), jest ustalany zgodnie z metodyką krajowej oceny ryzyka – aneks nr 1.

Ryzyko FT sektora fizycznego przewozu wartości majątkowych przez granicę – 2,88	
1 – 1,5	Niskie
1,6 – 2,5	Średnie
2,6 – 3,5	Wysokie
3,6 – 4	Bardzo wysokie
Ryzyko ML sektora fizycznego przewozu wartości majątkowych przez granicę – 3,10	
1 – 1,5	Niskie
1,6 – 2,5	Średnie
2,6 – 3,5	Wysokie
3,6 – 4	Bardzo wysokie

WNIOSEK 1: Poziom ryzyka wykorzystania fizycznego przewozu wartości majątkowych przez granicę do finansowania terroryzmu w Polsce znajduje się na poziomie wysokim.

WNIOSEK 2: Poziom ryzyka wykorzystania fizycznego przewozu wartości majątkowych przez granicę do prania pieniędzy w Polsce znajduje się na poziomie wysokim.

Mitygacja zidentyfikowanych ryzyk:

W celu ograniczenia prawdopodobieństwa wykorzystania fizycznego przewozu wartości majątkowych przez granicę do prania pieniędzy lub finansowania terroryzmu, zasadne jest podjęcie odpowiednich działań. Stosowanie zaproponowanych działań mitygujących powinno następować z uwzględnieniem rozpoznanego przez danę instytucję obowiązaną ryzyka.

Instytucje obowiązane powinny zwracać szczególną uwagę na transakcje wymiany walut związane z jurysdykcjami charakteryzujących się wyższym ryzykiem prania pieniędzy oraz finansowania terroryzmu. Instytucje obowiązane powinny położyć szczególny nacisk na ustalenie danych dotyczących źródła pochodzenia transferowanych wartości majątkowych, jak również dokumentów wskazujących na uzasadnienie przeprowadzenia danej transakcji. W przypadku wymiany lub wpłaty większej ilości gotówki przez nierezydentów UE, instytucje obowiązane powinny rozważyć zwrócenie się do klienta o przedstawienie informacji na temat

źródła pochodzenia wartości majątkowych, np. poprzez zwrócenie się do klientów z państw spoza UE o przedstawienie kopii lub potwierdzenia złożenia deklaracji dewizowych.

Instytucje obowiązane przyjmujące płatności albo wpłaty gotówkowe w walutach obcych, powinny weryfikować źródło pochodzenia wartości majątkowych, w tym zasadnym może się okazać pozyskanie od klienta informacji potwierdzających dokonanie wymiany waluty, czy też potwierdzających złożenie deklaracji dewizowych.

Instytucje obowiązane powinny przykładać szczególną wagę do czynników geograficznych mogących wskazywać na wyższe ryzyko prania pieniędzy czy też finansowania terroryzmu, takich jak niestabilna sytuacja polityczna czy konflikt zbrojny, czego najdobitniejszym przykładem w ostatnich latach jest wojna prowadzona przez Rosję przeciwko Ukrainie. Instytucje obowiązane powinny zwracać szczególną uwagę na wysokokwotowe transakcje gotówkowe przeprowadzane z rezydentami jurysdykcji objętych konfliktami, jak również na transakcje wskazujące, na wykorzystanie pośrednika do wymiany waluty.

Na poziomie systemowym zasadne jest podjęcie działań zmierzających do usprawnienia systemu ochrony granicy państwa przed niezgodnym z przepisami przepływem gotówki. W szczególności zasadnym byłoby wprowadzenie realnej kary za niezgłoszenie przewozu gotówki przez granicę, należy również rozważyć usprawnienie mechanizmów zatrzymania przewożonych niezgodnie z przepisami wartości majątkowych, wraz z ewentualną konfiskatą środków.

9. Obszar – gry hazardowe

Opis sektora – zawarty jest w podrozdziale 7.2.1 - „Podatność rynku finansowego”.

Scenariusze wystąpienia ryzyka (tj. możliwe przykłady wystąpienia ryzyka) dotyczyły wykorzystania do prania pieniędzy internetowych gier hazardowych; wykorzystania zakładów wzajemnych do legitymizowania środków pochodzących z nielegalnych źródeł; wykorzystania gier oferowanych w kasynie do zaciemnienia pochodzenia posiadanych pieniędzy; kupowania zwycięskich kuponów za środki pochodzące z nielegalnych źródeł, a do finansowania terroryzmu schematu internetowych gier hazardowych. Opis scenariuszy znajduje się poniżej.

Pranie pieniędzy

Tabela 42

Rodzaj wykorzystanych usług, produktów finansowych	Internetowe gry hazardowe
Ogólny opis ryzyka	Środki pochodzące z nielegalnych źródeł są prane przy pomocy internetowych gier hazardowych
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	Wykorzystanie internetowych platform hazardowych do prania pieniędzy pochodzących z czynów zabronionych, takich jak oszustwa. W toku analizy zawiadomień od instytucji obowiązanych oraz informacji od zagranicznych partnerów GIIF zidentyfikował następujący proceder: 1. Przestępca otwiera rachunek na platformie hazardowej na podstawie fałszywych albo skradzionych danych identyfikacyjnych lub przejmuje kontrolę nad istniejącym rachunkiem prowadzonym na rzecz innego podmiotu. 2. Przestępcy "hakowali" karty kredytowe, a następnie środki ukradzione z rachunków tych kart prali przy pomocy gier hazardowych dostępnych on-line w celu przeznaczenia ich potem na rzecz organizatorów tego procederu. 3. Wykorzystanie internetowych platform hazardowych do prania pieniędzy pochodzących z czynów zabronionych, takich jak oszustwa. 4. Przestępca wpłaca środki wykorzystując m.in. kryptowaluty, pieniądze zgromadzone na rachunku bankowym, uznania z kart płatniczych (często na podstawie skradzionych danych), anonimowe karty przedpłacone lub transfery pieniężne na odpowiedni rachunek powiązany z platformą hazardową. 5. Środki są wykorzystane do obstawiania gier o niskim poziomie ryzyka lub alternatywnie użyte w grach hazardowych w procesie tzw. chip dumpingu - jeden lub wielu graczy celowo przegrywa z innymi podstawionymi graczami, umyślnie przenosząc w ten sposób środki na rachunki innych uczestników. 6. Środki pod postacią "wygranej" są wyprowadzane z rachunku powiązanego z platformą hazardową za pośrednictwem transferów pieniężnych, przelewów na rachunki bankowe lub są wymieniane na waluty wirtualne.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Dostęp do internetowych gier hazardowych jest stosunkowo łatwy, bo wciąż pojawiają się w sieci nowe domeny z grami hazardowymi. Licencja wydana przez inne państwo jednak nie legalizuje działalności hazardowej w Polsce. W przypadku zagranicznych kasyn online łatwe jest ukrycie danych identyfikacyjnych gracza. Istnieje możliwość realizacji transakcji o charakterze międzynarodowym, zwłaszcza w przypadku dokonywania transakcji finansowych, w przypadku gdy rachunki podmiotu prowadzącego internetowe gry hazardowe są ulokowane za granicą. Tym niemniej Krajowa Administracja Skarbowa (KAS) we współpracy z Komisją Nadzoru Finansowego (KNF) opracował zasady dotyczące ograniczenia wykorzystywania instrumentów bądź usług płatniczych oferowanych przez dostawców usług płatniczych w Polsce do dokonywania transakcji związanych z nielegalną grą hazardową. Hostingodawcy natomiast usuwają/blokują dostęp do zabronionych treści

	związanych z nielegalnymi grami online. Urządzanie gier hazardowych przez sieć Internet, z wyjątkiem zakładów wzajemnych i loterii promocyjnych, jest objęte monopolem państwa. Według polskiego prawa, na terenie Polski istnieje tylko jedno legalne kasyno online. Jest to powstałe w 2018 r. Total Casino, należące do państwowej firmy, jaką jest Totalizator Sportowy. Płatności w nim można dokonywać poprzez przelewy online, Visa, Dotpay czy BLIK. Wszystkie podmioty oferujące legalnie gry hazardowe są IO. Posiadają pewną świadomość swoich obowiązków z zakresu PPP/PFT, choć wciąż ujawniane są braki w ich wypełnianiu. Analiza otrzymywanych przez GIIF informacji wskazuje, że wartość środków która może podlegać praniu przez dany podmiot za pośrednictwem internetowych gier hazardowych jest jednostkowo niewielka przez wzgląd na ograniczenia nakładane przez podmioty prowadzące taką działalność oraz mechanizmy pozwalające na identyfikację powiązanych kont potencjalnie wykorzystywanych do czynów zabronionych. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Otrzymuje również informacje od zagranicznych partnerów informacje spontaniczne dotyczące transakcji podejrzanych zgłaszanych przez zagraniczne kasyna online mających związek z Polską i polskimi obywatelami. Istnieje duże prawdopodobieństwo, że przypadek prania pieniędzy w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	2
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie internetowych gier hazardowych może być jedną z metod prania środków pochodzących z nielegalnych źródeł. Zgodnie jednak z polskimi przepisami urządzanie gier hazardowych przez Internet, z wyjątkiem zakładów wzajemnych i loterii promocyjnych jest objęte monopolem państwa. Przepisy prawne zakazują zarówno urządzania gier hazardowych przez sieć przez podmioty nieuprawnione, jak i uczestniczenie w takich grach. Działalność kontrolna KAS, utworzenie Rejestru domen służących do oferowania gier hazardowych niezgodnie z ustawą oraz blokowanie dostępu do zabronionych domen internetowych może negatywnie wpływać na możliwość użycia nielegalnie pozyskanych środków pieniężnych. GIIF otrzymywał informacje o możliwości wykorzystywania w Polsce *modus operandi* polegającego na wykorzystaniu internetowych gier hazardowych dla prania pieniędzy. Sposób ten, z uwagi na uwarunkowania prawne, zdaje się być postrzegany przez sprawców jako mało atrakcyjny i stosunkowo ryzykowny, by legitymizować środki finansowe pochodzące z czynów zabronionych. Ponadto potrzebne jest planowanie, wiedza i umiejętności do zastosowania tego *modus operandi*. WNIOSEK: Wykorzystanie internetowych gier hazardowych do prania środków pochodzących z nielegalnych źródeł stwarza średnie zagrożenie dla prania pieniędzy.

Tabela 43

Rodzaj wykorzystanych usług, produktów finansowych	Zakłady wzajemne
Ogólny opis ryzyka	Wykorzystanie zakładów wzajemnych do legitymizowania środków pochodzących z nielegalnych źródeł
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	Przestępca przewidując wyniki wydarzeń sportowych dokonuje zakładów bukmacherskich przy wykorzystaniu pieniędzy pochodzących z nielegalnych źródeł (często – w celu zwiększenia szans na wygraną – dywersyfikując realizowane zakłady, przeznaczając pieniądze na różne zakłady dot. różnych wydarzeń sportowych). Wygrane są jego legalnym zyskiem, potwierdzone

	rachunkiem otrzymanym od bukmachera.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Dostęp do zakładów wzajemnych jest stosunkowo łatwy. Na rynku funkcjonują dwa podstawowe rodzaje firm bukmacherskich: tzw. bukmacherzy naziemni, czyli firmy posiadające punkty stacjonarne (przysłowiowe okienka), w których płaci się gotówką lub kartą i w zamian otrzymuje określony kupon, oraz tzw. bukmacherzy internetowi, którzy działają w sieci. W Internecie stosunkowo łatwe jest ukrycie danych identyfikacyjnych nielegalnego gracza, zwłaszcza w przypadku korzystania z internetowych platform płatniczych zagranicznych operatorów. Legalni bukmacherzy stosują odpowiednie środki bezpieczeństwa finansowego. Istnieje możliwość realizacji transakcji o charakterze międzynarodowym, szczególnie w przypadku dokonywania transakcji finansowych, w przypadku gdy rachunki podmiotu prowadzącego internetowe gry hazardowe (operatora zagranicznego) są ulokowane za granicą. Z szacunków Ministerstwa Finansów wynika, iż „szara strefa" w sektorze internetowych zakładów wzajemnych w 2021 r. wyniosła 8,2% (spadek o 1,2% w stosunku do roku 2022). Udział szarej strefy w Polsce w zakładach wzajemnych w roku 2021 kształtuje się poniżej średniej państw UE.[63] Wszystkie podmioty oferujące legalnie gry hazardowe są IO. Posiadają pewną świadomość swoich obowiązków z zakresu PPP/PFT, choć wciąż ujawniane są braki w ich wypełnianiu. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek prania pieniędzy w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	3
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie zakładów wzajemnych do legitymizowania środków pochodzących z nielegalnych źródeł jest jedną z często używanych metod prania pieniędzy. Fałszywe zaświadczenia potwierdzające wygrane w zakładach są dokumentami, które mogą przyczyniać się do legalizowania zysków z przestępczej działalności. Jest to sposób stosunkowo łatwy, szeroko dostępny, wymagający jedynie umiarkowanej wiedzy specjalistycznej. Jego zastosowanie tak naprawdę niewiele kosztuje i jest postrzegany przez sprawców raczej jako atrakcyjny. Przestępcy wybierając ten *modus operandi* często nielegalnie wpływają na wyniki obstawianych przez nich zdarzeń, np. wydarzeń sportowych (bądź innych obstawianych zdarzeń). Zastosowanie tego *modus operandi* wymaga jednak zaplanowania, wiedzy o systemie ustalania kursów (lub wpływania na prawidłowość oszacowania przez bukmachera zaistnienia danego zdarzenia). GIIF otrzymywał informacje o wykorzystaniu tej metody do prania pieniędzy. WNIOSEK: Wykorzystanie zakładów wzajemnych do legitymizowania środków pochodzących z nielegalnych źródeł stwarza wysokie zagrożenie prania pieniędzy.

[63] https://www.gov.pl/web/finanse/sytuacja-na-rynku-gier-hazardowych-online

Tabela 44

Rodzaj wykorzystanych usług, produktów finansowych	Kasyno
Ogólny opis ryzyka	Wykorzystanie gier oferowanych w kasynie do zaciemnienia pochodzenia posiadanych pieniędzy
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Przestępca kupuje żetony w kasynie np. za gotówkę. Po użyciu niewielkiej części z nich wymienia z powrotem posiadane żetony na pieniądze. 2. Przy pomocy gry w pokera jeden z przestępców umyślnie przegrywa żetony zakupione za środki pochodzące z nielegalnych źródeł na rzecz osoby z nim powiązanej, która następnie wymienia je na gotówkę.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Dostęp do gier hazardowych (zwłaszcza internetowych) jest stosunkowo łatwy. W legalnych ośrodkach gier prowadzi się jednak rejestrację gości. Rejestracja jest warunkiem wstępu gości do ośrodka gier. Łatwe jest ukrycie prawdziwych danych identyfikacyjnych gracza przez Internet, ale płatności internetowe muszą pochodzić z rachunku osoby zarejestrowanej i środki mogą wrócić także na rachunek osoby zarejestrowanej. W jedynym legalnym polskim kasynie *online* gra w pokera jest możliwa tylko z krupierem. W kasynach zagranicznych można grać z innymi osobami, jednak branie udziału w internetowych grach hazardowych, które nie posiadają na terenie Polski odpowiedniego zezwolenia jest nielegalne i stanowi wykroczenie lub przestępstwo skarbowe. W przypadku udziału gracza w grze w nielegalnym kasynie istnieje możliwość realizacji transakcji o charakterze międzynarodowym, zwłaszcza gdy rachunki podmiotu prowadzącego internetowe gry hazardowe są ulokowane za granicą. Wszystkie podmioty oferujące legalnie gry hazardowe są IO. Posiadają pewną świadomość swoich obowiązków z zakresu PPP/PFT, choć wciąż ujawniane są braki w ich wypełnianiu. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek prania pieniędzy w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	4
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie gier oferowanych w kasynie do zaciemnienia pochodzenia posiadanych pieniędzy jest jedną z najlepiej opisanych metod prania pieniędzy. Jedyne legalnie działające kasyno online w Polsce jest prowadzone przez Totalizator Sportowy Sp. z o. o. Wykorzystanie gier oferowanych w kasynie jest to sposób szeroko dostępny, jego zastosowanie niewiele kosztuje i jest postrzegany przez sprawców jako bardzo atrakcyjny. Wykorzystanie gier oferowanych w kasynie do zaciemnienia pochodzenia posiadanych pieniędzy nie wymaga specjalistycznej wiedzy o samym kasynie ani specjalistycznych umiejętności dotyczących gier. Metoda wykorzystywana często przez zorganizowaną przestępczość, niekiedy wiąże się z korupcją pracowników kasyn. Środki bezpieczeństwa finansowego stosowane przez kasyna są omijane w tym *modus operandi* poprzez korupcję pracowników kasyn bądź fałszerstwo dokumentów. Wydane przez kasyna zaświadczenia o wygranych są ważnym dokumentem do udowodnienia legalności pochodzenia posiadanych przez przestępców środków finansowych. WNIOSEK: Wykorzystanie gier oferowanych w kasynie do zaciemnienia pochodzenia posiadanych pieniędzy stwarza bardzo wysokie zagrożenie prania pieniędzy.

Tabela 45

Rodzaj wykorzystanych usług, produktów finansowych	Gry losowe
Ogólny opis ryzyka	Kupowanie zwycięskich kuponów za środki pochodzące z nielegalnych źródeł
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	Przestępca, będąc w zmowie z osobą zaangażowaną w prowadzenie gier losowych, identyfikuje zwycięzców tych gier. Następnie odkupuje od nich zwycięskie kupony.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Dostęp do gier losowych jest stosunkowo łatwy. Łatwe jest ukrycie danych identyfikacyjnych gracza, zwłaszcza w przypadku realizacji płatności za los gotówką. Wszystkie podmioty oferujące w Polsce legalnie gry hazardowe są IO. Posiadają pewną świadomość swoich obowiązków z zakresu PPP/PFT, choć wciąż ujawniane są braki w ich wypełnianiu. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek prania pieniędzy w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	2
Uzasadnienie dla poziomu zagrożenia	Kupowanie zwycięskich kuponów za środki pochodzące z nielegalnych źródeł może być jedną z metod prania pieniędzy. GIIF otrzymywał nieliczne informacje o wykorzystywaniu takiego *modus operandi*, ale ten sposób jest postrzegany jako mało atrakcyjny i stosunkowo niebezpieczny. Podmiot realizujący wypłaty z gier losowych bądź zakładów wzajemnych nie udostępnia listy podmiotów wygrywających, trzeba do wygrywających dotrzeć. Nie jest to też sposób tani, bo obowiązuje dziesięcioprocentowy podatek od wygranych, co podraża koszty zastosowania. Potrzebne jest planowanie, wiedza i umiejętności do zastosowania tego *modus operandi*. WNIOSEK: Kupowanie zwycięskich kuponów za środki pochodzące z nielegalnych źródeł stwarza średnie zagrożenie dla prania pieniędzy.

Finansowanie terroryzmu

Tabela 46

Rodzaj wykorzystanych usług, produktów finansowych	Internetowe gry hazardowe
Ogólny opis ryzyka	Środki pozyskane nielegalnie na cele promowania terroryzmu były prane przy pomocy internetowych gier hazardowych

Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Przestępcy "hakowali" karty kredytowe, a następnie środki ukradzione z rachunków tych kart prali przy pomocy gier hazardowych dostępnych on-line w celu przeznaczenia ich potem na płatności za strony internetowe, na których promowali walkę i "męczeństwo" terrorystów, a które były też wykorzystywane do kontaktów pomiędzy terrorystami oraz przekazywania informacji o sposobie produkcji bomb. 2. Wykorzystanie internetowych platform hazardowych do prania pieniędzy pochodzących z czynów zabronionych, takich jak oszustwa. Osoba wspierająca ugrupowania o charakterze terrorystycznym wpłaca środki na odpowiedni rachunek powiązany z platformą hazardową. Środki przekazywane są z powrotem do omawianego klienta platformy pod postacią "wygranej", a następnie wykorzystane w procederze finansowania terroryzmu.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Dostęp do internetowych gier hazardowych jest stosunkowo łatwy, bo wciąż pojawiają się w sieci nowe domeny z grami hazardowymi. .Licencja wydana przez inne państwo jednak nie legalizuje działalności hazardowej w Polsce. W przypadku zagranicznych kasyn online łatwe jest ukrycie danych identyfikacyjnych gracza. Istnieje możliwość realizacji transakcji o charakterze międzynarodowym, zwłaszcza w przypadku dokonywania transakcji finansowych, w przypadku gdy rachunki podmiotu prowadzącego internetowe gry hazardowe są ulokowane za granicą. Tym niemniej Krajowa Administracja Skarbowa (KAS) we współpracy z Komisją Nadzoru Finansowego (KNF) opracował zasady dotyczące ograniczenia wykorzystywania instrumentów bądź usług płatniczych oferowanych przez dostawców usług płatniczych w Polsce do dokonywania transakcji związanych z nielegalną grą hazardową. Hostingodawcy natomiast usuwają/blokują dostęp do zabronionych treści związanych z nielegalnymi grami online. W grudniu 2018 r. powstało w Polsce pierwsze (legalne) kasyno online. Według ustawy, jedyną firmą która ma prawo oferować usługi tego rodzaju w sieci jest Totalizator Sportowy. Płatności w nim można dokonywać poprzez przelewy online, Visa, Dotpay czy BLIK. Wszystkie podmioty oferujące legalnie gry hazardowe są IO. Posiadają pewną świadomość swoich obowiązków z zakresu PPP/PFT, choć wciąż ujawniane są braki w ich wypełnianiu. Relatywnie niewiele – w porównaniu z innymi IO – informacji o podejrzanych transakcjach/podejrzanej działalności przekazywanych jest przez podmioty prowadzące działalność w zakresie gier hazardowych. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	1
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie internetowych gier hazardowych może być jedną z metod użycia nielegalnie pozyskanych środków na cele finansowania terroryzmu. Zgodnie jednak z polskimi przepisami urządzanie gier hazardowych przez Internet, z wyjątkiem zakładów wzajemnych i loterii promocyjnych jest objęte monopolem państwa. Przepisy prawne zakazują zarówno urządzania gier hazardowych przez sieć przez podmioty nieuprawnione, jak i uczestniczenie w takich grach. Działalność kontrolna KAS, utworzenie Rejestru domen służących do oferowania gier hazardowych niezgodnie z ustawą oraz blokowanie dostępu do zabronionych domen internetowych może negatywnie wpływać na możliwość użycia nielegalnie pozyskanych środków na cele finansowania terroryzmu. GIIF nie otrzymywał informacji o możliwości wykorzystywania w Polsce *modus operandi* polegającego na wykorzystaniu internetowych gier hazardowych dla finansowania terroryzmu. Sposób ten, z uwagi na uwarunkowania prawne, zdaje się być postrzegany przez sprawców jako mało atrakcyjny i stosunkowo ryzykowny, by legitymizować środki finansowe pochodzące z czynów zabronionych. Ponadto

	potrzebne jest planowanie, wiedza i umiejętności do zastosowania tego *modus operandi*. WNIOSEK: Wykorzystanie internetowych gier hazardowych stwarza niskie zagrożenie finansowaniem terroryzmu.

Prawną podstawą funkcjonowania rynku hazardowego w Polsce jest *ustawa o grach hazardowych z dnia 19 listopada 2009 r.*, wraz z późniejszymi nowelizacjami, w tym z kluczową dla tego rynku nowelizacją z 15 grudnia 2016 r. Rynek gier hazardowych w Polsce jest rynkiem regulowanym, nie jest objęty przepisami wspólnotowymi. Na rynku gier hazardowych w UE funkcjonuje zasada subsydiarności. Dla rynku hazardu oznacza to tyle, że zgodnie z tą zasadą kraje członkowskie mają możliwość niezależnego kreowania przepisów dotyczących hazardu na swoim terenie. Obejmuje to zarówno kwestie dostępu do rynku, kwestie podatkowe, jak i kwestie ochrony uczestników gier.

Światowy rynek gier hazardowych w większości segmentów tego rynku jest rynkiem regulowanym z ograniczeniami dostępu (poprzez systemy koncesji, licencji lub zezwoleń). Z uwagi na społeczną wrażliwość gier hazardowych, organy nadzoru starają się w ten sposób kontrolować podaż mając na względzie ochronę graczy. Ochrona graczy (jako obywateli konkretnego państwa) wiąże się z często występującym powierzeniem państwowym podmiotom prowadzenia gier o najwyższym ryzyku uzależnień. Należą do tego segmentu gry na automatach czy gry losowe online. Na światowym rynku gier hazardowych mamy też często do czynienia z funkcjonowaniem monopolu państwa w niektórych segmentach tego rynku. Najczęściej monopolem objęte są gry liczbowe i loterie pieniężne.

Immanentną cechą właściwie każdego rynku gier hazardowych na świecie jest występowanie podziału tego rynku na tzw. biały rynek, szarą strefę oraz czarny rynek. W wypadku rynku białego (legalnego) mamy z takim do czynienia, gdy operator jest operatorem posiadającym odpowiednią koncesję, licencję lub zezwolenie na organizację gier lub zakładów w tej samej jurysdykcji, w której znajduje się gracz. Szara strefa występuje natomiast w takich przypadkach, gdy operator jest licencjonowany na innym rynku krajowym niż ten, na którym znajduje się gracz. O czarnym rynku (nielegalnym) mówimy natomiast wtedy, gdy operator gier hazardowych nie posiada jakiegokolwiek zezwolenia w żadnej jurysdykcji. W zależności od konkretnej jurysdykcji definicje działalności nielegalnej mogą się oczywiście różnić, kładąc akcent na różne elementy związane z rynkiem gier hazardowych. Biorąc pod uwagę charakterystyczne elementy polskiego rynku gier hazardowych można stwierdzić, że właściwie nie występują na nim aktywne segmenty czarnego rynku. Poza rynkiem należącym do legalnych operatorów w Polsce występuje raczej tylko szara strefa. Jest to związane z tym, że firmy będące operatorami gier hazardowych, działające w szarej strefie nie mają problemów z zakładaniem legalnych spółek np. na Malcie i świadczeniem usług hazardowych polskim klientom. Według wielu opinii czarny rynek hazardu na terenie Europy kontynentalnej jest statystycznie raczej pomijalny, natomiast koncentruje się on głównie na rynkach USA, Azji i Australii.

Jak zauważono w ponadnarodowej ocenie ryzyka[64] (SNRA) sektor hazardowy charakteryzuje się szybkim wzrostem gospodarczym i rozwojem technologicznym, pomimo przypuszczalnego

[64] REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities; {SWD(2022) 344 final}

spadku w 2020 i 2021 roku z powodu kryzysu pandemii COVID-19. Całkowite przychody z gier hazardowych w Europie oszacowano w przedmiotowym dokumencie na 75,9 mld EUR w 2020 r. (23% spadek w porównaniu do 98,6 mld EUR przychodów brutto z gier w 2019 r.). Przychody z gier hazardowych online w UE i Wielkiej Brytanii oszacowano na około 26,3 mld EUR w 2020 r., w porównaniu z 16,5 mld w 2015 r. Przychody z rynku gier hazardowych offline/placówek stacjonarnych również spadły z około 77,5 mld EUR w 2015 r. do około EUR 49,6 mld w 2020 r. z powodu zamykania placówek stacjonarnych podczas kryzysu pandemii COVID-19.

W Polsce uczestnictwo w nielegalnych grach hazardowych jest przestępstwem skarbowym[65]. Dotyczy to też udziału w zagranicznej grze hazardowej lub w grze hazardowej urządzanej lub prowadzonej wbrew przepisom *ustawy z dnia 19 listopada 2009 r. o grach hazardowych* lub warunkom koncesji lub zezwolenia. Przestępstwo to jest zagrożone karą grzywny do 120 stawek dziennych.

Uczestnik nielegalnie urządzanej gry hazardowej podlega też karze pieniężnej w wysokości 100% uzyskanej wygranej bez pomniejszenia o wpłacone stawki. Legalnie można uczestniczyć jedynie w grach urządzanych przez podmioty posiadające zezwolenie na domenach wymienionych na stronie Portalu Podatkowego.

Podatność sektora

Na podstawie ustawy AML/CTF wszystkie podmioty prowadzące działalność w zakresie gier losowych, zakładów wzajemnych, gier w karty i gier na automatach w rozumieniu *ustawy z dnia 19 listopada 2009 r. o grach hazardowych* są instytucjami obowiązanymi. Powoduje to obowiązek stosowania środków bezpieczeństwa finansowego w każdym przypadku obstawiania stawek oraz odbioru wygranych o równowartości 2000 euro lub większej, bez względu na to, czy transakcja jest przeprowadzana jako pojedyncza operacja, czy kilka operacji, które wydają się ze sobą powiązane.

Wymienione w ustawie środki bezpieczeństwa finansowego obejmują przede wszystkim czynności związane z identyfikacją klienta oraz weryfikacją jego tożsamości; identyfikację beneficjenta rzeczywistego oraz podejmowanie uzasadnionych czynności w celu weryfikacji jego tożsamości. Ponadto ww. instytucje obowiązane badają źródła pochodzenia wartości majątkowych będących w dyspozycji klienta w przypadkach uzasadnionych okolicznościami, monitorują na bieżąco klientów oraz monitorują ich transakcje w celu wytypowania transakcji podejrzanych.

Na skutek pandemii koronawirusa i ustanowienia wielu ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii pomiędzy 2020 r. a 2021 r. nastąpił duży wzrost nielegalnej aktywności w obszarze gier hazardowych. Duża część graczy nie ma świadomości, że uczestniczy w nielegalnie organizowanych grach hazardowych (z reguły u operatora zagranicznego). Nie wiedzą też, w jaki sposób znaleźć legalnego operatora, ponieważ zgodnie z obowiązującymi przepisami w przestrzeni publicznej nie ma o takich operatorach wystarczających informacji.

Oceniając poziom podatności systemu w obszarze gier hazardowych należy mieć na uwadze potencjalne możliwości infiltracji lub przejęcia przez zorganizowane grupy przestępcze

[65] https://www.podatki.gov.pl/pozostale-podatki/gry-hazardowe/rejestr-domen/ , dostęp 26.01.2023 r.

operatorów rynku lub firm pośredniczących, za pomocą których ci operatorzy działają na rynku. Najmniejsze ryzyko infiltracji operatora rynku gier hazardowych czy przejęcia podmiotu pośredniczącego w sprzedaży usług gier hazardowych występuje wtedy, gdy mamy do czynienia z monopolem państwa na konkretnym rynku. Duże znaczenie ma też objęcie operatorów rynku gier hazardowych systemem reglamentacji działalności gospodarczej, której wykonywanie wymaga spełnienia określonych warunków, przewidzianych w prawie.

W dystrybuowanej przez GIIF w sierpniu 2021 r. do instytucji obowiązanych i jednostek współpracujących ankiecie, zawierającej prośbę o wskazanie 5 produktów (maksymalnie) i usług oferowanych poza rynkiem finansowym, które są lub mogą być najczęściej wykorzystywane do prania pieniędzy, internetowe gry hazardowe znalazły się wśród 5 produktów i usług najczęściej wymienianych zarówno przez jednostki współpracujące, jak i instytucje obowiązane. Rynek internetowych gier hazardowych w Polsce jest rynkiem regulowanym. Zgodnie z treścią art. 5 ust. 1b *ustawy o grach hazardowych* urządzanie gier hazardowych przez sieć Internet, z wyjątkiem zakładów wzajemnych i loterii promocyjnych, jest objęte monopolem państwa. Jedyne kasyno internetowe, w którym można grać legalnie na pieniądze to Total Casino, nadzorowane przez Totalizator Sportowy. Total Casino udostępnia metody dokonywania płatności takie jak: Dotpay, BLIK, karty płatnicze, przelew bankowy. Ponadto Total Casino akceptuje płatności jedynie w złotówkach. W celu ochrony rynku internetowych gier hazardowych minister właściwy do spraw finansów publicznych prowadzi Rejestr domen służących do oferowania gier hazardowych niezgodnie z ustawą. Rejestr jest jawny i każdy ma prawo dostępu do danych zawartych w Rejestrze. Wpisowi do Rejestru podlega nazwa domeny internetowej wykorzystywanej do urządzania gier hazardowych lub nazwa domeny służącej do reklamowania lub promowania gier hazardowych niezgodnie z przepisami prawa dostępnej dla znajdujących się na terytorium RP użytkowników sieci Internet.

W świetle obowiązujących przepisów ustawy *o grach hazardowych*, stacjonarne kasyna gry mogą być prowadzone przez podmioty prywatne – działalność kasyn jest jednak koncesjonowana. O koncesję, przyznawaną na 6 lat, mogą starać się jedynie spółki z ograniczoną odpowiedzialnością lub spółki akcyjne, które dysponują kapitałem zakładowym wynoszącym co najmniej 4 miliony złotych, wobec których to spółek nie istnieją uzasadnione zastrzeżenia z punktu widzenia bezpieczeństwa państwa, porządku publicznego, bezpieczeństwa interesów ekonomicznych państwa, a także przestrzegania przepisów regulujących przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Ponadto podmioty chcące prowadzić kasyno – o ile spełnią warunki ustawowe – muszą jeszcze wziąć udział w przetargu ogłoszonym przez Ministra Finansów, jeśli o koncesję w danym miejscu stara się więcej niż tylko jeden podmiot. Dopuszczalna liczba kasyn stacjonarnych uzależniona jest też od uwarunkowań geograficznych i społecznych. Liczba kasyn stacjonarnych ustalana jest w zależności od liczby mieszkańców – na obszar, w którym mieszka mniej niż 250 tysięcy osób przypada jedno kasyno, a na każde kolejne 250 tysięcy liczba kasyn może być zwiększona odpowiednio o jedno. Jednakże łączna liczba kasyn gry w województwie nie może być wyższa niż 1 kasyno na każde pełne 650 tys. mieszkańców województwa. W praktyce kasyna stacjonarne charakteryzują się niewielką podatnością na pranie pieniędzy czy finansowanie terroryzmu. Koncesjonowane kasyna stacjonarne stosują środki bezpieczeństwa finansowego, przechowują dane, a także osobie wchodzącej do kasyna robione jest zdjęcie. Dzięki temu pracownicy kasyna wiedzą, kto o której godzinie wszedł do kasyna, jaki dokument tożsamości pokazała osoba oraz jak wyglądała osoba wchodząca do kasyna. Dzięki temu możliwa jest

prawidłowa identyfikacja, nawet jeśli dana osoba posługuje się jednym lub kilkoma fałszywymi dokumentami tożsamości. Kasyna korzystają np. z oprogramowania do rozpoznawania twarzy. W obszarze kasyna systemy telewizji przemysłowej obejmują nie tylko obszar gier, ale także inne kluczowe obszary działalności. Wszystkie odbywające się w kasynie transakcje są monitorowane i dokumentowane. Istotnym jest, że kwoty gotówki, które potencjalnie można by było wyprać w kasynie, są bardzo ograniczone z uwagi na to, że każda znacząca ilość gotówki natychmiast zwróciłaby uwagę pracowników kasyna. Ponadto już samo żądanie wydania zaświadczenia o wygranej z kasyna powoduje działania weryfikacyjne dotyczące przebiegu gry żądającego, przeprowadzane przez personel kasyna.

Urządzanie gier na automatach dozwolone jest jedynie w salonach gier na automatach. Samo prowadzenie salonów zostało powierzone Totalizatorowi Sportowemu (na koniec 2020 roku funkcjonowało ponad 500 salonów gier, natomiast na koniec 2021 roku prawie 900 salonów gier). Salony gier na automatach objęte są ponadto restrykcjami, takimi jak: wymóg rejestracji graczy; wymogi lokalizacyjne salonów gier - nie więcej niż 1 salon na 1 000 mieszkańców powiatu; limity czasowe i kwotowe dotyczące gry na automatach; wymóg prowadzenia systemu centralnego rejestrującego zdarzenia w czasie rzeczywistym; wymóg prowadzenia systemu audiowizyjnego; system certyfikacji automatów; zakaz jackpotów.

Zakłady wzajemne są działalnością regulowaną i mogą być organizowane przez podmioty prywatne działające w formie spółki z ograniczoną odpowiedzialnością lub spółki akcyjnej. Przepisy przewidują również wymóg minimalnej wysokości kapitału zakładowego spółki (operatora), który dla podmiotów z branży bukmacherskiej został przewidziany na poziomie 2 000 000 zł. Zezwolenie Ministra Finansów na urządzanie zakładów wzajemnych jest uzyskiwane przez podmioty osobno w stosunku do urządzania zakładów wzajemnych w punktach naziemnych, a osobno do urządzania i prowadzenia działalności w zakresie zakładów wzajemnych przez Internet. W celu ochrony rynku zakładów wzajemnych funkcjonuje wspomniany wyżej rejestr domen służących do oferowania gier hazardowych niezgodnie z ustawą, prowadzony przez Ministra Finansów.

Legalna część branży kasyn i zakładów bukmacherskich online[66] wygenerowała w tym czasie 26,6 mld zł obrotu, podczas gdy legalne podmioty na stacjonarnym rynku osiągnęły obroty na poziomie 7,4 mld zł (1,5 mld zł bukmacherzy oraz 5,9 mld zł kasyna). Zatem wartość obrotów całego rynku kasyn i zakładów bukmacherskich w Polsce osiągnęła 61,7 mld zł, nie licząc szarej strefy na rynku stacjonarnym.

Nadzór nad przestrzeganiem prawa przez podmioty organizujące gry hazardowe poprzez wykonywanie kontroli celno-skarbowych sprawuje minister finansów i organy KAS. Podstawę prowadzenia kontroli rynku gier hazardowych stanowi *ustawa z dnia 16 listopada 2016 r.*

[66] https://www.isbtech.pl/2022/12/raport-ey-szara-strefa-w-branzy-hazardowej-online-to-juz-ponad-50/, dostęp 26.01.2023 r. Według raportu firmy doradczej EY sporządzonego dla stowarzyszenia "Graj Legalnie", obroty wygenerowane w szarej strefie rynku hazardowego online w Polsce wyniosły 27,7 mld zł w 2021 roku. Oznacza to, że szara strefa w ujęciu obrotów stanowiła w ubiegłym roku 51,0% całego rynku kasyn i zakładów bukmacherskich online. Tym samym skarb państwa stracił z tytułu nieodprowadzonego podatku od gier 782 mln zł w 2021 roku. Eksperci EY szacują, że w 2021 roku wartość obrotów w szarej strefie internetowego rynku kasyn i zakładów bukmacherskich wyniosła 27,7 mld zł, co stanowiło 51,0% obrotów na tym rynku. Z przedmiotowego badania wynika także, że 22 proc. polskich użytkowników gier hazardowych online wykorzystuje w celu gry w nielegalnie funkcjonującym kasynie lub u bukmachera, obce waluty. Ponadto 16 proc. graczy posługuje się aplikacjami typu VPN. Te dwa rozwiązania są sposobem na obchodzenie blokad nielicencjonowanych operatorów hazardowych. Coraz powszechniejsze są też płatności w kryptowalutach.

o Krajowej Administracji Skarbowej (Dz. U. z 2023 r. poz. 615). Do zadań Krajowej Administracji Skarbowej należy wykonywanie kontroli celno-skarbowych w obszarze gier hazardowych oraz rozpoznawanie, wykrywanie, zapobieganie i zwalczanie przestępstw skarbowych i wykroczeń skarbowych przeciwko organizacji gier hazardowych oraz ściganie ich sprawców. Do zadań KAS należy również prowadzanie kontroli podatkowych podatku od gier oraz dopłat. Ogółem w roku 2021 organy KAS przeprowadziły 1 004 kontrole celno-skarbowe[67] przestrzegania przepisów regulujących urządzanie i prowadzenie gier hazardowych (o 315 kontroli więcej niż w roku 2020). Organami uprawnionymi do wykonywania kontroli celno-skarbowych w zakresie określonym *ustawą o grach hazardowych w* roku 2021 byli naczelnicy urzędów celno-skarbowych.

Sam sektor gier hazardowych jest sektorem zróżnicowanym pod względem podatności na możliwość prania pieniędzy czy finansowania terroryzmu. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek PP w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców.

Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie.

Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.

Zagrożenia w sektorze

W sektorze gier hazardowych pod względem oceny zagrożenia praniem pieniędzy internetowe gry hazardowe znalazły się wśród 5 produktów i usług najczęściej wymienianych zarówno przez jednostki współpracujące, jak i instytucje obowiązane. Jak z powyższego wynika, głównym czynnikiem zagrożenia nie są konkretne gry czy formy uprawiania hazardu, ale charakter przeprowadzanych transakcji w formie online. Właściwie wszystkie produkty hazardowe są dostępne online. Zagrożenie może jeszcze być pogłębione przez anonimizację transakcji na rynku gier hazardowych (zwłaszcza u operatorów zagranicznych) spowodowaną wykorzystaniem Internetu w celu zawarcia transakcji. Niektóre z produktów istniejących na rynku gier hazardowych online stwarzają szczególne ryzyko, ponieważ można dokonywać zakładów poprzez kilka posiadanych rachunków i obstawiać właściwie każdy możliwy wynik, przez co zmniejsza się ryzyko przegranej. W przypadku pokera online (szczególnie u operatorów zagranicznych) istnieje również potencjalnie szczególne ryzyko zmowy.

Co do zasady internetowe gry hazardowe powinny się opierać na płatnościach z rachunków bankowych lub płatniczych, na których klient jest już zidentyfikowany i zweryfikowany przez finansowe instytucje obowiązane dostarczające mu ww. rachunki. Tym niemniej w niektórych przypadkach platform gier hazardowych operatorów zagranicznych istnieje możliwość korzystania z mniej identyfikowalnych sposobów płatności, tj. anonimowych/przedpłaconych pieniędzy elektronicznych lub nawet walut wirtualnych, jeśli są dozwolone. Dotyczy to zwłaszcza platform hazardowych nie posiadających żadnej koncesji, które nie podlegają wymogom należytej staranności wobec klientów, wymogom prowadzenia rejestrów i sprawozdawczości. Platformy te nie są kontrolowane przez żaden organ nadzorczy. Zdarza

[67] Informacja o realizacji *ustawy o grach hazardowych* w roku 2021; Warszawa 2022 r. https://www.podatki.gov.pl/pozostale-podatki/gry-hazardowe/raporty/ dostęp 27.01.2023 r.

się też, że platforma gier hazardowych online znajduje się w jednym państwie członkowskim UE, a emitent pieniądza elektronicznego udostępnia środki w innym państwie członkowskim. Czasami platformy gier hazardowych są koncesjonowane w jednym państwie, ale działają na terenie innego państwa przez pośrednika. W takich sytuacjach dochodzi do konfliktu jurysdykcyjnego, dotyczącego tego, która jurysdykcja jest właściwa do dokonywania czynności nadzorczych i pod jakim kątem badać stosowanie wymogów dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu.

Na rynku gier hazardowych istnieją potencjalnie duże możliwości naruszenia przepisów karnych. Policja, opisując sposoby działania przestępców z wykorzystaniem sieci Internet wskazała na potencjalną możliwość omijania polskich regulacji i przeniesienie zjawiska nielegalnych gier hazardowych do cyberprzestrzeni: W obszarze internetowych gier hazardowych mających wpływ na możliwość prania pieniędzy Policja identyfikuje kilka modus operandi, które polegają na tym, że:

- niekoncesjonowane w Polsce kasyna online w swoich regulaminach dopuszczają możliwość transferowania środków finansowych między klientami bez użycia konta kasyna. Powoduje to, że klienci mogą zatem potencjalnie pożyczać środki finansowe z nieznanych, nieweryfikowalnych źródeł. W istotny sposób takie kasyna zwiększają zagrożenie prania pieniędzy czy finansowania terroryzmu powodując możliwość wykorzystania do transakcji środków finansowych pochodzących z nielegalnej działalności;
- większość kasyn online ma przepisy dotyczące wniesienia depozytu. Jest to kwota, jaką należy wpłacić by uczestniczyć w ogólnych transakcjach, lub kwota, którą należy wpłacić, aby ubiegać się o bonus kasynowy. Wiele e-portfeli akceptuje gotówkę jako depozyty. Klienci dokonują wpłaty do e-portfela za pomocą konta instytucji finansowych, natomiast potwierdzenie wydane przez tę instytucję będzie uwzględniało jedynie wpłatę do e-portfela, a nie transakcję z kasynem internetowym;
- w wypadku gry w pokera w Internecie gra ta często ma miejsce na platformach, które są dzielone przez wielu operatorów kasyn. Sama platforma odgrywa kluczową rolę w monitorowaniu wzoru oraz wartości gry z punktu widzenia potencjalnych działań związanych z praniem pieniędzy, na przykład dumpingiem żetonów. Strategia taka polega na tym, że gracze będący w zmowie świadomie wykonują zagrania, które mają na celu sztuczne sterowanie dystrybucją żetonów (np. do jednego z góry wskazanego gracza), dla zapewnienia sobie korzyści;
- przy wykorzystaniu internetowych gier hazardowych przestępcy wpłacają środki na odpowiedni rachunek powiązany z platformą hazardową zagranicznego operatora. Następnie środki przekazywane są z powrotem do klienta platformy pod postacią tzw. „wygranej", co umożliwia ukrycie danych identyfikacyjnych gracza, zwłaszcza w przypadku zagranicznych kasyn online.

W sektorze gier hazardowych niewielkie zagrożenie oraz wykazaną niską podatność na pranie pieniędzy i finansowanie terroryzmu należy stwierdzić w odniesieniu do loterii fantowych. Biorąc pod uwagę całość rynku gier hazardowych loterie fantowe stanowią niszowy, nieistotny pod względem wielkości obrotów finansowych rodzaj gier hazardowych. W przeciwieństwie do innych rodzajów hazardu w loteriach fantowych dopuszczony został udział osób niepełnoletnich. Jako charakterystyczne cechy loterii fantowych uwzględnia się w szczególności zależność wyniku gry od przypadku, konieczne określenie warunków gry w

regulaminie oraz oferowanie przez podmiot urządzający grę wyłącznie wygranych rzeczowych (nie jest możliwe, by wygraną stanowiły pieniądze). Organizacja loterii dokonywana jest zgodnie z zezwoleniem, o które może wystąpić osoba fizyczna, osoba prawna czy jednostka organizacyjna bez osobowości prawnej. Jeśli wartość puli wygranych nie będzie przekraczać wartości kwoty bazowej, wystarczy dokonać zgłoszenia organizacji loterii właściwemu Naczelnikowi Urzędu Celno-Skarbowego na co najmniej 30 dni przed planowanym wydarzeniem. W przypadku organizowania loterii przez organizację pożytku publicznego wartość puli wygranych może wynosić do piętnastokrotności kwoty bazowej przy zachowaniu limitu łącznej wartość puli wygranych nie wyższej niż trzydziestokrotność kwoty bazowej. Organizator takiej loterii musi najpóźniej 30 dni po jej zakończeniu przedstawić sprawozdanie z realizacji loterii. Odpowiedniemu zabezpieczeniu muszą podlegać losy na loterię, tj. muszą być zabezpieczone przed manipulacjami, a organizator musi zapewnić możliwość ich kontroli. Również osoby organizujące loterię muszą spełnić określone wymagania np. muszą być niekarane. Ponadto dochód z loterii fantowej musi być w całości przeznaczany na realizację określonych w regulaminie gry celów społecznie użytecznych, w szczególności dobroczynnych. Kwota bazowa dla ustalenia wartości nagród w roku 2022 r. określona została na 5 774,13 zł. Piętnastokrotność tej kwoty to 86 611,95 zł, a trzydziestokrotność 173 223,90 zł. Pomijając możliwość manipulacji wartością nominalną nagród, loterie fantowe dają teoretyczną możliwość transferu kilkudziesięciotysięcznych wartości, ale w praktyce zdecydowanej większości loterii fantowych przytoczone wartości kwot nagród są dużo niższe. Ponieważ większość loterii fantowych jest organizowana przez organizacje pozarządowe w toku wydarzeń okolicznościowych dla danej społeczności, a poziom szacunków wartości przeznaczanych na nagrody jest w tych loteriach wartościowo niewielki – można określić obszar loterii fantowych jako obszar o niewielkim zagrożeniu dla prania pieniędzy i finansowania terroryzmu. Najczęściej nagrodami są drobne przedmioty o niskiej wartości, niejednokrotnie wykonane własnoręcznie lub pozyskane w ramach lokalnej społeczności. Nie jest możliwa do określenia średnia wartość fantów przekazywanych w trakcie losowania loterii fantowych, tym niemniej ich łączna wartość nie jest wyższa niż piętnastokrotność kwoty bazowej. Ich praktyczna wartość z punktu widzenia narażenia na pranie pieniędzy czy finansowanie terroryzmu nie jest stosunkowo istotna. Dla oddania skali obrotu w wypadku loterii fantowych całkowity podatek deklarowany przez podatników wyniósł 13 tys. zł w 2019 r. oraz 4 tys. zł w 2020 r. Nastąpił spadek o 9 tys. zł rok do roku tj. o 67,1 %. Porównując podatek w obszarze loterii fantowych do podatku w obszarze np. loterii pieniężnych (225 mln zł w 2019 r. i 219 mln zł w 2020 r.) widoczny jest incydentalny udział podatku od loterii fantowych (właściwie pomijalny) w całości podatku od gier hazardowych. Wskazuje to też niewątpliwie na nieistotne dla obszaru hazardu wielkości wartości finansowych, które są w obrocie związanym z loteriami fantowymi.

Jak wynika z ponadnarodowej oceny ryzyka (SNRA) nie ma dowodów na to, że grupy terrorystyczne wykorzystywały platformy gier online do finansowania terroryzmu. Natomiast wydaje się, że pewne luki systemowe w przepisach dotyczących gier hazardowych online stwarzają potencjał do ewentualnych przyszłych nadużyć ze strony terrorystów oraz ich popleczników, którzy byliby w stanie dokonywać finansowania terroryzmu z wykorzystaniem przedmiotowego sektora. W swojej praktyce GIIF nie otrzymywał informacji o możliwości wykorzystywania w Polsce modus operandi polegającego na wykorzystaniu sektora gier internetowych, w tym internetowych gier hazardowych dla finansowania terroryzmu. Brak również informacji, by sektor ten był przedmiotem działań operacyjnych polskich organów ścigania w przedmiocie finansowania terroryzmu.

Uśredniony poziom zagrożenia sektora gier hazardowych – ML - 2,75 i FT – 1

Uśredniony poziom podatności sektora gier hazardowych – ML - 2,0 i FT – 2

Oszacowany poziom prawdopodobieństwa dla sektora – ML – 2,30 i FT - 1,60

Poziom ryzyka jest ostatecznie określany przez kombinację zagrożenia i podatności. Macierz ryzyka określająca ten poziom ryzyka opiera się na wadze 40% (zagrożenie) + 60% (podatność) – przy założeniu, że komponent podatności ma większą zdolność określania poziomu ryzyka. Zakłada się, że poziom podatności może zwiększyć atrakcyjność, a tym samym zamiary przestępców/terrorystów, aby użyć danego modus operandi – wpływając w ten sposób ostatecznie na poziom zagrożenia. Poziom ryzyka sektora, z uwzględniem prawdopobieństwa i konsekwencji (współczynnik 2,5 dla PP i 1,5 dla FT), jest ustalany zgodnie z metodyką krajowej oceny ryzyka – aneks nr 1.

Ryzyko FT sektora gier hazardowych – 1,56	
1 – 1,5	Niskie
1,6 – 2,5	Średnie
2,6 – 3,5	Wysokie
3,6 – 4	Bardzo wysokie
Ryzyko ML sektora gier hazardowych – 2,38	
1 – 1,5	Niskie
1,6 – 2,5	Średnie
2,6 – 3,5	Wysokie
3,6 – 4	Bardzo wysokie

WNIOSEK 1: Poziom ryzyka wykorzystania sektora gier hazardowych do finansowania terroryzmu w Polsce znajduje się na poziomie niskim.

WNIOSEK 2: Poziom ryzyka wykorzystania sektora gier hazardowych znajduje się na poziomie średnim.

Mitygacja zidentyfikowanych ryzyk:

W celu ograniczenia prawdopodobieństwa wykorzystania sektora gier hazardowych do prania pieniędzy lub finansowania terroryzmu, zasadne jest podjęcie odpowiednich działań. Stosowanie zaproponowanych działań mitygujących powinno następować z uwzględnieniem rozpoznanego przez daną instytucję obowiązaną ryzyka.

Instytucje obowiązane z sektora gier hazardowych powinny zwracać szczególną uwagę na przypadki wpłaty większej ilości gotówki, szczególnie przez nierezydentów UE. Zasadnym byłoby pozyskiwanie informacji na temat źródła pochodzenia wartości majątkowych, np. poprzez weryfikację deklaracji dewizowych klientów z państw spoza UE.

Instytucje obowiązane powinny przywiązywać szczególną wagę do bieżącej analizy transakcji przeprowadzanych przez klientów będących firmami hazardowymi, jak również klientów uzyskujących zyski z hazardu. Szczególnie dotyczy to klientów wypłacających zyski z hazardu pochodzące od operatorów zagranicznych.

Podmioty z sektora gier hazardowych, w tym świadczące usługi online, powinny wprowadzać i rozwijać zaawansowane narzędzia i systemy informatyczne, wspomagające realizację celów przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, w szczególności poprzez usprawnienie oraz automatyzację procesów związanych z bieżącą analizą przeprowadzanych transakcji.

Podmioty sektora gier hazardowych powinny wzmacniać działania związane z odpowiednią oceną stosunków gospodarczych, w szczególności poprzez uzyskiwanie odpowiednich informacji na temat klienta, źródła pochodzenia wartości majątkowych oraz celu i zamierzonego charakteru stosunków gospodarczych. Należy również podkreślić konieczność aktualizacji zgoromadzonych informacji o kliencie.

W sektorze gier hazardowych powinny być podejmowane działania wzmacniające poziom świadomości narażenia na przestępstwo prania pieniędzy oraz finansowania terroryzmu, jak również podnoszące poziom wyszkolenia pracowników tego sektora w analizie sygnałów ostrzegawczych wynikających z transakcji podejrzanych.

Zalecane jest uczestnictwo przedstawicieli instytucji obowiązanych w szkoleniach podnoszących świadomość AML/CTF, organizowanych zarówno przez GIIF, jak i przez UKNF w ramach Programu CEDUR.

Instytucje Obowiązane z sektora gier hazardowych powinny zwracać szczególną uwagę na transfery środków do jurysdykcji charakteryzujących się wyższym ryzykiem prania pieniędzy oraz finansowania terroryzmu (w szczególności wypłaty z kont klientów podmiotów świadczących usługi online). Instytucje obowiązane powinny położyć szczególny nacisk na ustalenie źródła pochodzenia wartości majątkowych będących w dyspozycji klienta, jak również na możliwość pozyskania od klienta dokumentów weryfikujących przekazane informacje na temat źródła pochodzenia wartości majątkowych.

Instytucje obowiązane powinny przykładać szczególną wagę do czynników geograficznych mogących wskazywać na wyższe ryzyko prania pieniędzy czy też finansowania terroryzmu, takich jak niestabilna sytuacja polityczna czy konflikt zbrojny, czego najdobitniejszym przykładem w ostatnich latach jest wojna prowadzona przez Rosję przeciwko Ukrainie. Z uwagi na wysokie ryzyko transferowania środków pochodzących z nielegalnego handlu, przemytu ludzi, handlu bronią czy też działań zmierzających do omijania sankcji gospodarczych, szczególnie istotne jest analizowanie przez instytucje obowiązane źródła pochodzenia wartości majątkowych klienta. Podmioty z sektora gier hazardowych powinny zwracać szczególną uwagę na klientów z jurysdykcji objętych konfliktem, obstawiających wysokie kwoty czy też przejawiających agresywny styl gry.

10. Obszar – organizacje typu non-profit

Opis sektora – zawarty jest w podrozdziale 2.2 – „Rynek pozafinansowy" oraz w podrozdziale 7.2.2 - „Podatność rynku pozafinansowego".

Scenariusze wystąpienia ryzyka (tj. możliwe przykłady wystąpienia ryzyka) dotyczyły wykorzystania do prania pieniędzy działalności charytatywnej prowadzonej przez fundacje i stowarzyszenia; wykorzystania gier oferowanych w kasynie do zaciemnienia pochodzenia posiadanych pieniędzy, a do finansowania terroryzmu schematów wykorzystania funduszy gromadzonych na cele charytatywne na finansowanie organizacji terrorystycznych. Opis scenariuszy znajduje się poniżej.

Pranie pieniędzy

Tabela 47

Rodzaj wykorzystanych usług, produktów finansowych	Działalność charytatywna
Ogólny opis ryzyka	Wykorzystanie fundacji i stowarzyszeń do prania pieniędzy
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Przestępcy przekazują za pośrednictwem różnych słupów i przedsiębiorstw symulujących pieniądze pochodzące z nielegalnej działalność na rzecz kontrolowanych przez siebie fundacji i stowarzyszeń tytułem darowizn. Pieniądze są następnie przekazywane na rzecz przestępców lub osób z nimi powiązanych tytułem stypendiów, zapomóg, pożyczek na działalność gospodarczą, odpowiednio do zapisów statutowych tych podmiotów. 2. Założenie organizacji typu non-profit w celu przelewania środków pieniężnych (z tytułu 'wynagrodzenia') osobom zatrudnionym nielegalnie na terenie RP.
Poziom podatności	3
Uzasadnienie dla poziomu podatności	Założenie fundacji lub stowarzyszenia jest utrudnione (wymagane jest spełnienie konkretnych obowiązków, m.in. sporządzenie statutu, rejestracja w KRS, ponadto należy liczyć się z nadzorem organów administracji publicznej). Łatwe jest ukrycie danych identyfikacyjnych prawdziwych darczyńców i beneficjentów, zwłaszcza w przypadku gdy fundacja lub stowarzyszenie jest kontrolowane przez sprawców. Istnieje możliwość realizacji transakcji o charakterze międzynarodowym. Fundacje i stowarzyszenia posiadające osobowość prawną są IO jedynie w zakresie, w jakim przyjmują lub dokonują płatności w gotówce o wartości równej lub przekraczającej równowartość 10 tys. EUR, bez względu na to, czy płatność jest przeprowadzana jako pojedyncza operacja, czy kilka operacji, które wydają się ze sobą powiązane. Ww. podmioty posiadają pewną świadomość swoich obowiązków z zakresu PPP/PFT, choć wciąż ujawniane są braki w ich wypełnianiu. Nie przekazują lub przekazują relatywnie mało informacji o podejrzanych transakcjach/podejrzanej działalności do GIIF. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek prania pieniędzy w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	3
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie mechanizmu polegającego na zakładaniu fundacji i stowarzyszeń, za pośrednictwem których będą przekazywane wybranym beneficjentom środki finansowe może być postrzegane w Polsce jako dosyć atrakcyjna metoda prania pieniędzy. Brudne pieniądze – w wielu schematach –

	mogą być przekazywane do legalnie działających fundacji bądź stowarzyszeń, by potem, zgodnie ze statutem danej fundacji/stowarzyszenia, zasilić legalnymi już środkami konkretnych beneficjentów bądź ich firmy. Donatorami mogą być podmioty krajowe bądź zagraniczne, z którymi w razie potrzeby poprowadzenia śledztwa może być niemożliwy kontakt. Swoboda dysponowania środkami finansowymi przez każdego posiadacza i brak konieczności tłumaczenia się z podjętych decyzji o donacji konkretnej fundacji wpływa na atrakcyjność tego *modus operandi.* Stosowanie tej metody nie wymaga od podmiotu legalizującego środki pochodzące z czynu zabronionego wysokospecjalistycznej wiedzy, dużego planowania czy unikalnych umiejętności. Czasami towarzyszą tej metodzie porady kancelarii prawnych czy wyspecjalizowanych kancelarii podatkowych. W niektórych przypadkach może być wykorzystywana fałszywa dokumentacja. WNIOSEK: Zakładanie fundacji i stowarzyszeń by przekazywać poprzez nie środki pochodzące z nielegalnych źródeł stanowi wysokie zagrożenie prania pieniędzy.

Finansowanie terroryzmu

Tabela 48

Rodzaj wykorzystanych usług, produktów finansowych	Działalność charytatywna
Ogólny opis ryzyka	Wykorzystanie funduszy gromadzonych na cele charytawne na finansowanie organizacji terrorystycznych
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Wykorzystanie kontrolowanych przez terrorystów organizacji charytatywnych (zarejestrowanych i niezarejestrowanych) do gromadzenia i przekazywania pieniędzy na cele organizacji terrorystycznych. 2. Przeznaczenie środków na finansowanie terroryzmu przez osoby działające w ramach NPO - na etapie zbierania, tj. przed wpłaceniem środków na rachunek organizacji. 3. Zwolennik grupy terrorystycznej, mający dostęp do pieniędzy gromadzonych przez legalną organizację charytatywną jako jej pracownik, odpowiedzialny za ich księgowanie lub nadzór nad tym obszarem, ułatwia ich przekazanie na cele tejże grupy terrorystycznej. 4. Podszywanie się przez zwolenników grup terrorystycznych pod legalnie działające organizacje charytatywne i gromadzenie pieniędzy pod fikcyjnymi tytułami celem przekazania ich na cele tych grup. 5. W organizacji charytatywnej, kontrolowanej przez zwolenników grup terrorystycznych, fundusze gromadzone na potrzeby pomocy humanitarnej są mieszane ze środkami gromadzonymi na cele terrorystyczne, celem ich ukrycia i łatwiejszego transferowania na rzecz tych grup terrorystycznych. 6. Fundusze gromadzone na legalne cele charytatywne - po ich przesłaniu do miejsc docelowych w obszarach konfliktu lub w ich sąsiedztwie - są przejmowane przez organizacje terrorystyczne dla swoich celów. 7. Pobieranie przez dostawców z zakresu usług transferu środków pieniężnych "podatku" za przekazywanie środków pochodzących od tych organizacji w rejon docelowy. "Podatek" jest następnie przekazywany organizacji terrorystycznej prowadzącej działalność na danym terytorium. 8. Przesyłanie przez NPO środków od darczyńców do zagranicznego NPO, który przeznaczył otrzymane wartości majątkowe na finansowanie terroryzmu.
Poziom podatności	3
Uzasadnienie dla poziomu podatności	Założenie fundacji lub stowarzyszenia jest utrudnione (wymagane jest spełnienie konkretnych obowiązków, m.in. sporządzenie statutu, rejestracja w KRS, ponadto należy liczyć się z nadzorem organów administracji publicznej). Łatwe jest ukrycie danych identyfikacyjnych prawdziwych darczyńców i beneficjentów, zwłaszcza w przypadku gdy fundacja lub stowarzyszenie jest kontrolowane przez sprawców. Istnieje możliwość realizacji transakcji o charakterze

	międzynarodowym. Fundacje i stowarzyszenia posiadające osobowość prawną są IO jedynie w zakresie, w jakim przyjmują lub dokonują płatności w gotówce o wartości równej lub przekraczającej równowartość 10 tys. EUR, bez względu na to, czy płatność jest przeprowadzana jako pojedyncza operacja, czy kilka operacji, które wydają się ze sobą powiązane. Ww. podmioty posiadają pewną świadomość swoich obowiązków z zakresu PPP/PFT, choć wciąż ujawniane są braki w ich wypełnianiu. Nie przekazują lub przekazują relatywnie mało informacji o podejrzanych transakcjach/podejrzanej działalności do GIIF. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	2
Uzasadnienie dla poziomu zagrożenia	Organizacje charytatywne mogą być wykorzystywane przez ugrupowania terrorystyczne do ich finansowania na różne sposoby. Może to polegać na bezpośrednim przekazywaniu części pozyskiwanych przez NPO środków na cele działalności terrorystycznej albo na przekazywaniu całości środków pozyskiwanych przez NPO, gdy organizacja ta jest tylko kamuflażem dla działalności terrorystycznej. Organizacja charytatywna może również prowadzić rzeczywistą działalność charytatywną, jednak pomoc udzielana jest przez komórki tej organizacji, które są kontrolowane przez członków związanych z ugrupowaniami terrorystycznymi. Prowadzi to do sytuacji, w której beneficjenci pomocy są przeświadczeni, że otrzymują wsparcie od organizacji terrorystycznej. Takie działanie przynosi spore korzyści propagandowe. NPO są wykorzystywane przez organizacje terrorystyczne, gdyż poprzez działalność charytatywną cieszą się one dużym zaufaniem społecznym. Przekazywane za pośrednictwem NPO treści mają duży wpływ na postawy ludzi, a ewentualne przeciwdziałanie organów państwowych może się spotkać z zarzutami o prześladowania, rasizm, łamanie praw człowieka. Samo stosowanie tego *modus operandi* jest postrzegane z ww. powodów za dosyć atrakcyjne i bezpieczne. Przygotowanie logistyki dla takich operacji to średni poziom przygotowania. GIIF otrzymywał nieliczne informacje o możliwości wykorzystania tej metody do finansowania działalności terrorystycznej. WNIOSEK: Wykorzystanie organizacji charytatywnych dla finansowania terroryzmu w Polsce stwarza średnie zagrożenie finansowaniem terroryzmu.

W polskim prawodawstwie, podobnie jak w prawodawstwie UE, brak jest definicji legalnej dotyczącej organizacji non-profit. Organizacje non-profit są społecznymi organizacjami pozarządowymi, które prowadząc swoją działalność skupiają się na wspieraniu prywatnego lub publicznego dobra, nie kierując się osiągnięciem zysku. Odwołując się do definicji organizacji pozarządowych, zawartej w treści art. 3 ust. 2 *ustawy o działalności pożytku publicznego i o wolontariacie*, to przede wszystkim fundacje i stowarzyszenia są zaliczane do organizacji

pozarządowych[68] o charakterze non-profit i jako takie podlegają regulacjom tej ustawy, mając tym samym możliwość ubiegania się o status organizacji pożytku publicznego czy korzystania z dotacji administracji publicznej.

Uznanie działalności niezarobkowej (ang. non-profit) jako obszaru ryzyka do nadużyć na potrzeby prania pieniędzy czy finansowania terroryzmu ma związek z rekomendacjami FATF. W rekomendacji nr 8 FATF wskazała, że poszczególne kraje powinny dołożyć wszelkich starań, aby zapewnić, iż organizacje typu non-profit (NPO) nie będą wykorzystywane dla celów prania pieniędzy czy finansowania terroryzmu. Zgodnie z definicją FATF poprzez NPO należy rozumieć osobę prawną lub porozumienie prawne, lub też organizację, która zaangażowana jest przede wszystkim w gromadzenie, dystrybucję funduszy dla celów charytatywnych, religijnych, kulturalnych, edukacyjnych, społecznych lub braterskich albo też, aby realizować innego rodzaju „dobrą robotę"[69].

Fundacja zgodnie z brzmieniem *ustawy z dnia 6 kwietnia 1984 r. o fundacjach* jest to forma prawna organizacji pozarządowej, w której istotnym elementem jest kapitał przeznaczony na określony cel. Fundacja może być ustanowiona dla realizacji zgodnych z podstawowymi interesami Rzeczypospolitej Polskiej celów społecznie lub gospodarczo użytecznych, w szczególności takich, jak: ochrona zdrowia, rozwój gospodarki i nauki, oświata i wychowanie, kultura i sztuka, opieka i pomoc społeczna, ochrona środowiska oraz opieka nad zabytkami. Stowarzyszenie natomiast jest podstawową formą organizacyjno-prawną, w której realizowane jest zagwarantowane konstytucyjnie jedno z najistotniejszych praw obywatelskich – prawo wolności swobodnego zrzeszania się i podejmowania wspólnych działań. Według art. 2 ust. 1 *ustawy z 7 kwietnia 1989 r. - Prawo o stowarzyszeniach* stowarzyszenie jest „dobrowolnym, samorządnym, trwałym zrzeszeniem o celach niezarobkowych".

Organizacje non-profit działają w Europie w czterech podstawowych modelach działalności. Po pierwsze model skandynawski, w którym na 10 tys. mieszkańców wypada ponad 200 organizacji pozarządowych. Cechą skandynawskiego modelu funkcjonowania sektora[70], która najbardziej wpływa na tak duże „nasycenie" tych krajów organizacjami, jest wysoki poziom uczestnictwa w stowarzyszeniach (w zależności od źródła od 50% do nawet 90% obywateli przynależy do jakiejś organizacji). Po drugie w modelu reńskim, występującym w Niemczech oraz Belgii (a także np. Austrii). Różnica z modelem skandynawskim polega na podziale zadań między państwem a organizacjami w obszarze usług społecznych. O ile w krajach skandynawskich to państwo zajmuje się ich dostarczaniem (choć robi to w sposób bardzo zdecentralizowany), o tyle w Niemczech czy Belgii zadania publiczne z obszaru polityki społecznej realizują organizacje pozarządowe (na zasadzie kontraktowania). Odróżnia się powyższych modeli model anglosaski (funkcjonujący np. w Wielkiej Brytanii, Stanach Zjednoczonych czy Kanadzie). Od modelu reńskiego model anglosaski różni się m.in. inną

[68] Organizacjami pozarządowymi są:
1) niebędące jednostkami sektora finansów publicznych w rozumieniu *ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych* lub przedsiębiorstwami, instytutami badawczymi, bankami i spółkami prawa handlowego będącymi państwowymi lub samorządowymi osobami prawnymi,
2) niedziałające w celu osiągnięcia zysku
– osoby prawne lub jednostki organizacyjne nieposiadające osobowości prawnej, którym odrębna ustawa przyznaje zdolność prawną, w tym fundacje i stowarzyszenia, z zastrzeżeniem ust. 4.

[69] Best practices - Combating the abuse of non-profit organisations (Recommendation 8), FATF, czerwiec 2015 r., https://www.fatf-gafi.org/fr/publications/Inclusionfinanciere/Meilleures-pratiques-abus-obnl.html

[70] https://publicystyka.ngo.pl/ile-organizacji-jest-w-polsce-i-na-swiecie dostęp 28.01.2023 r.

pozycją organizacji na rynku usług społecznych. O ile w Niemczech czy Belgii są one preferowane jako wykonawcy zadań publicznych, o tyle w modelu anglosaskim muszą konkurować o środki publiczne (w formie kontraktów) lub prywatne (w formie opłaty za usługi) z biznesem. Powoduje to profesjonalizację, ale i urynkowienie organizacji. Powoduje to dużą konkurencję w sektorze. Istnieją też modele śródziemnomorskie oraz krajów Europy Środkowo-Wschodniej, w których zasady działania są mniej jasne do uchwycenia. Podlegają one zmianom i przekształceniom.

Podatność sektora

Zgodnie z treścią ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu fundacje i stowarzyszenia stają się instytucjami obowiązanymi jeżeli posiadają osobowość prawną, zostały ustanowione odpowiednio na podstawie *ustawy z dnia 6 kwietnia 1984 r. o fundacjach* oraz na podstawie *ustawy z dnia 7 kwietnia 1989 r. – Prawo o stowarzyszeniach*, a także przyjmują lub wykonują płatności gotówkowe o łącznej wartości równej lub wyższej niż 10 000 EUR, bez względu na to, czy taka płatność jest dokonywana w formie jednej operacji czy kilku operacjach, które wydają się być ze sobą powiązane. Będą również instytucjami obowiązanymi, gdy prowadzą działalność w zakresie gier losowych w rozumieniu *ustawy o grach hazardowych*, np. prowadzą charytatywne loterie fantowe, a także gdy prowadzą działalność w zakresie usługowego prowadzenia ksiąg rachunkowych.

Na podstawie danych udostępnionych przez stowarzyszenie Klon/Jawor w raporcie „2021 Kondycja organizacji pozarządowych – najważniejsze fakty" na koniec grudnia 2021 r. w Polsce było 107 tys. stowarzyszeń /bez OSP/ oraz 31 tys. fundacji. Z tego aktywnych było łącznie tylko 70 tys. stowarzyszeń i fundacji. GIIF natomiast w sprawozdaniu z realizacji *ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* w 2021 roku przekazał, że z informacji uzyskanych w trybie art. 14 ust. 4 ustawy AML/CTF od starostów, wojewodów i ministrów zidentyfikowano łącznie (wg stanu na 31 grudnia 2021 r.) 18 instytucji obowiązanych. Wśród nadzorowanych przez ww, organy instytucji obowiązanych, 9 z nich stanowiły stowarzyszenia, a 9 fundacje. Biorąc pod uwagę, że tylko jedna trzecia z podmiotów obowiązanych do przekazania informacji dotyczących stowarzyszeń i fundacji trybie art. 14 ust. 4 ustawy AML/CTF przekazała te informacje, należy stwierdzić, że ilość stowarzyszeń i fundacji będących instytucjami obowiązanymi jest w Polsce niewielka. Ponadto na podstawie przesłanych informacji 92% starostów (sprawują oni kontrolę wykonywania przez instytucje obowiązane – stowarzyszenia i fundacje - obowiązków w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu) oceniło posiadane zasoby ludzkie i finansowe jako wystarczające do realizacji zadań z zakresu przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, natomiast 8% posiadane zasoby ludzkie i finansowe oceniło jako niewystarczające. W większości starostw zadaniami związanymi z realizacją zadań z zakresu przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu zajmował się jeden bądź dwóch pracowników. W zdecydowanej większości starostw przeprowadzono w 2021 r. jedno lub dwa szkolenia z zakresu przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu.

Stowarzyszenia i fundacje, które są instytucjami obowiązanymi, powinny stosować wymienione w ustawie z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu środki bezpieczeństwa finansowego. Środki te obejmują przede wszystkim czynności związane z identyfikacją klienta oraz weryfikacją jego tożsamości;

identyfikację beneficjenta rzeczywistego oraz podejmowanie uzasadnionych czynności w celu weryfikacji jego tożsamości oraz ustalenia struktury własności i kontroli w przypadku klienta będącego osobą prawną albo jednostką organizacyjną nieposiadającą osobowości prawnej. Ponadto stowarzyszenia i fundacje będące instytucjami obowiązanymi powinny dokonywać oceny stosunków gospodarczych kontrahenta oraz (stosownie do sytuacji) uzyskiwać informacje na temat ich celu i zamierzonego charakteru. Na bieżąco też powinny monitorować stosunki gospodarcze swoich klientów. Zdecydowana większość stowarzyszeń i fundacji nie jest jednak w Polsce instytucjami obowiązanymi. Wynika to też m.in. z tego, że przeciętny roczny budżet organizacji pozarządowej w 2020 r. wyniósł 26 tys. zł. W strukturze przychodów organizacji pozarządowych w 2020 roku dominował przedział od 10 tys. do 100 tys. zł, w którym to przedziale znalazło się 36% organizacji. 23% organizacji pozarządowych w 2020 r. dysponowało budżetem w przedziale 100 tys. zł do 1 mln zł, a 6% organizacji pozarządowych w Polsce dysponowało budżetem powyżej 1 mln zł.

W praktyce swoich działań GIIF zauważył, że wśród postępowań analitycznych wszczętych przez GIIF w latach 2016-2018 stosunkowo niewielki był odsetek takich postępowań, w których zarejestrowane były podmioty ze słowami „stowarzyszenie" lub „fundacja" w nazwie (ok. 1,2 % wszystkich postępowań analitycznych). Podobny odsetek odnotowano również dla postępowań analitycznych, w których w latach 2016-2018 kierowano zawiadomienia do prokuratury i w których zarejestrowane były podmioty ze słowem „stowarzyszenie" lub „fundacja" w nazwie, w stosunku do wszystkich postępowań analitycznych, w których zawiadomienia skierowano do prokuratury w związku z podejrzeniem prania pieniędzy (tj. ok. 1,2%). Natomiast wśród wszczętych przez GIIF w latach 2019-2022 postępowań analitycznych było jedynie 6 postępowań, w których zarejestrowane były podmioty posiadające w nazwie słowa „fundacja" lub „stowarzyszenie".

Organizacje pozarządowe muszą stosować standardy przejrzystości. Organizacje powinny informować o działaniach i projektach, w których uczestniczą i które organizują. Obowiązek przejrzystości działania obejmuje informacje o tym, skąd organizacja otrzymuje finansowanie, jak działa wewnętrznie i kogo wspiera. Np. jeśli organizacja pozarządowa zakłada rachunek (konto) w banku, to zgłasza to do urzędu skarbowego na odpowiednim formularzu. Obowiązek ten dotyczy każdego kolejnego konta bankowego. Jednorazowe darowizny otrzymane od osoby fizycznej czy osoby prawnej przekraczające kwotę 15 000 zł, są zgłaszane do urzędu skarbowego na odpowiednim formularzu, a informację o tym fakcie udostępnia się do publicznej wiadomości. Natomiast jeśli suma wszystkich darowizn otrzymanych od jednej osoby prawnej bądź fizycznej przekracza 35 000 zł, organizacja pozarządowa informuje o tym urząd skarbowy na odpowiednim formularzu, a informację o tym fakcie udostępnia się do publicznej wiadomości. Organizacja pozarządowa i osoby w niej pracujące mają obowiązek rozliczania się z różnych działań, finansów, polityk i innych przedsięwzięć.

Samo finansowanie organizacji pozarządowych przybiera różne formy. Ogólne dotacje operacyjne są przeznaczane na pokrycie ogólnych wydatków bieżących i wspieranie misji organizacji, natomiast finansowanie projektowe przeznaczane jest na cele związane z konkretnym projektem. Organizacje pozarządowe mogą otrzymywać też środki z grantów. Finansowanie stowarzyszeń i fundacji może również pochodzić z darowizn, pochodzących zazwyczaj od osób fizycznych lub prawnych; dotacji; odpłatnej działalności pożytku publicznego; działalności gospodarczej; zbiórek publicznych; darowizn pieniężnych i darów rzeczowych; sponsoringu; aukcji charytatywnych. Niezależnie od źródła, fundusze

przekazywane przez darczyńców mają kluczowe znaczenie dla funkcjonowania organizacji pozarządowych i pozwalają na kontynuację pracy tych organizacji.

Duża część organizacji non-profit zajmuje się pomocą humanitarną tzn. ratowaniem i ochroną życia w czasie klęsk i katastrof spowodowanych warunkami naturalnymi lub wywołanych działalnością człowieka, a także udzielaniem koniecznej pomocy i wsparcia ludziom narażonym na długotrwałe kryzysy. Występuje tu pomoc w czasie konfliktów wojennych lub też w zakresie radzenia sobie z jego skutkami. Właśnie z powodu działania w takich trudnych warunkach społeczno-geograficznych organizacje non-profit mogą być narażone na infiltrację przez organizacje przestępcze lub terrorystyczne, które mogą ukrywać beneficjenta rzeczywistego podarowanych lub otrzymywanych środków finansowych i utrudniać śledzenie przepływów finansowych. Organizacje non-profit świadczące usługi mogą być bezpośrednio narażone zwłaszcza na finansowanie terroryzmu z uwagi na charakter działalności tych organizacji, która obejmuje finansowanie do i z obszarów objętych konfliktami lub do państw graniczących z tymi obszarami.

W przypadku instytucji obowiązanych będących stowarzyszeniami oraz fundacjami istnieje co prawda nadzór określony przepisami *ustawy z dnia 6 kwietnia 1984 r. o fundacjach* oraz *ustawy z dnia 7 kwietnia 1989 r. – Prawo o stowarzyszeniach*, sprawowany w przypadku fundacji przez ministrów i starostów, a w przypadku stowarzyszeń – przez wojewodów i starostów. Jednak powyższe przepisy prawne nie przewidują uprawnień dla ww. organów do weryfikacji sprawozdań czy dokumentów księgowych lub finansowych stowarzyszeń i fundacji w celu rozpoznania, które z nich są instytucjami obowiązanymi. Dokonanie odpowiedniego przeglądu i zaproponowanie ewentualnych zmian przepisów prawnych dotyczących stowarzyszeń i fundacji, umożliwiających właściwym organom realne działania nadzorcze nad nimi zostało przewidziane w *strategii przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu*[71].

Oceniając poziom podatności systemu przeciwdziałania praniu pieniędzy oraz finansowania terroryzmu w obszarze organizacji typu non-profit należy mieć na uwadze potencjalną możliwość infiltracji lub przejęcia przez zorganizowane grupy przestępcze tych organizacji, ewentualnie przejęcia kluczowych stanowisk w tych organizacjach, umożliwiających zarządzanie nimi. Ma to istotne znaczenie przede wszystkim z punktu widzenia możliwości finansowania terroryzmu przez te organizacje.

Sam sektor organizacji typu non-profit jest sektorem zróżnicowanym pod względem podatności na możliwość prania pieniędzy czy finansowania terroryzmu. Wynika to ze zróżnicowanej sfery działań, obejmującej m.in. sport, turystykę, rekreację i hobby, edukację czy obszar kultury i sztuki. Dużą role w podatności odgrywa też duże zróżnicowanie w formach pozyskiwania przez stowarzyszenia i fundacje środków finansowych, umożliwiających skuteczną działalność tych organizacji. Pozyskiwanie środków może się przecież odbywać w postaci wysoce zanonimizowanej np. poprzez darowizny gotówkowe czy zbiórki społeczne. Ww. podmioty posiadają pewną świadomość swoich obowiązków z zakresu AML/CTF, choć wciąż ujawniane są braki w ich wypełnianiu. Nie przekazują lub przekazują relatywnie mało informacji o podejrzanych transakcjach/podejrzanej działalności do GIIF.

[71] UCHWAŁA NR 50 RADY MINISTRÓW z dnia 19 kwietnia 2021 r. w sprawie przyjęcia strategii przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.

Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek PP w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców.

Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie.

Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.

Zagrożenia w sektorze

W sektorze organizacji non-profit pod względem oceny zagrożenia praniem pieniędzy, ale też zagrożenia finansowania terroryzmu, szczególne zagrożenie stwarzają sytuacje, gdy w działalności przedmiotowych stowarzyszeń czy fundacji występują powiązania osobowe oraz kontakty z osobami i podmiotami pochodzącymi z państw wysokiego ryzyka prania pieniędzy oraz finansowania terroryzmu. Podobnie rzecz się ma, gdy mamy do czynienia z działalnością fundacji czy stowarzyszeń zagranicznych mających siedzibę za granicą i tworzących przedstawicielstwa na terytorium Rzeczpospolitej Polskiej. W takim wypadku istnieje poważne zagrożenie, że to zagraniczne ugrupowania terrorystyczne mogą podszywać się pod legalne podmioty, jak np. fundacje oraz stowarzyszenia i pozyskiwać fundusze na cele o charakterze terrorystycznym. Mogą też występować organizacje non-profit powiązane z osobami reprezentującymi ruchy ekstremistyczne. Organizacje non-profit powiązane osobowo lub ideologicznie z osobami reprezentującymi ruchy ekstremistyczne (np. skrajnie islamistyczne, prawicowe, lewicowe) mogą wspierać podmioty lub osoby poprzez np. organizowanie zbiórek, finansowanie szkoleń paramilitarnych, czy też wydarzeń oraz materiałów propagandowych.

Inną sytuacją związaną z zagrożeniem ML i FT jest udzielanie pomocy humanitarnej na obszarach obarczonych dużym ryzykiem finansowania terroryzmu. W takim wypadku fundacje czy stowarzyszenia świadczące pomoc humanitarną na obszarach obarczonych takim dużym ryzykiem, gdzie mają miejsce konflikty zbrojne bądź aktywnie działają niepaństwowe grupy zbrojne lub terroryści – narażone są na infiltrację bądź nawet przejęcie organizacji przez organizacje terrorystyczne. Możliwe jest też służenie takiej organizacji za przykrywkę do finansowania terroryzmu.

Zagrożenie ML i FT jest stwarzane również przez fakt reprezentowania fundacji czy stowarzyszenia stowarzyszenia przez osoby zajmujące eksponowane stanowiska polityczne (ang. PEP – Politically Exposed Persons). Również zagrożenie ML i FT stwarzają powiązania osobowe członków zarządu organizacji non-profit z podmiotami prowadzącymi działalność gospodarczą, będącymi kontrahentami fundacji czy stowarzyszenia. Niepokojącym sygnałem jest również prowadzenie działalności pod adresem tzw. biura wirtualnego.

Zagrożenie stwarzają też sytuacje podjęcia przez fundację czy stowarzyszenie działalności gospodarczej niezgodnej ze statutem.

Większość organizacji non-profit korzysta z kilku źródeł finansowania (58% z nich korzysta z nie więcej niż 3 źródeł finansowania). Jednakże właśnie liczne źródła pozyskiwania funduszy umożliwiają ukrycie transferowania wartości majątkowych pochodzących z nielegalnej działalności do organizacji typu non-profit w celu ich wyprania. Na przykład środki pieniężne

uzyskane w wyniku przestępstwa, wpłacane jako darowizny podstawionych lub nieistniejących osób fizycznych lub prawnych, mogą być następnie – w legalny sposób – transferowane na rzecz konkretnych osób lub podmiotów gospodarczych, rzekomo zgodnie z celami wskazanymi w statucie organizacji.

Źródłem zagrożeń w sektorze organizacji non-profit może być wykorzystywanie sposobów gromadzenia środków pieniężnych ułatwiających ukrycie źródeł ich pochodzenia i tożsamości rzeczywistych darczyńców (np. część zbiórek publicznych, aukcji charytatywnych). Takim źródłem zagrożeń może też być wykorzystywanie przez fundacje czy stowarzyszenia nowych narzędzi technologicznych sprzyjających ukryciu źródeł ich pochodzenia, takich jak „crowdfunding" (finansowanie społecznościowe) czy „blockchain" (transakcje w walutach wirtualnych).

Niepokojący jest w każdym przypadku brak ogólnodostępnych informacji na stronach internetowych o fundacji czy stowarzyszeniu, w szczególności o zakresie działalności, przykładowych inicjatywach, sposobie wykorzystywania funduszy – zgodnych ze statutem. Dotyczy to też braku informacji na temat końcowego wykorzystania funduszy. Czerwoną flagą staje się też krótki okres funkcjonowania fundacji czy stowarzyszenia połączony z wyjątkowo wysokimi obrotami.

Potencjalne zagrożenie stwarza również uzyskanie negatywnych informacji o działalności fundacji czy stowarzyszenia, np. mogących wskazywać na wykorzystanie do popełnienia przestępstwa. Podobną sytuacje stwarza informacja np. o zawieszeniu zarządu fundacji i wyznaczenie zarządcy przymusowego lub zawieszenie w czynnościach zarządu stowarzyszenia i wyznaczenie przedstawiciela do prowadzenia bieżących spraw stowarzyszenia.

W raporcie Europolu TESAT 2022 można znaleźć informacje, że kilka krajów Bałkanów Zachodnich potwierdziło obserwowany w poprzednich latach trend, zgodnie z którym niektóre grupy ekstremistów przedstawiają się jako pozarządowe organizacje humanitarne. Jako takie organizacje pomocowe zbierają darowizny, które są następnie kierowane do zwolenników lub sympatyków radykalnych ideologii islamistycznych. W niektórych przypadkach grupy te nawiązały kontakty ze społecznościami migrantów pochodzących z Bałkanów Zachodnich w krajach UE. W przedmiotowym raporcie przedstawiono też przypadki grup terrorystycznych wykorzystujących organizacje non-profit do zbierania środków finansowych pod przykrywką zbiórek charytatywnych. W Hiszpanii trzech podejrzanych zostało aresztowanych za finansowanie terroryzmu przy użyciu takiego właśnie schematu. Pieniądze zostały zebrane przez organizację religijną pod pretekstem pomocy humanitarnej dla syryjskich sierot, ale w rzeczywistości zostały przeznaczone na finansowanie bojowników Al-Kaidy w Syrii za pośrednictwem organizacji non-profit.

Zauważono ponadto, że niektóre fundacje otwarcie zbierają fundusze dla Foreign Terrorist Fighters i ich rodzin w strefach konfliktów i obozach jenieckich w Syrii.

Na forum FATF kilka krajów zauważyło możliwości wykorzystania sektora organizacji non-profit do finansowania terroryzmu. Republika Południowej Afryki podała informację, że organizacje non-profit są wykorzystywane do generowania funduszy na cele terorystyczne. Fundusze te są następnie wykorzystywane w celu przekazania dla Państwa Islamskiego i podmiotów stowarzyszonych. Wielka Brytania odnotowała, że Państwo Islamskie zbiera

pieniądze za pośrednictwem firm-przykrywek, organizacji charytatywnych i platform internetowych. Federacja Rosyjska natomiast poinformowała, że zauważa iż w niektórych krajach często zdarzają się przypadki wykorzystywania organizacji charytatywnych i pozarządowych do pozyskiwania środków na działalność terrorystyczną prowadzoną pod pozorem realizacji programów dotyczących praw człowieka, humanitarnych i charytatywnych. Otrzymane środki są przeznaczane na promocję ideologii terrorystycznej i przyciąganie rekrutów do uzbrojonych gangów na Bliskim Wschodzie, w Europie i krajach Wspólnoty Niepodległych Państw. Charakter działalności tych organizacji ma zazwyczaj orientację religijną. Jednocześnie prawdziwy cel gromadzonych środków często nie jest ujawniany kierownictwu tych organizacji. Wśród pracowników organizacji są ekstremiści, którzy wykorzystują projekty charytatywne do znajdowania nowych bojowników i tworzenia komórek w różnych krajach świata. Działania te są prowadzone przy wysokim poziomie konspiracji.

Z uwagi na charakter swojej działalności wśród organizacji non-profit istnieje zróżnicowanie pod kątem poziomu ryzyka prania pieniędzy i finansowania terroryzmu. Duże, sformalizowane strukturalnie organizacje non-profit zajmujące się pośredniczeniem w przekazywaniu środków na cele społecznie użyteczne, mogą być infiltrowane przez organizacje przestępcze lub terrorystyczne. Organizacje te mogą ukrywać beneficjenta rzeczywistego i utrudniać śledzenie przepływów finansowych, ale ich działania są poddane środkom bezpieczeństwa finansowego w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. Takie zagrożenie prania pieniędzy i finansowania terroryzmu może być jednak obniżone poprzez sposób otrzymywania środków oraz nadzór nad ich dystrybucją ze strony darczyńcy. Np. duża część organizacji non-profit otrzymuje środki na finansowanie pomocy humanitarnej z funduszy Unii Europejskiej bądź z państw członkowskich. Środki te podlegają ścisłym ramom umownym i podlegają wysokim standardom sprawozdawczym pod kątem ich wykorzystania zgodnie z celem. Ponadto finansowanie pomocy humanitarnej UE i państw członkowskich jest przekazywane za pośrednictwem organizacji pozarządowych, które są wybierane na podstawie z góry określonych kryteriów prawnych, finansowych i operacyjnych.

Natomiast organizacje non-profit świadczące bezpośrednie usługi charytatywne (organizujące pomoc rzeczową i finansową z wykorzystaniem swoich członków) mogą być bardziej narażone na pranie pieniędzy i finansowanie terroryzmu ze względu na nieodłączny, mniej przejrzysty charakter ich działalności. Działalność ta może obejmować bezpośrednie finansowanie do i z obszarów objętych konfliktami lub do i z państw graniczących z państwami określanymi jako państwa podwyższonego ryzyka.

Na wyższe zagrożenie prania pieniędzy i finansowania terroryzmu wpływ mają sposoby finansowania organizacji non-profit. Wysokość zagrożenia jest zależna od źródeł finansowania tych organizacji, zwłaszcza gdy w grę wchodzą nieznane źródła darowizn, gotówka, źródła międzynarodowe czy też środki pochodzą z krajów wysokiego ryzyka. Wyższe zagrożenie prania pieniędzy i finansowania terroryzmu zależne jest też od sposobu dystrybucji funduszy przekazywanych na cele charytatywne, czy występuje wykorzystanie nieformalnych kanałów do przesyłania pieniędzy za granicę. Ponadto wpływ na wysokość zagrożenia prania pieniędzy i finansowania terroryzmu ma rodzaj działalności organizacji non-profit, jej profesjonalizacja oraz rodzaj i charakter beneficjentów pomocy udzielanej przez organizacje non-profit. Zagrożenie wzrasta, gdy beneficjentami pomocy są podmioty nieznane bądź mało znane, zlokalizowane zwłaszcza w krajach wysokiego ryzyka.

Od strony przedmiotowej zagrożenie prania pieniędzy i finansowania terroryzmu wzrasta, gdy organizacje non-profit działają na obszarach, które geograficznie są obarczone wysokim ryzykiem prania pieniędzy i finansowania terroryzmu. Do obszarów takich należą strefy konfliktów, gdzie toczą się działania zbrojne, gdzie obecne są niepaństwowe ugrupowania zbrojne lub osoby lub bojownicy określani jako terroryści. Działalność organizacji non-profit w obszarach państw bezpośrednio graniczących z takimi strefami konfliktu również ma wpływ na podwyższenie zagrożenia prania pieniędzy i finansowania terroryzmu.

Choć najczęściej terminu organizacja pozarządowa czy organizacja non-profit używa się w stosunku do fundacji i stowarzyszeń, to do takich organizacji zalicza się także kluby sportowe i uczniowskie kluby sportowe, organizacje działające na podstawie odrębnych przepisów takie jak Polski Czerwony Krzyż, Związek Ochotniczych Straży Pożarnych RP, Polski Związek Działkowców, koła łowieckie, komitety społeczne (np. społeczne komitety budowy dróg, wodociągów), stowarzyszenia jednostek samorządu terytorialnego, spółdzielnie socjalne, partie polityczne, związki zawodowe, samorządy zawodowe, federacje i konfederacje pracodawców, izby gospodarcze, izby rzemieślnicze, organizacje kościelne, związki rolników, kółka rolnicze i kola gospodyń wiejskich, grupy, takie jak kluby osiedlowe czy grupy wsparcia, grupy samopomocowe. Ponieważ finansowanie takich organizacji związane jest z istnieniem konkretnej potrzeby oraz na cele związane z konkretnym projektem, określonym przepisami prawa[72], zagrożenie prania pieniędzy i finansowania terroryzmu ze strony takich organizacji jest niewielkie.

W warunkach polskich nadzorująca śledztwa w sprawach terrorystycznych Prokuratura Krajowa nie prowadziła jak dotąd analiz zaangażowania organizacji pozarządowych, a w szczególności fundacji i stowarzyszeń, w przestępczość polegającą na finansowaniu terroryzmu. Jedynie w śledztwie Podlaskiego Wydziału Zamiejscowego Departamentu do Spraw Przestępczości Zorganizowanej i Korupcji Prokuratury Krajowej w Białymstoku, w którym o finansowanie terroryzmu oskarżono czterech obywateli Federacji Rosyjskiej, ujawniono, iż do przekazywania osobom prowadzącym działalność terrorystyczną wsparcia materialnego w postaci wyrobów paramilitarnych, wykorzystywano pracowników Fundacji „Ocalenie" niosącej pomoc humanitarną uchodźcom z Czeczenii. Do zaangażowania w finansowanie terroryzmu samej Fundacji jednak nie doszło.

Uśredniony poziom zagrożenia sektora organizacji typu non-profit – ML – 3,0 i FT – 2,0

Uśredniony poziom podatności sektora organizacji typu non-profit – ML – 3,0 i FT – 3,0

Oszacowany poziom prawdopodobieństwa dla sektora – ML – 3,00 i FT - 2,60

Poziom ryzyka jest ostatecznie określany przez kombinację zagrożenia i podatności. Macierz ryzyka określająca ten poziom ryzyka opiera się na wadze 40% (zagrożenie) + 60% (podatność) – przy założeniu, że komponent podatności ma większą zdolność określania poziomu ryzyka. Zakłada się, że poziom podatności może zwiększyć atrakcyjność, a tym samym zamiary przestępców/terrorystów, aby użyć danego modus operandi – wpływając w ten sposób ostatecznie na poziom zagrożenia. Poziom ryzyka sektora, z uwzględniem prawdopobieństwa

[72] np. ochotnicze straże pożarne to jednostki ochrony przeciwpożarowej będące formalnoprawnie stowarzyszeniami w rozumieniu *ustawy z dnia 7 kwietnia 1989 r. – Prawo o stowarzyszeniach*, ale będące jednocześnie jednostkami umundurowanymi, wyposażonymi w specjalistyczny sprzęt, przeznaczonymi do walki z pożarami, klęskami żywiołowymi lub innymi miejscowymi zagrożeniami, w tym prowadzącymi działania w zakresie ratownictwa specjalistycznego jednostkami ochrony przeciwpożarowej

i konsekwencji (współczynnik 2,5 dla PP i 1,5 dla FT), jest ustalany zgodnie z metodyką krajowej oceny ryzyka – aneks nr 1.

Ryzyko FT sektora organizacji typu non-profit – 2,16	
1 – 1,5	Niskie
1,6 – 2,5	Średnie
2,6 – 3,5	Wysokie
3,6 – 4	Bardzo wysokie
Ryzyko ML sektora organizacji typu non-profit – 2,80	
1 – 1,5	Niskie
1,6 – 2,5	Średnie
2,6 – 3,5	Wysokie
3,6 – 4	Bardzo wysokie

WNIOSEK 1: Poziom ryzyka wykorzystania sektora organizacji typu on-profit do finansowania terroryzmu w Polsce znajduje się na poziomie śrenim.

WNIOSEK 2: Poziom ryzyka wykorzystania sektora organizacji typu non-profit znajduje się na poziomie wysokim.

Mitygacja zidentyfikowanych ryzyk:

W celu ograniczenia prawdopodobieństwa wykorzystania sektora organizacji typu non-profit do prania pieniędzy lub finansowania terroryzmu, zasadne jest podjęcie odpowiednich działań. Stosowanie zaproponowanych działań mitygujących powinno następować z uwzględnieniem rozpoznanego przez danę instytucję obowiązaną ryzyka.

Fundacje i stowarzyszenia posiadające osobowość prawną są instytucjami obowiązanymi jedynie w zakresie, w jakim przyjmują lub dokonują płatności w gotówce o wartości równej lub przekraczającej równowartość 10 tys. EUR, bez względu na to, czy płatność jest przeprowadzana jako pojedyncza operacja, czy kilka operacji, które wydają się ze sobą powiązane. Czynnikiem ograniczającym ryzyko związane z działalnością organizacji typu non-profit są uprawnienia kontrolne dotyczące obowiązków związanych z przeciwdziałaniem praniu pieniędzy oraz finansowaniu terroryzmu, niemniej jako konieczne jest usprawnienie procedur, celem zapewnienia sprawnej wymiany informacji na temat organizacji typu non-profit, które w danym okresie wypełniają ustawową przesłankę uznania za instytucję obowiązaną.

W sektorze organizacji typu non-profit powinny być podejmowane działania podnoszące świadomość narażenia na przestępstwo prania pieniędzy oraz finansowania terroryzmu, jak również podnoszące poziom wyszkolenia pracowników takich organizacji w analizie sygnałów ostrzegawczych wynikających z transakcji podejrzanych.

Instytucje obowiązane z sektora organizacji typu non-profit powinny zwracać szczególną uwagę na transfery środków na rzecz beneficjentów organizacji z jurysdykcji charakteryzujących się wyższym ryzykiem prania pieniędzy oraz finansowania terroryzmu. Instytucje obowiązane z sektora organizacji typu non-profit powinny położyć szczególny nacisk na uzyskanie informacji na temat celu i zamierzonego charakteru stosunków łączących organizację typu non-profit z beneficjentem środków gromadzonych poprzez taką organizację. Istotnym zagrożeniem w obszarze organizacji typu non-profit jest możliwość infiltracji lub przejęcia przez zorganizowane grupy przestępcze tych organizacji, ewentualnie przejęcia kluczowych stanowisk w tych organizacjach, umożliwiających zarządzanie nimi. Instytucje obowiązane powinny zwracać uwagę na aktualizację informacji o klientach z obszaru organizacji typu non-profit, celem wychwytywania zmiany sposobu funkcjonowania organizacji typu non-profit, w związku z potencjalnym przejęciem zarządzania organizacją przez osoby zamierzające wykorzystać taką organizację do prania pieniędzy lub finansowania terroryzmu.

Z uwagi na brak ogólnodostępnych poprzez sieć internet informacji o fundacji czy stowarzyszeniu, w szczególności o zakresie działalności, przykładowych inicjatywach czy też wskazanych w statucie sposobów wykorzystywania funduszy, instytucje obowiązane nawiązujące relacje z podmiotem z sektora organizacji non-profit, powinny zwracać szczególną uwagę na pozyskanie odpowiednich, aktualnych informacji o kliencie. Czynnikami mogącymi wskazywać na próbę wykorzystania organizacji typu non-profit do działalności przestępczej powinny być w szczególności:

- sytuacje podjęcia przez fundację czy stowarzyszenie działalności gospodarczej niezgodnej ze statutem;
- powiązania osobowe członków zarządu organizacji non-profit z podmiotami prowadzącymi działalność gospodarczą, będącymi kontrahentami fundacji czy stowarzyszenia;
- prowadzenie działalności pod adresem tzw. biura wirtualnego;
- krótki okres funkcjonowania fundacji czy stowarzyszenia połączony z wyjątkowo wysokimi obrotami.

11. Finansowanie społecznościowe

Opis sektora – zawarty jest w podrozdziale 7.2.2 - „Podatność rynku pozainansowego".

Scenariusze wystąpienia ryzyka obejmują możliwość wykorzystania platformy crowdfundingowej do finansowania działalności nielegalnej.

Pranie pieniędzy

Tabela 49

Rodzaj wykorzystanych usług, produktów finansowych	Finansowanie społecznościowe (crowdfunding)
Ogólny opis ryzyka	Organizowanie akcji crowdfundingowej w celu legitymizowania posiadanych lub przekazywanych środków pieniężnych
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Zorganizowanie akcji gromadzenia funduszy na przykład na uruchomienie legalnej działalności gospodarczej poprzez platformę crowdfundigową. Środki, pochodzące z działalności przestępczej są przekazywane przez podstawione lub fikcyjne osoby fizyczne jednorazowo w relatywnie niewielkich kwotach. 2. Wykorzystywanie platform crowdfundingowych do gromadzenia środków pochodzących z nieuprawnionego użycia kart płatniczych i wypłacanie ich/transferowanie na kolejne rachunki bankowe.
Poziom podatności	4
Uzasadnienie dla poziomu podatności	Relatywnie łatwe jest rozpoczęcie akcji crowdfundingowej, np. za pośrednictwem mediów społecznościowych. Łatwe jest ukrycie danych identyfikacyjnych darczyńców i beneficjentów. Istnieje możliwość realizacji transakcji o charakterze międzynarodowym. Teoretycznie każdy może prowadzić akcję crowdfundingową. Podmioty prowadzące takie akcje nie są IO. Jednakże w wypadku przedsięwzięć gospodarczych obowiązują od listopada 2021 r. nowe przepisy zawarte w *ustawie o finansowaniu społecznościowym*. Pojawił się w takim wypadku obowiązek posiadania licencji przez platformy zajmujące się crowdfundingiem oraz ich bieżący nadzór przez Komisję Nadzoru Finansowego. Zwiększa się także limit kwoty, którą można uzyskać poprzez taką formę finansowania – z 1 mln do 5 mln EURO. Organy administracji publicznej posiadają podstawową wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma ograniczone możliwości gromadzenia i analizowania informacji dot. tego typu akcji. Istnieje prawdopodobieństwo, że przypadek prania pieniędzy w zakresie analizowanego scenariusza nie zostanie wykryty. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne nie odpowiadają zakresowi analizowanego ryzyka.
Poziom zagrożenia	2
Uzasadnienie dla poziomu zagrożenia	Finansowanie społecznościowe stanowi alternatywne źródła finansowania. Jest formą finansowania różnego rodzaju projektów przez społeczność, która jest lub zostanie wokół tych projektów zorganizowana. Pranie pieniędzy, w przypadku np. zorganizowanych grup przestępczych, stanowi rodzaj przedsięwzięcia i w tym przypadku jest ono finansowane poprzez dużą liczbę drobnych, jednorazowych wpłat dokonywanych przez osoby które uczestniczą w procederze prania pieniędzy. Zazwyczaj jednak cel zbiórki pieniędzy nie jest przedstawiany wprost. Crowdfunding środków niewiele kosztuje i jako *modus operandi* może być postrzegany przez sprawców jako w miarę atrakcyjny i szeroko dostępny sposób w zakresie prania pieniędzy, jednakże okupione jest to sporym ryzykiem. Z reguły akcja zbierania środków trwa jakiś czas, więc crowdfunding jest stosunkowo łatwy do namierzenia i może nie przynieść spodziewanych rezultatów, co wpływa na postrzeganie tej metody jako stosunkowo mało atrakcyjnej. Zorganizowanie akcji crowdfundingowej środków może być związane z pewnymi kosztami (pośrednictwo platformy crowdfundignowej jest związane z prowizją sięgającą czasami kilku procent, zwykle od zebranych środków). Ponadto wymaga odpowiedniego planowania i wiedzy, a także czasu na jej przeprowadzenie. GIIF

	otrzymywał bardzo nieliczne informacje o możliwości wykorzystania tej metody do prania pieniędzy. WNIOSEK: Wykorzystanie mechanizmu crowdfundingu stwarza średnie zagrożenie prania pieniędzy.

Finansowanie terroryzmu

Tabela 50

Rodzaj wykorzystanych usług, produktów finansowych	Finansowanie społecznościowe
Ogólny opis ryzyka	Pozyskiwanie darczyńców środków na rzecz organizacji terrorystycznych przy wykorzystaniu nowoczesnych sieci komunikacyjnych
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Organizowanie akcji poprzez platformę *crowdfundigową* w celu zbiórki środków na potrzeby działalności o charakterze terrorystycznym. Rzeczywisty cel zbiórki funduszy nie będzie bezpośrednio wskazywał na zamiar wykorzystania zgromadzonych środków do finansowania terroryzmu. 2. Zwolennicy organizacji terrorystycznej rozsyłają apele o fundusze poprzez media społecznościowe. Darczyńcy przekazują inicjatorom akcji datki w gotówce, walutach wirtualnych lub kupują międzynarodowe karty przedpłacone, których numery następnie im udostępniają. 3. Zbiórka funduszy oparta na przedsprzedaży np. książki - w tym modelu zbierane są środki na wydanie ważnego dzieła literackiego czy realizację poszczególnych etapów jego stworzenia. Wpłacający zdają sobie sprawę, że prawdziwym odbiorcą środków jest organizacja terrorystyczna.
Poziom podatności	4
Uzasadnienie dla poziomu podatności	Relatywnie łatwe jest rozpoczęcie akcji crowdfundingowej, np. za pośrednictwem mediów społecznościowych. Łatwe jest ukrycie danych identyfikacyjnych darczyńców i beneficjentów. Istnieje możliwość realizacji transakcji o charakterze międzynarodowym. Teoretycznie każdy może prowadzić akcję crowdfundingową. Podmioty prowadzące takie akcje nie są IO. Jednakże w wypadku przedsięwzięć gospodarczych obowiązują od listopada 2021 r. nowe przepisy zawarte w *ustawie o finansowaniu społecznościowym*. Pojawił się w takim wypadku obowiązek posiadania licencji przez platformy zajmujące się crowdfundingiem oraz ich bieżący nadzór przez Komisję Nadzoru Finansowego. Zwiększa się także limit kwoty, którą można uzyskać poprzez taką formę finansowania – z 1 mln do 5 mln EURO. Organy administracji publicznej posiadają podstawową wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma ograniczone możliwości gromadzenia i analizowania informacji dot. tego typu akcji. Istnieje prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy nie zostanie wykryty. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne nie odpowiadają zakresowi analizowanego ryzyka.
Poziom zagrożenia	2

Uzasadnienie dla poziomu zagrożenia	Finansowanie społecznościowe stanowi alternatywne źródła finansowania, również dla działalności terrorystycznej. Jest formą finansowania różnego rodzaju projektów przez społeczność, która jest lub zostanie wokół tych projektów zorganizowana. Działalność terrorystyczna jako pewnego rodzaju przedsięwzięcie jest w takim przypadku finansowane poprzez dużą liczbę drobnych, jednorazowych wpłat dokonywanych przez osoby zainteresowane wspieraniem działalności terrorystycznej. Zazwyczaj jednak cel zbiórki pieniędzy nie jest przedstawiany wprost. Crowdfunding środków niewiele kosztuje i jako *modus operandi* może być postrzegany przez sprawców jako w miarę atrakcyjny i szeroko dostępny sposób dla finansowania terroryzmu, jednakże okupione jest to sporym ryzykiem. Z reguły akcja zbierania środków trwa jakiś czas, więc crowdfunding jest stosunkowo łatwy do namierzenia i może nie przynieść spodziewanych rezultatów, co wpływa na postrzeganie tej metody jako stosunkowo mało atrakcyjnej. GIIF otrzymywał bardzo nieliczne informacje o możliwości wykorzystania tej metody do finansowania działalności terrorystycznej. WNIOSEK: Wykorzystanie mechanizmu crowdfundingu stwarza średnie zagrożenie finansowaniem terroryzmu.

Szczególnie istotnym zagrożeniem jest możliwość wykorzystania tej formy finansowania do wspierania działalności terrorystycznej. Organizacjom ekstremistycznym łatwo jest używać wszelkich rodzajów zbiórek na cele charytatywne ponieważ prowadzą działalność polityczną i odwołują się do uczuć swoich zwolenników, którzy identyfikują się z postulatami danej organizacji. Środki mogą być gromadzone na fałszywie opisane cele, których faktyczne znaczenie znają tylko wtajemniczeni lub być gromadzone pod chwytliwym w danej społeczności celem, a następnie wykorzystane w dowolny sposób. Przedmiotem wsparcia mogą być pomoc faktycznym osobom np. poszkodowanym w trakcie walk, którzy faktycznie są rannymi bojownikami. Może się to również wyrażać zbiórką na projekt, który jest formą budowania infrastruktury organizacji terrorystycznej. Nadzór nad faktycznym wykorzystaniem środków pozostaje pod kontrolą bojowników. Łatwo jest również rozpropagować fakt istnienia zbiórki wśród zwolenników.

Użycie platformy crowdfundingowej jest mniej prawdopodobne w przypadku prania pieniędzy pochodzących z przestępstwa. Pomimo tego możliwy jest scenariusz, w którym grupa przestępcza zakłada fałszywą zbiórkę dla legalizowania pieniędzy pochodzących z nielegalnej działalności. Scenariusz taki wymaga zorganizowania grupy podmiotów, których dane byłyby wiarygodne oraz przekazanie ich w sposób dający pozory uczciwych transakcji. Zalegalizowane w ten sposób środki mogą być później użyte przez grupę do finansowania swojej działalności lub wypłaty zysku swoim członkom. Wypłata środków z konta przeznaczonego na zbiórkę może nastąpić na rzecz legalnie istniejących podmiotów, czy też w celu sfinansowania zgodnego z prawem projektu, kontrolowanego przez przestępców. Ten sposób finansowania może zostać użyty również przez osoby działające jako pośrednicy lub świadczący usługi prania pieniędzy dla innych podmiotów.

Podatność

29 lipca 2022 r. weszły w życie przepisy *ustawy z 7 lipca 2022 r. o finansowaniu społecznościowym i pomocy kredytobiorcom*. Akt ten zaimplementował do polskiego systemu prawnego zapisy rozporządzenia Parlamentu Europejskiego i Rady UE 2020/1503 wprowadzającego regulacje systemu na poziomie unijnym. Ustawa reguluje kwestie związane z wewnętrzna organizacją i działalnością platform. Akt prawny wskazał, że zgody na

świadczenie usług crowdfundingu udziałowego udziela KNF. Z powyższego wynika, że Komisja posiada uprawnienia do nadzoru i kontroli działalności danego podmiotu w tym zakresie. Limit kwoty zebranej bez przedstawienia prospektu emisyjnego został ustalony na równowartość 5 000 000 EUR, pod warunkiem korzystania z platformy zarejestrowanej przez KNF[73]. W zbiórce zastosować można różne formy środków płatniczych. KNF ostrzega o zagrożeniach płynących z inwestowania w tej formie[74].

Platformy crowdfundingowe działają w przestrzeni wirtualnej. Co za tym idzie znaczna ich część jest zarejestrowana poza terytorium kraju. Ogranicza to możliwość pełnej kontroli działalności podmiotów świadczących takie usługi oraz samego procesu zbiórki.

Użycie platformy crowdfundingowej wymaga odpowiedniego planowania oraz przygotowania. Konieczne jest odpowiednie przedstawienie przedmiotu zbiórki, który musi być na tyle wiarygodny by nie wzbudzać podejrzeń. Konieczne jest również istnienie odpowiedniej grupy ofiarodawców dokonujących wpłat, lub zasymulowanie ich istnienia. Sam proces zbiórki wymaga dokonania znacznej ilości niewielkich wpłat. Pomimo tych trudności odpowiednio zdeterminowana grupa przestępcza lub terrorystyczna jest w stanie zorganizować.

Zagrożenia w sektorze

Większość wpłat na platformach crowdfundingowych dotyczy niewielkich kwot, przez co nie wzbudza podejrzeń organów kontroli. Sukces zbiórki zależy w tym wypadku od istnienia odpowiedniej grupy osób wspierających, których można zmobilizować do wsparcia, na bazie uczuć religijnych lub poglądów politycznych. Łatwe jest przy tym zachowanie anonimowości darczyńców, którzy mają najczęściej szerokie spektrum kanałów wsparcia od płatności elektronicznych, przekazów za pomocą usług telekomunikacyjnych, aż po specyficzne rozwiązania takie jak automaty do wpłacania datków[75].

Przeprowadzenie zbiórki w celach przestępczych jest szczególnie łatwe dla organizacji ekstremistycznych odwołujących się do emocji i postaw etycznych swoich zwolenników. Łatwiejsze jest w takich okolicznościach zmobilizowanie szeregu realnie istniejących, a przez to nie wzbudzających podejrzeń osób do wspomożenia celów organizacji. Jednocześnie, z uwagi na znajomość społeczności do której dana organizacja kieruje swój przekaz temat założonej zbiórki może być dobrze sprofilowany. W przypadku wcześniejszego istnienia kanałów komunikacji ze zwolennikami dużo szybciej można rozpropagować fakt rozpoczęcia gromadzenia środków. Jednocześnie gromadząc grupę realnie istniejących osób można liczyć na różnorodność w sposobie działania osób wspierających, które mogą przekazywać środki różnymi dostępnymi sobie środkami dodatkowo utrudniając rozpoznanie źródeł pochodzenia przekazanych środków.

Przeprowadzenie zbiórki jest ułatwione w tych środowiskach, w których istnieje kultura udzielania pomocy charytatywnej. Tradycje takie jak muzułmański zakat zwiększają zasób środków, które mogą zostać przekazane w ramach crowdfundingu. Potencjalni darczyńcy mogą uznać, że przekazanie datku na określony cel wypełnia ich potrzeby etyczno-moralne. Powiększa to ilość potencjalnych ofiarodawców poza krąg popierających idee ekstremistyczne o osoby o umiarkowanych poglądach, które mogą wesprzeć dany cel z powodów etycznych,

[73] *Ustawa z dnia 7 lipca 2022 r. o finansowaniu społecznościowym dla przedsięwzięć gospodarczych i pomocy kredytobiorcom*,
[74] https://www.knf.gov.pl/dla_rynku/crowdfunding/inwestorzy, dostęp: 27.12.2022 r.,
[75] How Card Payment Machines Can Help Charities (paymentplus.ie), dostęp: 27.12.2022 r.,

nie mając świadomości, że wspierają grupę terrorystyczną. Założyć można, że faktycznie większość gromadzonych środków może pochodzić od osób, których celem nie jest wspierania działań bojowych.

W mediach pojawiały się informacje o gromadzeniu środków na cele humanitarne, które przekazywane były dla wsparcia działalności grup terrorystycznych. W sprawie ujawnionej w Niemczech w 2022 r. środki zgromadzone za pomocą crowdfundingu jako wsparcie dla rodzin bojowników internowanych w obozie al-Hol w Syrii. Stwierdzono, że część pieniędzy użyto do wywiezienia niektórych osadzonych osób i przekazania ich do obozów szkoleniowych ISIS i innych organizacji terrorystycznych[76]. Zdarzenia takie wyraźnie wskazują, że wsparcie nawet usprawiedliwionych etycznie celów może prowadzić do finansowania działalności ekstremistycznej, gdyż ofiarodawcy nie mają możliwości zweryfikowania sposobu rozdysponowania zgromadzonych środków. Od prowadzącego zbiórkę najczęściej nie wymaga się szczegółowego rozliczenia, a sposób ich faktycznego wykorzystania jest łatwy do ukrycia.

Z uwagi na mechanizm działania użycie metod finansowania społecznościowego do prania pieniędzy ma inny charakter. W takim przypadku konieczne jest zorganizowanie odpowiedniej ilości wiarygodnych podmiotów, które posłużyły by do przekazania środków, a następnie dokonanie wpłat za ich pośrednictwem. Nie istnieje wcześniejsze zaplecze społeczne, przy pomocy którego można w łatwy sposób przeprowadzić proces prania, a działalność prowadzona w takich warunkach nie może oprzeć się na szerokim gronie faktycznie istniejących osób, które w tym przypadku muszą działać w jakimś stopniu świadomie. Przestępcy działając cynicznie i z rozmysłem nie mogą również liczyć na zaangażowanie z powodów etycznych i moralnych.

Najczęściej crowdfunding jest wykorzystywany jako mechanizm przestępstwa bazowego[77]. Darczyńcy często nie weryfikują faktycznego celu zbiórki, prawdziwości intencji prowadzącego zbiórkę czy wręcz faktycznego istnienia osób (podmiotów) potrzebujących. Możliwe jest także podszywanie się pod faktycznie istniejące osoby, przy nieautoryzowanym użyciu prawdziwych dokumentów i danych[78]. Jeżeli portal crowdfundingowy posiada swój system weryfikacji zbiórek, kontroli podlega wyłącznie proces gromadzenia środków w systemie. Portal pozostaje pośrednikiem pomiędzy darczyńcami a beneficjentem. Środki ostatecznie przekazane na konto organizatora zbiórki przechodzą na jego własność i mogą być dowolnie wykorzystane.

Finansowanie społecznościowe zakłada wspieranie danego projektu przez szereg niewielkich podmiotów, wspierających zbiórkę niewielkimi kwotami. Sam proces zbiórki przeprowadzanej za pomocą platformy crowdfundingowej może być skuteczny w odniesieniu do tych środków, które pochodzą z przestępstw nie angażujących znacznych kwot. Jest to wygodny sposób dla prania środków pochodzących z przestępstw elektronicznych, ponieważ cały proces przesyłania pieniędzy odbywa się wtedy w cyberprzestrzeni. Ważną zaletą dla sprawców jest fakt, że przelew przychodzący na ich rachunek pochodzi od platformy crowdfundingowej, czyli podmiotu najczęściej posiadającego rozpoznawalną markę i pozostającego poza podejrzeniem.

[76] Crowdfunding the 'Islamic State' group – DW – 09/10/2022, dostęp: 27.12.2022 r.,
[77] Bezpieczeństwo w firmie Najpopularniejsze oszustwa na (politykabezpieczenstwa.pl); dostęp: 09.03.2023 r.,
[78] Żył z fałszywych zbiórek. Policja zatrzymała oszusta - Money.pl; dostęp: 09.03.2023 r.

Crowdfunding jest stosunkowo nowym narzędziem finansowania co za tym idzie znaczna część działalności platform crowdfundingowych pozostaje nieuregulowana. Dotyczy to w szczególności finansowania projektów o charakterze filantropijnym, pomocowym. W opisie zagrożeń związanych z rynkiem zauważ się brak jasnych procedur przeciwdziałania AML/CTF nawet u największych dostawców usług tego typu[79]. Niewątpliwie brak jasnych regulacji oraz znaczna elastyczność działalności powoduje, że finansowanie społecznościowe jest atrakcyjnym sposobem działania dla niektórych rodzajów przestępców oraz grup ekstremistycznych. Sprzyja temu znaczny rozwój tego sektora w ostatnich latach, powodujący zwiększenie zasobu podmiotów uczestniczących w rynku oraz zwiększenie ilości obecnych na nim środków[80].

Uśredniony poziom zagrożenia sektora finansowania społecznościowego – ML – 2,0 i FT – 2,0

Uśredniony poziom podatności sektora finansowania społecznościowego – ML – 4,0 i FT – 4,0

Oszacowany poziom prawdopodobieństwa dla sektora – ML – 3,20 i FT - 3,20

Poziom ryzyka jest ostatecznie określany przez kombinację zagrożenia i podatności. Macierz ryzyka określająca ten poziom ryzyka opiera się na wadze 40% (zagrożenie) + 60% (podatność) – przy założeniu, że komponent podatności ma większą zdolność określania poziomu ryzyka. Zakłada się, że poziom podatności może zwiększyć atrakcyjność, a tym samym zamiary przestępców/terrorystów, aby użyć danego modus operandi – wpływając w ten sposób ostatecznie na poziom zagrożenia. Poziom ryzyka sektora, z uwzględniem prawdopobieństwa i konsekwencji (współczynnik 2,5 dla PP i 1,5 dla FT), jest ustalany zgodnie z metodyką krajowej oceny ryzyka – aneks nr 1.

Ryzyko FT sektora finansowania społecznościowego – 2,52	
1 – 1,5	Niskie
1,6 – 2,5	Średnie
2,6 – 3,5	Wysokie
3,6 – 4	Bardzo wysokie
Ryzyko ML sektora finansowania społecznościowego – 2,92	
1 – 1,5	Niskie
1,6 – 2,5	Średnie
2,6 – 3,5	Wysokie
3,6 – 4	Bardzo wysokie

WNIOSEK 1: Poziom ryzyka wykorzystania finansowania społecznościowego do finansowania terroryzmu w Polsce znajduje się na poziomie średnim.

WNIOSEK 2: Poziom ryzyka wykorzystania finansowania społecznościowego do prania pieniędzy w Polsce znajduje się na poziomie wysokim.

Mitygacja zidentyfikowanych ryzyk:

W celu ograniczenia prawdopodobieństwa wykorzystania finansowania społecznościowego do prania pieniędzy lub finansowania terroryzmu, zasadne jest podjęcie

[79] Crowdfunding: A Criminal's Hiding Place? (linkedin.com), dostęp: 28.12.2022 r.,
[80] Crowdfunding: Fraud and Money Laundering Risks - Sanction Scanner, dostęp: 28.12.2022 r.,

odpowiednich działań. Stosowanie zaproponowanych działań mitygujących powinno następować z uwzględnieniem rozpoznanego przez danę instytucję obowiązaną ryzyka.

Instytucje obowiązane których działalność obejmuje rówież finansowanie społecznościowe, a także instytucje obowiązane, których klientami są podmioty zajmujące się finansowaniem społecznościowym, powinny zwracać szczególną uwagę na transfery środków z lub do jurysdykcji charakteryzujących się wyższym ryzykiem prania pieniędzy oraz finansowania terroryzmu.

Instytucje obowiązane których działalność obejmuje rówież finansowanie społecznościowe, powinny położyć szczególny nacisk na uzyskanie informacji na temat celu i zamierzonego charakteru stosunków łączących klienta z beneficjentem środków gromadzonych poprzez finansowanie społecznościowe. Instytucje obowiązane, których klientami są podmioty zajmujące się finansowaniem społecznościowym, powinny położyć szczególny nacisk na uzyskanie od klienta informacji na temat celu i zamierzonego charakteru stosunków łączących klienta z beneficjentem środków gromadzonych poprzez finansowanie społecznościowe.

Instytucje obowiązane których działalność obejmuje rówież finansowanie społecznościowe, oraz instytucje obowiązane, których klienci zajmują się finansowaniem społecznościowym, powinny zwracać uwagę na przeprowadzane transfery środków na rachunki niezwiązane z beneficjentem zbiórki, na transfery środków do państw trzecich, czy też na przypadki dokonywania na rachunek danej zbiórki dużej ilości wpłat w krótkim czasie, jak również na wpłaty o nienormatywnie dużej wartości, w szczególności z obcych jurysdykcji.

Instytucje obowiązane, których działalność obejmuje rówież finansowanie społecznościowe, oraz instytucje obowiązane, których klientami są podmioty zajmujące się finansowaniem społecznościowym, powinny na bieżąco monitorować stosunki gospodarcze i w uzasadnionych sytuacjach występować do klienta o przekazanie informacji i dokumentów dotyczących wpłat dokonywanych na daną zbiórkę, czy też beneficjentów organizowanych zbiórek. Informacje dostępne w otwartych źródłach (w szczególności w internecie), dotyczące przeznaczenia zbiórki czy też zawierające opis beneficjenta zbiórki, mogą nie być prawdziwe. W tym zakresie wprowadzające w błąd informacje mogą pochodzić od organizatora zbiórki, albo bezpośrednio od osoby lub podmiotu, na rzecz którego zbiórka jest organizowana. W związku z tym instytucje obowiązane, których działalność obejmuje rówież finansowanie społecznościowe, oraz instytucje obowiązane, nawiązujące relacje z podmiotem z sektora finansowania społecznościowego, powinny zwracać szczególną uwagę na pozyskanie odpowiednich, aktualnych informacji o kliencie, źródle pochodzenia wartości majątkowych, a w trakcie stosunków gospodarczych również o transakcjach przeprowadzanych na rzecz klienta (realizowanych na rzecz danego podmiotu wpłatach).

12. Handel dobrami o wysokiej wartości

Opis sektora – zawarty jest w podrozdziale 2.2 – „Rynek pozafinansowy" oraz w podrozdziale 7.2.2 - „Podatność rynku pozafinansowego".

Scenariusze wystąpienia ryzyka obejmują możliwość pozyskiwania środków dla sfinansowania działalności nielegalnej z obrotu towarami o wysokiej wartości tj. złotem, kamieniami szlachetnymi, antykami, dziełami sztuki itp. Mogą również zakładać użycie takich dóbr do lokowania środków pochodzących z przestępstwa. Przedmiotowa okoliczność dotyczyć przede wszystkim zakupu towarów luksusowych, antyków, dzieł sztuki i towarów służących lokacji kapitału np. metali lokacyjnych, kamieni szlachetnych. Dobra mogą być nabywane zarówno za gotówkę jak również inne środki płatnicze lub w ramach handlu wymiennego. Scenariusz zakłada również wprowadzenia do obrotu dóbr uzyskanych w drodze kradzieży lub paserstwa. Stają się one w takim przypadku źródłem przychodu przestępcy lub grupy przestępczej.

W przypadku finansowania terroryzmu scenariusz zakłada możliwość przywozu na teren kraju dóbr wysokiej wartości w celu ich sprzedaży lub tranzytu. Może to dotyczyć dóbr kultury zrabowanych właścicielom, zdobytych nielegalnie lub wyprowadzanych z majątku innego państwa, pozyskanych na terenach objętych walkami metali i kamieni szlachetnych itp.

Pranie pieniędzy

Tabela 51

Rodzaj wykorzystanych usług, produktów finansowych	Kamienie i metale szlachetne
Ogólny opis ryzyka	Inwestowanie środków pochodzących z nielegalnych źródeł w zakup metali i kamieni szlachetnych
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Przestępcy kupują sztabki złota, złote monety, diamenty i inne wartościowe kamienie w celu przewiezienia przez granicę (kurierem lub przy wykorzystaniu przesyłek pocztowych i przewozów cargo) i sprzedania w krajach charakteryzujących się mniejszą kontrolą obrotu finansowego. Pieniądze ze sprzedaży są następnie inwestowane w legalnie działające przedsięwzięcia lub wprowadzane do systemu bankowego. 2. Przestępcy kupują sztabki złota, złote monety, diamenty i inne wartościowe kamienie w innych krajach za wytransferowane środki pochodzące z nielegalnych źródeł. Zakupiony towar jest potem sprzedawany w Polsce lub w krajach trzecich na podstawie fałszywych faktur i certyfikatów pochodzenia. 3. Przestępcy kupują biżuterię ze złota i srebra, a następnie odsprzedają niniejsze przedmioty firmom z krajów trzecich, które zajmują się tzw. przetwórstwem metali szlachetnych.
Poziom podatności	3
Uzasadnienie dla poziomu podatności	O ile kupno i sprzedaż relatywnie niewielkich ilości tego typu towarów nie nastręcza większej trudności (np. w sklepach jubilerskich), to kupno/sprzedaż ich dużych/hurtowych ilości już tak. Łatwo jest jednak uniknąć identyfikacji, zwłaszcza przy zakupie/sprzedaży towarów o wartości poniżej równowartości 15 tys. EUR. Istnieje możliwość kupowania/sprzedawania przez Internet, a tym samym realizowania transakcji o charakterze międzynarodowym (np. przy zakupie kamieni lub metali od podmiotu zagranicznego). Obecnie podmioty prowadzące działalność w zakresie obrotu metalami lub kamieniami szlachetnymi i półszlachetnymi nie są IO, o ile nie przyjmują lub dokonują płatności za towary w gotówce o wartości równej lub przekraczającej równowartość 10 tys. EUR, bez względu na to, czy transakcja jest przeprowadzana jako pojedyncza operacja, czy kilka operacji, które wydają się ze sobą powiązane lub o ile nie prowadzą działalności kantorowej w zakresie kupna i sprzedaży złota dewizowego i platyny dewizowej. W Polsce istnieje możliwość zakupu złota w formie sztabek, a także złotych monet – tzw. monet bulionowych (bez wartości numizmatycznych). Oprócz tego monety bulionowe traktowane są jako legalny środek płatniczy, co zapewnia możliwość przewiezienia monet z kraju do kraju. Ponadto import, przetwarzanie oraz obrót diamentami nie jest działalnością reglamentowaną prawnie, co oznacza, że nie trzeba mieć na nią ani zezwolenia, ani koncesji, ani żadnej innej decyzji organu administracji publicznej. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek prania pieniędzy w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	3

Uzasadnienie dla poziomu zagrożenia	Wykorzystanie mechanizmu inwestowania środków pochodzących z nielegalnych źródeł w zakup metali i kamieni szlachetnych jest jedną z najczęściej spotykanych metod prania pieniędzy. Z uwagi na stabilną wartość kruszców i kamieni, łatwość ich przemieszczania (nawet za granicę) oraz niewielką stosunkowo objętość powodującą łatwość ich ukrycia, metoda ta jest stosunkowo często stosowana. Jest to sposób szeroko dostępny, jego zastosowanie stosunkowo niewiele kosztuje i jest postrzegany przez sprawców raczej jako atrakcyjny. Wykorzystanie mechanizmu inwestowania środków pochodzących z nielegalnych źródeł w zakup metali i kamieni szlachetnych nie wymaga wysokospecjalistycznej wiedzy ani specjalistycznych umiejętności. Metoda wykorzystywana często przez zorganizowaną przestępczość, wiąże się czasem z korupcją, ponieważ w niektórych przypadkach wymaga sporządzenia fałszywych certyfikatów lub innej dokumentacji. GIIF otrzymywał informacje o wykorzystywaniu teju metody do prania pieniędzy. WNIOSEK: Wykorzystanie mechanizmu inwestowania środków pochodzących z nielegalnych źródeł w zakup metali i kamieni szlachetnych stwarza wysokie zagrożenie prania pieniędzy.

Tabela 52

Rodzaj wykorzystanych usług, produktów finansowych	Antyki oraz dzieła sztuki
Ogólny opis ryzyka	Inwestowanie środków pochodzących z nielegalnych źródeł w zakup antyków i dzieł sztuki
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Przestępcy kupują za środki pochodzące z nielegalnych źródeł antyki i dzieła sztuki, które przechowują traktując je jako rodzaj inwestycji lub przewożą za granicę w celu sprzedaży. 2. Użycie przez przestępców tzw. NTF[81] (np. wirtualnych dzieł sztuki), czyli niewymienialnych tokenów (ang. *non-fungible token)* w celu wprowadzania do obrotu gospodarczego środków pieniężnych pochodzących z nielegalnych źródeł, np. zorganizowana grupa przestępcza tworzy NFT w celu jego odsprzedaży osobom również powiązanym z ww. grupą. Transakcja realizowana jest *on-line*.
Poziom podatności	3
Uzasadnienie dla poziomu podatności	Kupno/sprzedaż antyków czy dzieł sztuki jest relatywnie łatwe. Istnieje wiele firm handlujących tego typu towarami, na podstawie przepisów *ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców* (domy aukcyjne, antykwariaty). Istnieje możliwość kupowania/sprzedawania przez Internet, a tym samym realizowania transakcji o charakterze międzynarodowym. Istotnym instrumentem, który rozszerzył spektrum kupna/sprzedaży dzieł sztuki na rynku, także międzynarodowym są tokeny NFT. Obecnie funkcjonowanie tzw. *non-fungible tokens* nie jest uregulowane (organy UE prowadzą działania w celu dostosowania regulacji prawnych do powstałego instrumentu bazującego na technologii blockchain). Subiektywna wartość tokenów NFT oraz brak kontroli nad tym instrumentem tworzy pole do nadużyć w tym zakresie. Obecnie przedsiębiorcy prowadzący działalność polegającą na obrocie lub pośrednictwie w obrocie dziełami sztuki, przedmiotami kolekcjonerskimi oraz antykami oraz prowadzący działalność polegającą na przechowywaniu dzieł sztuki, przedmiotów kolekcjonerskich oraz antyków, gdy działalność taka jest prowadzona z wykorzystaniem tzw. wolnego portu, w zakresie transakcji o wartości równej lub przekraczającej równowartość 10 000 EUR, bez względu na to, czy transakcja jest przeprowadzana jako pojedyncza operacja, czy kilka operacji, które wydają się ze sobą powiązane - są instytucjami obowiązanymi w rozumieniu przepisów AML/CTF. Przepisy dotyczące działalności gospodarczej polegającej na handlu dziełami sztuki oraz dodatkowe regulacje (m.in.

[81] unikatowa, cyfrowa jednostka danych oparta na architekturze *blockchain*, którą użytkownicy protokołu mogą między sobą handlować, reprezentująca szeroką gamę przedmiotów materialnych, tj. m.in. wirtualne dzieła sztuki

	stosowanie dyrektywy AML oraz konieczność prowadzenia księgi ewidencyjnej zabytków przyjętych lub oferowanych do zbycia) nakładają na sprzedawców z polskiego rynku rygorystyczne obowiązki, skutkujące precyzyjną identyfikacją wszystkich stron transakcji oraz transparentnością całego procesu sprzedaży, łącznie z identyfikowaniem źródła pochodzenia obiektu. Aktualnie obowiązujące, jedne z bardziej restrykcyjnych na tle ustawodawstwa europejskiego i światowego, przepisy dotyczące eksportu i importu antyków powodują, że legalnie działające podmioty gospodarcze mają pełną ewidencję obiektów wwiezionych i wywiezionych z kraju. Sporą niewiadomą jest jednak działalność polegająca na obrocie lub pośrednictwie w obrocie dziełami sztuki, przedmiotami kolekcjonerskimi oraz antykami pozyskanymi i przemyconymi z terenów objętych działaniami wojennymi na Ukrainie. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek prania pieniędzy w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	2
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie mechanizmu inwestowania środków pochodzących z nielegalnych źródeł w zakup antyków i dzieł sztuki jest jedną z metod prania pieniędzy. Jest to inwestycja długoterminowa i zyskowna, ale też obarczona kilkoma wadami. Główną zaletą dzieł sztuki jest stałe zwiększanie wartości, dosyć trudno na takiej inwestycji stracić, bo popyt systematycznie wzrasta, natomiast podaż jest ograniczona. Wadą jest jednak niska płynność, w obrocie na rynku jest bardzo mała ilość wartościowych obiektów. Inwestowanie w zakup antyków i dzieł sztuki wymaga dużej cierpliwości, a zysk zależny jest od mody. Trzeba mieć duże rozeznanie w rynku i spore doświadczenie. Inwestowanie wymaga skorzystania z usług doradztwa, należy sporządzić wyceny, a problemem może być autentyczność przedmiotów. Wykorzystanie mechanizmu inwestowania środków pochodzących z nielegalnych źródeł w zakup antyków i dzieł sztuki jest postrzegane raczej jako mało atrakcyjny sposób prania pieniędzy. GIIF otrzymywał nieliczne informacje o wykorzystywaniu tej metody do prania pieniędzy. WNIOSEK: Wykorzystanie mechanizmu inwestowania środków pochodzących z nielegalnych źródeł w zakup antyków i dzieł sztuki stwarza niskie zagrożenie prania pieniędzy.

Finansowanie terroryzmu

Tabela 53

Rodzaj wykorzystanych usług, produktów finansowych	Kamienie i metale szlachetne
Ogólny opis ryzyka	Kamienie i metale szlachetne zagrabione przez terrorystów są przemycane do innych krajów w celu ich sprzedaży
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Na rachunek bankowy spółki C wpływały relatywnie duże kwoty pieniędzy od podmiotów zajmujących się obrotem diamentami. Pieniądze były następnie transferowane na Środkowy Wschód na korzyść obywatela jednego z krajów europejskich - osoby A, pochodzącego z Afryki. Część środków była transferowana przez rachunek jednego z dyrektorów spółki C. Pieniądze były wymieniane na EUR, a następnie przekazywane na rzecz pana B. Pan A i B skupowali diamenty od rebeliantów działających w jednym z krajów afrykańskich, a następnie przemycali je do Europy. 2. Zakup przez polską spółkę metali szlachetnych, takich jak złoto, od spółki zagranicznej, pośredniczącej w obrocie kruszcem. Metale szlachetne mogą

	pochodzić z terenu objętego działalnością grup terrorystycznych a fundusze uzyskane z ich sprzedaży mogą zostać przeznaczone na ich finansowanie.
Poziom podatności	3
Uzasadnienie dla poziomu podatności	O ile kupno i sprzedaż relatywnie niewielkich ilości tego typu towarów nie nastręcza większej trudności (np. w sklepach jubilerskich), to kupno/sprzedaż ich dużych/hurtowych już tak. Łatwo jest jednak uniknąć identyfikacji, zwłaszcza przy zakupie/sprzedaży towarów o wartości poniżej równowartości 15 tys. EUR. Istnieje możliwość kupowania/sprzedawania przez Internet, a tym samym realizowania transakcji o charakterze międzynarodowym (np. przy zakupie kamieni lub metali od podmiotu zagranicznego). Obecnie podmioty prowadzące działalność w zakresie obrotu metalami lub kamieniami szlachetnymi i półszlachetnymi nie są IO, o ile nie przyjmują lub dokonują płatności za towary w gotówce o wartości równej lub przekraczającej równowartość 10 tys. EUR, bez względu na to, czy transakcja jest przeprowadzana jako pojedyncza operacja, czy kilka operacji, które wydają się ze sobą powiązane lub o ile nie prowadzą działalności kantorowej w zakresie kupna i sprzedaży złota dewizowego i platyny dewizowej. W Polsce istnieje możliwość zakupu złota w formie sztabek, a także złotych monet – tzw. monet bulionowych (bez wartości numizmatycznych). Oprócz tego monety bulionowe traktowane są jako legalny środek płatniczy, co zapewnia możliwość przewiezienia monet z kraju do kraju. Ponadto import, przetwarzanie oraz obrót diamentami nie jest działalnością reglamentowaną prawnie, co oznacza, że nie trzeba mieć na nią ani zezwolenia, ani koncesji, ani żadnej innej decyzji organu administracji publicznej. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	1
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie handlu kamieniami i metalami szlachetnymi zagrabionymi przez terrorystów jest jedną ze zidentyfikowanych metod finansowania terroryzmu. Kamienie bądź metale szlachetne są przemycane przez organizacje terrorystyczne ze stref wojny, gdzie działają te organizacje do innych krajów w celu ich sprzedaży na cele działalności terrorystycznej. Jest to jednak sposób finansowania częstokroć wymagający sporządzenia fałszywych certyfikatów pochodzenia dla sprzedawanych towarów. Nie jest całkiem bezpieczny, ponieważ może wzbudzić zainteresowanie służb kraju sprzedaży. Zastosowanie tego *modus operandi* wymaga znajomości lokalnego rynku, zaplanowania i specjalistycznej wiedzy na średnim poziomie. Brak jest informacji o możliwości wykorzystania tej metody do finansowania działalności terrorystycznej w Polsce. WNIOSEK: Wykorzystanie mechanizmu zakupu kamieni i metali szlachetnych od osób związanych z działalnością o charakterze terrorystycznym do finansowania terroryzmu stwarza w Polsce niskie zagrożenie.

Tabela 54

Rodzaj wykorzystanych usług, produktów finansowych	Antyki oraz dzieła sztuki
Ogólny opis ryzyka	Zakup skradzionych antyków i dzieł sztuki od osób związanych z działalnością o charakterze terrorystycznym
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	Zakup przez polskich kolekcjonerów dzieł sztuki oraz antyków pochodzących z obszarów objętych aktywnością organizacji terrorystycznych (np. Bliski Wschód). Zakupiony towar mógł zostać bezprawnie odebrany właścicielom przez

	organizację terrorystyczną w celu sfinansowania jej działalności.
Poziom podatności	3
Uzasadnienie dla poziomu podatności	Kupno/sprzedaż antyków czy dzieł sztuki jest relatywnie łatwe. Istnieje wiele firm handlujących tego typu towarami, na podstawie przepisów *ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców* (domy aukcyjne, antykwariaty). Istnieje możliwość kupowania/sprzedawania przez Internet, a tym samym realizowania transakcji o charakterze międzynarodowym. Obecnie przedsiębiorcy prowadzący działalność polegającą na obrocie lub pośrednictwie w obrocie dziełami sztuki, przedmiotami kolekcjonerskimi oraz antykami oraz prowadzący działalność polegającą na przechowywaniu dzieł sztuki, przedmiotów kolekcjonerskich oraz antyków, gdy działalność taka jest prowadzona z wykorzystaniem tzw. wolnego portu, w zakresie transakcji o wartości równej lub przekraczającej równowartość 10 000 euro, bez względu na to, czy transakcja jest przeprowadzana jako pojedyncza operacja, czy kilka operacji, które wydają się ze sobą powiązane - są instytucjami obowiązanymi w rozumieniu przepisów AML/CTF. Przepisy dotyczące działalności gospodarczej polegającej na handlu dziełami sztuki oraz dodatkowe regulacje (m.in. stosowanie dyrektywy AML oraz konieczność prowadzenia księgi ewidencyjnej zabytków przyjętych lub oferowanych do zbycia) nakładają na sprzedawców z polskiego rynku rygorystyczne obowiązki, skutkujące precyzyjną identyfikacją wszystkich stron transakcji oraz transparentnością całego procesu sprzedaży, łącznie z identyfikowaniem źródła pochodzenia obiektu. Aktualnie obowiązujące, jedne z bardziej restrykcyjnych na tle ustawodawstwa europejskiego i światowego, przepisy dotyczące eksportu i importu antyków powodują, że legalnie działające podmioty gospodarcze mają pełną ewidencję obiektów wwiezionych i wywiezionych z kraju. Sporą niewiadomą jest jednak działalność polegającą na obrocie lub pośrednictwie w obrocie dziełami sztuki, przedmiotami kolekcjonerskimi oraz antykami pozyskanymi i przemyconymi z terenów objętych działaniami wojennymi na Ukrainie. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	2
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie mechanizmu zakupu skradzionych antyków i dzieł sztuki od osób związanych z działalnością o charakterze terrorystycznym jest jednym ze sposobów finansowania działalności o charakterze terrorystycznym. Według ocen ekspertów jednym z podstawowych źródeł finansowania ISIS była kradzież i sprzedaż starożytnych dzieł sztuki z rejonu Syrii i Iraku. Nieznana jest jak dotąd skala przemytu dzieł sztuki z terenów objętych działaniami wojennymi na Ukrainie. Jednak sama metoda finansowania terroryzmu poprzez handel skradzionymi antykami i dziełami sztuki jest dosyć trudna do zastosowania. Wymaga sporych nakładów logistycznych, specjalistycznych ekspertyz, znajomości rynku dzieł sztuki, znajomości klientów gotowych zakupić towar na czarnym rynku, a każda operacja handlowa powinna pozostawać dyskrecjonalna. Częstokroć wymaga sporządzenia fałszywych certyfikatów pochodzenia dla sprzedawanych antyków i dzieł sztuki. Przeprowadzane operacje finansowe zawsze mogą wzbudzić podejrzenia co do ich legalności. Zastosowanie tego *modus operandi* wymaga zaplanowania i wysokospecjalistycznej wiedzy. Brak jest informacji o możliwości wykorzystania tej metody do finansowania działalności terrorystycznej w Polsce. WNIOSEK: Wykorzystanie mechanizmu zakupu skradzionych antyków i dzieł sztuki od osób związanych z działalnością o charakterze terrorystycznym do finansowania terroryzmu stwarza w Polsce średnie zagrożenie.

Podatność

Rynek dóbr wysokiej wartości jest pojęciem szerokim. Składa się na niego zarówno rynek dzieł sztuki, rynek antykwaryczny, rynek przedmiotów zabytkowych, bibliofilski, numizmatyczny, biżuteryjny, złota, srebra i kamieni szlachetnych itp.

Ilość opracowań dotyczących danego tematu nie jest duża. W niniejszym opracowaniu bazowano na informacjach Zespołu Naukowo-Badawczego Obrotu Dziełami Sztuki i Prawnej Ochrony Dziedzictwa Kulturowego Wydziału Prawa i Administracji, Uniwersytetu im. Adama Mickiewicza w Poznaniu, kierowanego przez prof. dr. hab. Wojciecha Szafrańskiego. Informacje te dotyczą przede wszystkim rynku dzieł sztuki.

Z wymienionych powyżej informacji wynika, że polski rynek sztuki składa się z rynku pierwotnego na którym następuje przepływ dzieł sztuki od artystów do kolekcjonerów oraz rynek wtórny, na którym zbywane są wcześniej zakupione dzieła. Większość dóbr podlegających obrotowi stanowią dzieła sztuki polskie lub z Polską związane.

Polski rynek dzieł sztuki został zbudowany oddolnie, przez podmioty z polskim kapitałem. Formowanie tego sektora następowało bez wsparcia państwa oraz w warunkach braku zainteresowania czynników politycznych kwestiami regulacji rynku. Istnieje na nim nierównowaga spowodowana dominacją kapitałową dużych domów aukcyjnych. Przejawia się to m.in. zacieraniem granic pomiędzy rynkiem pierwotnym i wtórnym, wyrażającym się m.in. organizacją przez duże podmioty z rynku wtórnego aukcji dzieł tzw. młodej sztuki.

Nie ma informacji ile faktycznie podmiotów działa na rynku. Istniejące dane wskazują na liczby od 200 do 600 podmiotów. Dane Zespołu Naukowo-Badawczego Obrotu Dziełami Sztuki i Prawnej Ochrony Dziedzictwa Kulturowego (dalej: Zespół), wskazują bardziej dokładnie liczbę pośredników w 2021 r. na blisko 380 podmiotów. Żadne dane nie uwzględniają w szczególności osób dokonujących okazjonalnej sprzedaży oraz tych, dla których sprzedaż dzieł sztuki jest faktycznie główną forma utrzymania, ale nie rejestrują działalności w tym zakresie. Szczególnie druga wymieniona kategoria osób pozostaje poza jakąkolwiek kontrolą, pomimo generowania stałego ruchu na rynku.

Nie ma również pewności co do obrotów na rynku. Istniejące dane są wyłącznie szacunkowe. Żadna instytucja nie gromadzi ich w sposób kompleksowy i obejmujący całość transakcji. Większość instytucji zaangażowanych, z danych Zespołu obejmujących bardzo szeroki zakres informacji wynika, że obroty na rynku dzieł sztuki można szacować w latach 2019 do 2021 na odpowiednio 467,5 mln, 561,8 mln oraz 838,6 mln złotych. Niewątpliwie wartość polskiego rynku dzieł sztuki rośnie z roku na rok. Świadczy o tym również umieszczenie dwóch podmiotów z Polski w pierwszej piętnastce największych pod względem obrotów domów aukcyjnych w Europie.

Brak jest odpowiednich regulacji dotyczących dokumentowania procesu sprzedaży, ich integralności oraz odpowiedzialności z tego tytułu. Nieuregulowany jest również zawód eksperta dla tego rynku. W obrocie funkcjonuje znaczna liczba wzorów dokumentów i certyfikatów, które ostatecznie nie mają faktycznego znaczenia.

Samoistnie kształtujący się rynek wytworzył szereg charakterystycznych sposobów działania. Jednym z nich jest dokonywanie transakcji bez spisywania formalnych umów. Niekontrolowany rozwój rynku spowodował zanik transparentności oraz upośledzenie możliwości oceny autentyczności obiektów oraz wiarygodności cen. Wszystko to działa w warunkach bezkrytycznego zaufania klienta do pośredników.

Przywołane informacje Zespołu dotyczą rynku dzieł sztuki, lecz są również właściwe dla pozostałych segmentów rynku dóbr wysokiej wartości. Nie ma faktycznej kontroli nad obrotem zarówno artykułami kolekcjonerskimi, kamieniami szlachetnymi, zabytkami itp.

Wybuch wojny na Ukrainie spowodował zwiększanie zagrożenia napływu dóbr wysokiej wartości nieznanego pochodzenia. Jeszcze przed wojną znacznym problemem był przemyt przez granicę zabytków[82], monet[83] oraz dzieł sztuki[8485]. Gwałtowny napływ uchodźców często przewożących swój majątek prywatny oraz niekontrolowanych w żaden sposób spowodował niewątpliwe zwiększenie ilości takich towarów w obrocie.

Zagrożenia w sektorze

Sektor obrotu towarami wielkiej wartości generuje znaczne ryzyko zarówno w zakresie AML/CTF jak i przestępstw bazowych.

Informacje Zespołu wskazują na szereg problemów charakterystycznych dla polskiego rynku sztuki np. brak regulacji zawodu rzeczoznawcy pozwala na manipulowanie wartością dóbr. Taki sam skutek może mieć brak kontroli nad procesem sprzedaży dzieł sztuki. Nie istnieje formalny mechanizm nadzoru nad np. procesem sprzedaży na aukcjach, gdzie potencjalnie możliwe jest windowanie cen danego dzieła. Problem był podnoszony przez licznych ekspertów rynku sztuki[86], opisujących zjawisko ogłaszania zakończenia licytacji danego dzieła uzyskaniem rekordowej ceny sprzedaży, pomimo iż nie doszło do faktycznej zmiany właściciela dzieła. Obiekty są później oferowane w sprzedaży prywatnej po obniżonej cenie.

Faktyczny brak zawodu eksperta, specyficznie ukształtowane „tradycje" oraz niska świadomość społeczna spowodowały, że patologią rynku polskiego jest obecność dużej ilości falsyfikatów. Można w tym zakresie przywołać sprawę prowokacji dziennikarskiej związanej z obrazem „Zjawa"[87]. Ekspertyzy i certyfikaty najczęściej sporządzane są przez podmioty, którym zależy na podwyższeniu wartości dzieła[88]. Okoliczności takie dają znaczną możliwość manipulowania cenami oraz stwarza możliwość dokonywania oszustw.

Dominacja poloników na rynku sztuki tworzy również warunki do powstawania baniek spekulacyjnych. Niedostatek dzieł uznanych twórców wywołał w ostatnich latach zwiększoną ilość tzw. aukcji młodej sztuki. Również dzieła uznanych artystów podlegają regularnym

[82] https://www.gov.pl/web/kas/przemyt-463-zabytkow-archeologicznych, dostęp: 23.01.2023 r.,
[83] https://www.gov.pl/web/kas/zatrzymalismy-przemyt-kilkuset-zabytkowych-monet, dostęp: 23.01.2023 r.,
[84]https://tygodniksanocki.pl/2017/08/11/drewniana-ikona-7-kg-bursztynu-1576-szt-tabletek-zatrzymali-podkarpaccy-funkcjonariusze-kas/, dostęp: 23.01.2023 r.,
[85]https://www.tvp.info/44561562/funkcjonariusze-kas-udaremnili-przemyt-zabytkowych-ikon, dostęp: 23.01.2022 r.,
[86] Janusz Miliszkiewicz „Agencja ratingowa dla rynku sztuki", Santander Art and Culture Law Review 1/2016 (2): str. 146
[87]https://www.tokfm.pl/Tokfm/7,103085,12079045,wojna-ze-zjawa-final-bezprecedensowej-prowokacji-dziennikarskiej.html, dostęp: 23.01.2023 r.,
[88] Janusz Miliszkiewicz „Agencja ratingowa dla rynku sztuki", str. 148

fluktuacjom. W przypadku braku faktycznego nadzoru nad rynkiem stwarza to realne zagrożenie dla pewności obrotu.

Osobnym problemem jest rosnący rynek sztuki w postaci NFT. Zespół wskazał liczne potencjalne zagrożenia jakie mogą wystąpić w związku z tym rynkiem m.in. brak stałego kursu sprzedaży, łatwość wymiany, zróżnicowanie platform wymiany NFT, duża liczba wirtualnych giełd, szybkość dokonywania transakcji oraz fakt, ze są to instrumenty na okaziciela.

Trudno jest ocenić jaki jest poziom wykorzystania innych rodzajów dóbr wysokiej wartości takich jak np. krwawe diamenty. W ostatnim czasie pojawiały się informacje o możliwości obrotu takimi dobrami przez przedstawicieli tzw. Grupy Wagnera. Pozyskiwane w Afryce kamienie transportowane są do Europy, głównie przez kraje afrykańskie, lecz podejrzewa się również transport oficjalnymi kanałami[89]. Jednocześnie sama Rosja nadal eksportuje znaczne ilości kamieni szlachetnych do państwa takich jak Chiny i Indie, Wskazuje się, że część ich może wracać do Europy pod postacią gotowej biżuterii[90]. W przypadku transportu kamieni szlachetnych z kierunku wschodniego nie można wykluczyć użycia terytorium Polski do ich tranzytu lub legalizacji.

Nierozwiązanym problemem jest kwestia używania do finansowania terroryzmu zrabowanych na terenach walk dóbr kultury. Najpoważniejszym źródłem takich artefaktów pozostaje obszar Bliskiego i Środkowego Wschodu. Pomimo utraty przez ISIS większości zajmowanych przez nią terenów na światowe rynki wciąż trafia strumień zrabowanych na terenie Syrii i Iraku zabytków[91]. Zauważyć należy, że w trakcie swojego istnienia na terenie części Iraku i Syrii samozwańczy kalifat dokonał licznych aktów wandalizmu niszcząc m.in. Muzeum Archeologiczne w Mosulu. Po wyzwoleniu miasta stwierdzono, że znaczna część zbirów nie została zniszczona, lecz podlegała najprawdopodobniej nielegalnemu wywozowi do państw ościennych. Ustalono równie, że ISIS prowadziła własne prace wykopaliskowe na terenach stanowisk archeologicznych, w północnej części Iraku i Syrii, niejednokrotnie zacierając ślady swojej działalności poprze niszczenie niektórych obiektów (np. świątynie Baala i Bela oraz łuk triumfalny w Palmyrze) lub niszcząc budynki przeszkadzające w tej działalności (np. Grobowiec Proroka Jonasza w Mosulu, zniszczony w celu zrabowania asyryjskiego pałacu znajdującego się pod nim). Działalność kalifatu w tym zakresie obejmowała także m.in. „opodatkowanie" innych grup rabujących zabytki oraz wytwarzanie handel podróbkami niektórych artefaktów[92]. Podobne zjawisko może wkrótce nastąpić na terenie Afganistanu, gdzie Talibowie przejęli zasoby m.in. Muzeum Narodowego w Kabulu oraz przygotowane we współpracy z instytucjami zagranicznymi dokumentację opisującą nowe stanowiska archeologiczne[93]. Utrata dostępu do kont zagranicznych, utrata finansowania z funduszy międzynarodowych oraz pogarszająca się sytuacja gospodarcza może, w dłuższej perspektywie wywołać chęć sięgnięcia do tych zasobów. Terytorium Polski może stać się co najmniej miejscem tranzytu takich obiektów lub miejscem, w którym będą legalizowane.

[89] https://www.money.pl/gospodarka/handel-krwawymi-diamentami-kwitnie-sprzedaje-je-nawet-grupa-wagnera-6840248757066272a.html, dostęp: 23.01.2023 r.,
[90]https://www.money.pl/gospodarka/krwawe-diamenty-putina-odzyskuja-blask-wymykaja-sie-sankcjom-6808012951693824a.html, dostęp: 23.01.2023 r.,
[91] https://pideeco.be/articles/terrorism-financing-blood-antiquities-looted-aml/, dostęp 23.01.2023 r.
[92] Destruction or theft? Islamic State, Iraqi antiquities and organized crime, marzec 2020 r.,
[93] Expert: Taliban will finance international terrorism by selling archaeological antiquities, 27.08.2021 r.

Uśredniony poziom zagrożenia sektora handlu dobrami wysokiej wartości – ML – 2,5 i FT – 1,5

Uśredniony poziom podatności sektora handlu dobrami wysokiej wartości – ML – 3,0 i FT – 3,0

Oszacowany poziom prawdopodobieństwa dla sektora – ML – 2,80 i FT - 2,40

Poziom ryzyka jest ostatecznie określany przez kombinację zagrożenia i podatności. Macierz ryzyka określająca ten poziom ryzyka opiera się na wadze 40% (zagrożenie) + 60% (podatność) – przy założeniu, że komponent podatności ma większą zdolność określania poziomu ryzyka. Zakłada się, że poziom podatności może zwiększyć atrakcyjność, a tym samym zamiary przestępców/terrorystów, aby użyć danego modus operandi – wpływając w ten sposób ostatecznie na poziom zagrożenia. Poziom ryzyka sektora, z uwzględniem prawdopobieństwa i konsekwencji (współczynnik 2,5 dla PP i 1,5 dla FT), jest ustalany zgodnie z metodyką krajowej oceny ryzyka – aneks nr 1.

Ryzyko FT sektora handlu dobrami wysokiej wartości – 2,04	
1 – 1,5	Niskie
1,6 – 2,5	Średnie
2,6 – 3,5	Wysokie
3,6 – 4	Bardzo wysokie
Ryzyko ML sektora handlu dobrami wysokiej wartości – 2,68	
1 – 1,5	Niskie
1,6 – 2,5	Średnie
2,6 – 3,5	Wysokie
3,6 – 4	Bardzo wysokie

WNIOSEK 1: Poziom ryzyka wykorzystania sektora handlu dobrami wysokiej wartości do finansowania terroryzmu w Polsce znajduje się na poziomie średnim.

WNIOSEK 2: Poziom ryzyka wykorzystania sektora handlu dobrami wysokiej wartości do prania pieniędzy w Polsce znajduje się na poziomie wysokim.

Mitygacja zidentyfikowanych ryzyk:

W celu ograniczenia prawdopodobieństwa wykorzystania sektora zajmującego się obrotem dobrami wysokiej wartości do prania pieniędzy lub finansowania terroryzmu, zasadne jest

podjęcie odpowiednich działań. Stosowanie zaproponowanych działań mitygujących powinno następować z uwzględnieniem rozpoznanego przez danę instytucję obowiązaną ryzyka.

Instytucje obowiązane z sektora zajmującego się obrotem dobrami wysokiej wartości powinny wdrożyć skuteczne procedury związane z odpowiednią oceną stosunków gospodarczych klienta oraz uzyskiwaniem informacji na temat ich celu i zamierzonego charakteru, a także powinny zapewnić bieżący monitoring stosunków gospodarczych. Instytucje obowiązane z sektora zajmującego się obrotem dobrami wysokiej wartości, powinny położyć nacisk na weryfikację źródła pochodzenia wartości majątkowych klientów.

W sektorze zajmującym się obrotem dobrami wysokiej wartości powinny być podejmowane działania podnoszące świadomość narażenia na przestępstwo prania pieniędzy oraz finansowania terroryzmu, jak również podnoszące poziom wyszkolenia pracowników tego sektora w analizie sygnałów ostrzegawczych wynikających z transakcji podejrzanych.

Organizowane powinny być szkolenia dla instytucji obowiązanych z sektora zajmującego się obrotem dobrami wysokiej wartości, podczas których będą przekazywane teoretyczne i praktyczne wskazówki dotyczące ustalania beneficjenta rzeczywistego oraz struktury własności i kontroli klientów a także raportowania rozbieżności do organu właściwego w sprawie CRBR. Zalecane jest uczestnictwo przedstawicieli instytucji obowiązanych w szkoleniach podnoszących świadomość AML/CTF, organizowanych zarówno przez GIIF, jak i przez UKNF w ramach Programu CEDUR.

Instytucje obowiązane z sektora zajmującego się obrotem dobrami wysokiej wartości powinny zwracać szczególną uwagę na źródło pochodzenia wartości majątkowych, jak również na źródło pochodzenia dóbr wysokiej wartości będących przedmiotem obrotu, w szczególności pod kątem pochodzenia z jurysdykcji charakteryzujących się wyższym ryzykiem prania pieniędzy oraz finansowania terroryzmu. Instytucje obowiązane powinny położyć szczególny nacisk na ustalenie danych dotyczących źródła pochodzenia dóbr będących przedmiotem obrotu a także wartości majątkowych, za które te dobra są nabywane.

Instytucje obowiązane powinny przykładać szczególną wagę do czynników geograficznych mogących wskazywać na wyższe ryzyko prania pieniędzy czy też finansowania terroryzmu, takich jak niestabilna sytuacja polityczna czy konflikt zbrojny, czego najdobitniejszym przykładem w ostatnich latach jest wojna prowadzona przez Rosję przeciwko Ukrainie. Z uwagi na wysokie ryzyko transferowania środków pochodzących z nielegalnego handlu, przemytu ludzi, handlu bronią, czy też działań zmierzających do omijania sankcji gospodarczych, szczególnie istotne jest analizowanie przez instytucje obowiązane nie tylko danych dotyczących samych stron transakcji, ale również beneficjentów rzeczywistych, czy też faktycznych celów przeprowadzania danych transakcji. Podmioty z sektora zajmującego się obrotem dobrami wysokiej wartości powinny weryfikować dokumenty dotyczące przedmiotów objętych obrotem, w szczególności, w uzasadnionych przypadkach, powinny występować do klientów o przedstawienie potwierdzenia złożenia deklaracji celnych dotyczących przywiezionych z zagranicy wartościowych przedmiotów, czy też uzyskania stosownych pozwoleń na przywóz dóbr kultury.

Istotnym czynnikiem ryzyka w działalności podmiotów z sektora zajmującego się obrotem dobrami wysokiej wartości jest dokonywanie transakcji bez spisywania formalnych umów. Z punktu widzenia obowiązków instytucji obowiązanych, brak udokumentowania przeprowadzanej transakcji jest niedopuszczalny. Występujący na rynku dóbr wysokiej

wartości zanik transparentności stanowi skutek obustronnie niekorzystny. Brak odpowiedniego dokumentowania transakcji stanowi istotne naruszenie obowiązujących przepisów dotyczących przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, co wobec przedsiębiorców zajmujących się obrotem dobrami wysokiej wartości może skutkować nałożeniem dotkliwej kary finansowej. Dla klientów, którzy nie udokumentowali przeprowadzenia transakcji, może wystąpić szereg niekorzystnych następstw, na przykład brak możliwości udowodnienia wartości przedmiotu na podstawie ceny nabycia (co może być kluczowe dla ewentualnych roszczeń klienta w sytuacji utraty lub zniszczenia przedmiotu zakupu). Działaniami mitygującymi opisane ryzyko byłoby przede wszystkim przestrzeganie obowiązujących procedur przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu. W celu mitygacji opisanego ryzyka konieczne może okazać się przyjęcie przepisów obligujących przedsiębiorców z sektora zajmującego się obrotem dobrami wysokiej wartości do rejestrowania transakcji w elektronicznym rejestrze.

Ryzykiem związanym z rynkiem dzieł sztuki jest nieuregulowanie zawodu eksperta, czego skutkiem jest funkcjonowanie wielu wzorów dokumentów i certyfikatów, które ostatecznie nie mają faktycznego, realnego znaczenia. W celu ograniczenia tego ryzyka należy rozważyć uregulowanie zawodu eksperta rynku dzieł sztuki.

13. Obszar – działalność gospodarcza (ogólnie)

Opis sektora – zawarty jest w podrozdziale 2.2 „Rynek pozafinansowy" oraz w podrozdziale 7.2.2. „Podatność rynku pozafinansowego".

Scenariusze wystąpienia ryzyka (tj. możliwe przykłady wystąpienia ryzyka) dotyczyły wykorzystania do prania pieniędzy legalnie funkcjonujących podmiotów gospodarczych, schematu przedsiębiorstw symulujących oraz usług prawniczych i doradztwa podatkowego, a do finansowania terroryzmu dotyczyły wykorzystania legalnie funkcjonujących podmiotów gospodarczych oraz schematu przedsiębiorstw symulujących. Opis scenariuszy znajduje się poniżej.

Pranie pieniędzy

Tabela 55

Rodzaj wykorzystanych usług, produktów finansowych	Legalna działalność podmiotów gospodarczych
Ogólny opis ryzyka	Wykorzystanie funkcjonujących podmiotów gospodarczych do prania pieniędzy
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Celowe łączenie środków pochodzących z nielegalnej działalności z legalnymi przychodami podmiotu gospodarczego zajmującego się handlem międzynarodowym w celu utrudnienia identyfikacji źródła pochodzenia konkretnych środków. 2. Wykorzystanie podmiotów gospodarczych, które w dużym stopniu uzyskują przychody z prowadzonej działalności gospodarczej w gotówce (np. restauracji, hoteli). Zawyżanie łącznej kwoty przychodów staje się sposobem wprowadzania do legalnego obrotu gospodarczego środków pochodzących z nielegalnej działalności. 3. Wykorzystywania podmiotów zakładanych za granicą (posiadających rachunki w RP) w celu wprowadzania do legalnego obrotu gospodarczego środków pochodzących z nielegalnej działalności. 4. Wykorzystania polskich spółek, w których właścicielami/udziałowcami są cudzoziemcy w celu wprowadzania do legalnego obrotu gospodarczego środków pochodzących z nielegalnej działalności. 5. Wykorzystywanie polskich spółek posiadających zagraniczne rachunki (prowadzone na rzecz rezydentów) w celu wprowadzania do legalnego obrotu gospodarczego środków pochodzących z nielegalnej działalności.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Założenie spółki prawa handlowego czy też rozpoczęcie działalności jako osoba fizyczna prowadząca działalność gospodarczą jest w pewnym zakresie ograniczona przepisami prawa, wymagającymi ich rejestracji i spełnienia pewnych warunków (np. w przypadku spółek kapitałowych i spółki komandytowo-akcyjnej posiadaniem kapitału zakładowego w określonej wysokości). Istnieją możliwości ukrycia danych beneficjenta rzeczywistego posłużeniem się słupami lub przedsiębiorstwami symulującymi. Wniesienie kapitału założycielskiego lub też kupno/nabycie już istniejącego podmiotu może być dokonane za pośrednictwem transakcji finansowej o międzynarodowym charakterze lub też przy udziale osób/podmiotów zagranicznych. Tylko część podmiotów gospodarczych należy do IO. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma ograniczone możliwości gromadzenia i analizowania informacji, jakkolwiek zdolność ich szybkiego analizowania jest ograniczona z powodu braków kadrowych i odpowiednio wydajnego software'u. Istnieje duże prawdopodobieństwo, że przypadek prania pieniędzy w zakresie analizowanych

	scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	4
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie funkcjonujących podmiotów gospodarczych do prania pieniędzy jest jedną z najczęściej spotykanych metod prania pieniędzy. Jest to sposób szeroko dostępny, jego zastosowanie niewiele kosztuje i jest postrzegany przez sprawców jako bardzo atrakcyjny. Wykorzystanie funkcjonujących podmiotów gospodarczych do prania pieniędzy nie wymaga specjalistycznej wiedzy o systemie bankowym ani szczególnych, specjalistycznych umiejętności. Wykorzystywany często przez zorganizowaną przestępczość. Gdy grupa przestępcza otrzymuje pieniądze np. z ulicznej sprzedaży narkotyków, wykorzystuje się do prania pieniędzy przedsiębiorstwa, które potencjalnie uzyskują w gotówce swoje przychody. Taniość metody zapewnia kreatywna księgowość oraz optymalizacja podatkowa. GIIF otrzymuje informacje o wykorzystywaniu tej metody do prania pieniędzy. WNIOSEK: Wykorzystanie funkcjonujących podmiotów gospodarczych do prania pieniędzy stwarza bardzo wysokie zagrożenie prania pieniędzy.

Tabela 56

Rodzaj wykorzystanych usług, produktów finansowych	Przedsiębiorstwa symulujące
Ogólny opis ryzyka	Wykorzystanie spółek nieprowadzących w praktyce działalności gospodarczej do prania pieniędzy
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Zakup spółek, które wcześniej prowadziły działalność gospodarczą, w celu wykorzystania ich do utrudnienia identyfikacji transferu wartości majątkowych pochodzących z nielegalnej działalności. 2. Sprawcy tworzą skomplikowane i długie łańcuchy powiązań organizacyjno-własnościowych pomiędzy podmiotami gospodarczymi, stowarzyszeniami, organizacjami charytatywnymi, trustami (przy zaangażowaniu podmiotów zarejestrowanych w różnych jurysdykcjach, w tym w rajach podatkowych) w celu utrudnienia identyfikacji rzeczywistych właścicieli podmiotów wykorzystywanych do prania pieniędzy. 3. Transferowanie wartości majątkowych pomiędzy ww. podmiotami pod fikcyjnymi tytułami (np. kupna/sprzedaży towarów/usług, udziałów/akcji, udzielenia/spłaty pożyczek) w celu ukrycia ich pochodzenia. 4. Wykorzystywanie usług z zakresu księgowości i administracji, oferowanych przez podmiot gospodarczy specjalizujący się w tego typu działalności, dla założenia i prowadzenia spółki z o. o., wykorzystywanej do prania pieniędzy.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Założenie spółki prawa handlowego czy też rozpoczęcie działalności jako osoba fizyczna prowadząca działalność gospodarczą jest w pewnym zakresie ograniczona przepisami prawa, wymagającymi ich rejestracji i spełnienia pewnych warunków (np. w przypadku spółek kapitałowych i spółki komandytowo-akcyjnej posiadaniem kapitału zakładowego w określonej wysokości). Istnieją możliwości ukrycia danych beneficjenta rzeczywistego posłużeniem się słupami lub przedsiębiorstwami symulującymi. Wniesienie kapitału założycielskiego lub też kupno/nabycie już istniejącego podmiotu może być dokonane za pośrednictwem transakcji finansowej o międzynarodowym charakterze lub też przy udziale osób/podmiotów zagranicznych. Tylko część podmiotów gospodarczych należy do IO. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma ograniczone możliwości gromadzenia i analizowania informacji, jakkolwiek zdolność ich szybkiego analizowania jest ograniczona z powodu braków kadrowych i odpowiednio wydajnego software'u. Istnieje duże

	prawdopodobieństwo, że przypadek prania pieniędzy w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	4
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie spółek nieprowadzących w praktyce działalności gospodarczej do prania pieniędzy jest jedną z najczęściej spotykanych metod prania pieniędzy. Jest to sposób szeroko dostępny, jego zastosowanie niewiele kosztuje i jest postrzegany przez sprawców jako atrakcyjny i bezpieczny. Częstokroć jest traktowany jako element niezbędny w operacjach mających na celu legitymizowanie środków pochodzących z działalności przestępczej. Wykorzystanie spółek nieprowadzących w praktyce działalności gospodarczej nie wymaga specjalistycznej wiedzy o systemie bankowym ani specjalistycznych umiejętności. Wykorzystywane są właściwie jedynie rachunki bankowe takich symulujących działalność firm. Przedsiębiorstwo symulujące może mieć tylko charakter elementu pośredniego w łańcuchu transakcji, mającego za zadanie zaciemnienie i wydłużenie ścieżki transakcyjnej dla pranych pieniędzy. Ale może też mieć charakter końcowego ogniwa w łańcuchu transakcyjnym. Przedsiębiorstwo symulujące działalność gospodarczą może być podmiotem krajowym, ale też może być zarejestrowane w obcej jurysdykcji, szczególnie w „raju podatkowym', gdzie obowiązują restrykcyjne przepisy dotyczące tajemnicy bankowej. GIIF otrzymuje informacje o wykorzystywaniu tej metody do prania pieniędzy. WNIOSEK: Wykorzystanie spółek nieprowadzących w praktyce działalności gospodarczej stwarza bardzo wysokie zagrożenie prania pieniędzy.

Tabela 57

Rodzaj wykorzystanych usług, produktów finansowych	Usługi prawnicze, doradztwa podatkowego
Ogólny opis ryzyka	Korzystanie z pośrednictwa innych podmiotów w legitymizowaniu środków pochodzących z nielegalnej działalności
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	Wspomaganie przestępców w przeprowadzaniu transakcji zakupu nieruchomości i towarów o wysokiej wartości, tworzeniu i prowadzeniu podmiotów gospodarczych, fundacji, trustów w kraju i za granicą, a także transakcji finansowych poprzez użyczanie swoich rachunków bankowych.
Poziom podatności	3
Uzasadnienie dla poziomu podatności	Dostęp do usług prawniczych i doradztwa podatkowego jest stosunkowo łatwy. Wspomagają one ukrywanie danych identyfikacyjnych klientów i realizowanie transakcji o charakterze międzynarodowym. Podmioty świadczące tego typu usługi są IO. Posiadają pewną świadomość swoich obowiązków z zakresu PPP/PFT. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma ograniczoną możliwość gromadzenia i analizowania informacji, jakkolwiek zdolność ich szybkiego analizowania jest ograniczona z powodu braków kadrowych i odpowiednio wydajnego software'u. Istnieje duże prawdopodobieństwo, że przypadek prania pieniędzy w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w niewielkiej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	4

Uzasadnienie dla poziomu zagrożenia	Korzystanie z pośrednictwa innych podmiotów (zwłaszcza adwokatów, doradców podatkowych, notariuszy) w celu transferowania i legitymizowania środków pochodzących z nielegalnych źródeł jest jedną z podstawowych metod prania pieniędzy. GIIF posiada informacje o wykorzystywaniu tego *modus operandi*. Przedstawiciele wyżej wymienionych zawodów zapewniają dostęp przestępcom do specjalistycznej wiedzy prawnej i wiedzy podatkowej. W sposób zasadniczy może to pomóc w praniu pieniędzy z czynów zabronionych. Nie bez znaczenia jest też możliwość ulokowania środków finansowych na rachunkach bankowych należących do prawników, np. w formie depozytu. Wypłata lub przelew na inny rachunek z takiego rachunku jest pozorowaniem legalnego pochodzenia wartości majątkowych uzyskanych w wyniku działalności przestępczej i ma wszelkie cechy legitymizowania środków podlegających praniu. Skorzystanie z pośrednictwa zawodów prawniczych czy doradcy podatkowego jest istotne również z tego powodu, ponieważ usługi oferowane przez te zawody są niekiedy niezbędne do realizacji konkretnej transakcji i zwiększają bezpieczeństwo przeprowadzanej transakcji. Sam dostęp do usług prawnych doradców podatkowych, notariuszy czy adwokatów jest dosyć łatwy i nie wymaga szczególnych kompetencji ani wiedzy specjalistycznej. Ten *modus operandi* postrzegany jest przez sprawców jako dosyć atrakcyjna i bezpieczna forma prania pieniędzy. WNIOSEK: wykorzystanie pośrednictwa innych podmiotów (zwłaszcza adwokatów, doradców podatkowych, notariuszy) w celu transferowania i legitymizowania środków pochodzących z nielegalnych źródeł stwarza wysokie zagrożenie dla prania pieniędzy.

Tabela 58

Rodzaj wykorzystanych usług, produktów finansowych	Przekupstwo zagraniczne (*ang. foreign bribery*)
Ogólny opis ryzyka	Przekupstwo zagranicznego funkcjonariusza publicznego[94]
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Urzędnik Ministerstwa Gospodarki w jednym z państw afrykańskich przyjął zaproponowaną mu korzyść majątkową w zamian za korzystne załatwienie kontraktu na rzecz polskiej firmy działającej na tym kontynencie. Środki pochodzące z przestępstwa zostały ulokowane w jednym z banków afrykańskich i w krótkim okresie czasu zostały wypłacone w gotówce przez osoby będące pełnomocnikami do rachunku bankowego. 2. Polskie służby zidentyfikowały kilka transakcji w polskim systemie finansowym, których beneficjentem był funkcjonariusz publiczny jednego z państw UE. Osoba ta prowadziła 'nieoficjalny" lobbing na rzecz realizacji przez państwo polskie kontraktu rządowego na terenie RP. Podmiot (wykonawca) kontraktu pochodził z państwa Unii Europejskiej lobbującego funkcjonariusza. Środki były wypłacane w gotówce, a następnie przewożone poza granicę RP.
Poziom podatności	3

[94] zagraniczny funkcjonariusz publiczny oznacza każdą osobę zajmującą stanowisko ustawodawcze, administracyjne lub sądowe w obcym państwie, zarówno mianowaną, jak i wybraną, jak również każdą osobę wykonującą funkcje publiczne na rzecz państwa obcego, włączając funkcjonariusza agendy publicznej lub przedsiębiorstwa publicznego i każdego funkcjonariusza lub przedstawiciela publicznej organizacji międzynarodowej

Uzasadnienie dla poziomu podatności	Pranie pieniędzy pochodzących z przestępstwa przekupstwa zagranicznego funkcjonariusza publicznego jest przestępstwem, które jest identyfikowane przez organy administracji publicznej. Polscy funkcjonariusze publiczni są zobowiązani do zgłaszania zarzutów popełnienia przestępstwa z art. 304 ust. 2 k.p.k. Niestosowanie się do art. 304 ust. 2 k.p.k. może stanowić przestępstwo z art. 231 kk. (nadużycie funkcji). Przestępstwo prania pieniędzy w przypadku przekupstwa zagranicznego funkcjonariusza publicznego zostało zawarte w art. 7 *Konwencji o zwalczaniu przekupstwa zagranicznych funkcjonariuszy publicznych w międzynarodowych transakcjach handlowych.* Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. Istnieje prawdopodobieństwo, że przypadek prania pieniędzy w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne które odpowiadają w zakresowi analizowanego ryzyka. W związku z trwającym konfliktem wojennym na Ukrainie, a także przyszłą odbudową państwa ukraińskiego istnieje zagrożenie przekupstwa zagranicznego funkcjonariuszy publicznych Ukrainy przez przedstawicieli zagranicznych firm, chcących uzyskać np. kontrakty na odbudowę powojenną tego kraju.
Poziom zagrożenia	4
Uzasadnienie dla poziomu zagrożenia	Przekupstwo zagranicznego funkcjonariusza publicznego jest przestępstwem trudnym do wykrycia i wymaga określonych działań podejmowanych przez służby danego państwa. Należy podkreślić fakt, że osoby pełniące wskazaną funkcję często korzystają z tzw. przywilejów i immunitetów dyplomatycznych, które uniemożliwiają bądź też utrudniają podjęcie działań odpowiednim służbom w sytuacji zidentyfikowania tego przestępstwa. Należy zaznaczyć, że konsekwencje wynikające z przekupstwa zagranicznego funkcjonariusza publicznego mogą mieć, w niektórych przypadkach, znaczący wpływ na prawidłowe funkcjonowanie danego państwa (informacje strategiczne dot. danego państwa, informacje wrażliwe itp.). GIIF posiada informacje o wykorzystywaniu tego *modus operandi*. Ten sposób wprowadzania do obrotu nielegalnych środków postrzegany jest przez sprawców jako dosyć atrakcyjna i bezpieczna forma prania pieniędzy. WNIOSEK: przekupstwo zagraniczne funkcjonariusza publicznego stwarza wysokie zagrożenie dla prania pieniędzy.

Finansowanie terroryzmu

Tabela 59

Rodzaj wykorzystanych usług, produktów finansowych	Legalna działalność podmiotów gospodarczych
Ogólny opis ryzyka	Wykorzystanie funkcjonujących podmiotów gospodarczych do finansowania terroryzmu.

Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Firma X działająca na rynku samochodów używanych finansuje terroryzm z przychodów uzyskanych z tytułu sprzedanych pojazdów. 2. Finansowanie działalności organizacji terrorystycznej z dochodów osiągniętych przez firmę zajmującą się leasingiem i obrotem nieruchomościami. 3. Celowe łączenie środków uzyskanych od sponsorów organizacji terrorystycznej z legalnymi przychodami podmiotu gospodarczego zajmującego się handlem międzynarodowym w celu utrudnienia identyfikacji procederu finansowania terroryzmu. 4. Osoba prowadząca działalność gospodarczą w sektorze IT świadczy usługi dla klientów z wielu krajów, może pracować zdalnie. Jako firma osoba ta akceptuje różne metody płatności, takie jak PayPal, przelewy bankowe, kryptowaluty itp. Firma ta przelewa i otrzymuje płatności od innej firmy świadczącej usługi informatyczne dla klientów zza granicy. Ta druga firma jest znana z tego, że próbowała już przelać środki osobie powiązanej z organizacją terrorystyczną.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Założenie spółki prawa handlowego czy też rozpoczęcie działalności jako osoba fizyczna prowadząca działalność gospodarczą jest w pewnym zakresie ograniczona przepisami prawa, wymagającymi ich rejestracji i spełnienia pewnych warunków (np. w przypadku spółek kapitałowych i spółki komandytowo-akcyjnej posiadaniem kapitału zakładowego w określonej wysokości). Istnieją możliwości ukrycia danych beneficjenta rzeczywistego posłużeniem się słupami lub przedsiębiorstwami symulującymi. Wniesienie kapitału założycielskiego lub też kupno/nabycie już istniejącego podmiotu może być dokonane za pośrednictwem transakcji finansowej o międzynarodowym charakterze lub też przy udziale osób/podmiotów zagranicznych. Tylko część podmiotów gospodarczych należy do IO. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma ograniczone możliwości gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	2

Uzasadnienie dla poziomu zagrożenia	Wykorzystanie funkcjonujących podmiotów gospodarczych do finansowania terroryzmu jest jednym z podstawowych sposobów finansowania działalności terrorystycznej. Legalnie funkcjonujące firmy działają na rzecz organizacji terrorystycznych, a część bądź całość zysków tych firm jest przekazywana na działalność związaną z terroryzmem. Firmy te zazwyczaj są ulokowane w branżach związanych z handlem nieruchomościami, handlem elektroniką, używanymi samochodami, metalami szlachetnymi, tekstyliami, eksportem i importem żywności oraz gastronomią. Legalnie działające firmy mogą zostać wykorzystane zarówno do bezpośredniego pozyskiwania funduszy wspierających działania terrorystyczne, jak i jako pasy transmisyjne do przekazywania środków związanych z finansowaniem takiej działalności. Często legalne środki podmiotu gospodarczego mieszane są ze środkami uzyskanymi ze źródeł finansujących terroryzm i przekazywane dalej, by utrudnić identyfikację środków jako wspierających terroryzm. Częstokroć legalnie działające firmy zajmujące się przepływem środków związanych z finansowaniem terroryzmu są prowadzone przez członków jednej grupy etnicznej, co wpływa na trudności w rozpoznaniu tego procederu. Jest to sposób stosunkowo łatwy i szeroko dostępny, jego zastosowanie niewiele kosztuje i może być postrzegany przez sprawców raczej jako w miarę atrakcyjny. Wykorzystanie funkcjonujących podmiotów gospodarczych do finansowania terroryzmu z reguły nie wzbudza podejrzeń. Wysoki wolumen obrotów przedmiotowych firm pozwala ukryć wykorzystanie tych firm do przekazywania pieniędzy na cele działalności terrorystycznej. Zwłaszcza gdy nie są to jednorazowo sumy zbyt wysokie. W celu ukrycia beneficjenta rzeczywistego częstokroć wykorzystuje się sfałszowaną dokumentację transakcji. Zastosowanie tego *modus operandi* wymaga jednak zaplanowania, wiedzy o rachunkowości i umiejętności logistycznych. W raporcie Europolu TE-SAT za 2020 r. Polska zauważyła, że składki na działalność prawicowych grup ekstremistycznych pochodzą od członków tych grup, posiadających legalne prywatne firmy. GIIF otrzymywał nieliczne informacje o możliwości wykorzystania tej metody do finansowania działalności terrorystycznej. WNIOSEK: Wykorzystanie funkcjonujących podmiotów gospodarczych do finansowania terroryzmu stwarza w Polsce średnie zagrożenie.

Tabela 60

Rodzaj wykorzystanych usług, produktów finansowych	Przedsiębiorstwa symulujące
Ogólny opis ryzyka	Wykorzystanie spółek nieprowadzących w praktyce działalności gospodarczej do finansowania terroryzmu.
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Zakup spółek, które wcześniej prowadziły działalność gospodarczą, w celu wykorzystania ich do utrudnienia identyfikacji transferu wartości majątkowych mających za cel finansowanie terroryzmu. 2. Prowadzenie na rzecz spółki z o.o. należącej do cudzoziemca usług z zakresu księgowości i administracji przez polski podmiot gospodarczy specjalizujący się w obsłudze przedsiębiorstw. Wykorzystanie omawianej spółki z o. o. do finansowania terroryzmu. 3. Sprawcy tworzą skomplikowane i długie łańcuchy powiązań organizacyjno-własnościowych pomiędzy podmiotami gospodarczymi, stowarzyszeniami, organizacjami charytatywnymi, trustami (przy zaangażowaniu podmiotów zarejestrowanych w różnych jurysdykcjach, w tym w rajach podatkowych) w celu utrudnienia identyfikacji rzeczywistych właścicieli podmiotów wykorzystywanych do finansowania terroryzmu. 4. Transferowanie wartości majątkowych za pośrednictwem ww. podmiotów pod fikcyjnymi tytułami (np. kupna/sprzedaży towarów/usług, udziałów/akcji, udzielenia/spłaty pożyczek) w celu sfinansowania potrzeb terrorystów.
Poziom podatności	2

Uzasadnienie dla poziomu podatności	Założenie spółki prawa handlowego czy też rozpoczęcie działalności jako osoba fizyczna prowadząca działalność gospodarczą jest w pewnym zakresie ograniczone przepisami prawa, wymagającymi ich rejestracji i spełnienia pewnych warunków (np. w przypadku spółek kapitałowych i spółki komandytowo-akcyjnej posiadaniem kapitału zakładowego w określonej wysokości). Istnieją możliwości ukrycia danych beneficjenta rzeczywistego posłużeniem się słupami lub przedsiębiorstwami symulującymi. Wniesienie kapitału założycielskiego lub też kupno/nabycie już istniejącego podmiotu może być dokonane za pośrednictwem transakcji finansowej o międzynarodowym charakterze lub też przy udziale osób/podmiotów zagranicznych. Tylko część podmiotów gospodarczych należy do IO. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma ograniczone możliwości gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	2
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie spółek nieprowadzących w praktyce działalności gospodarczej jest jednym z podstawowych sposobów dla przesyłu środków związanych z finansowaniem działalności terrorystycznej. Legalnie założone, ale nie funkcjonujące w praktyce działalności gospodarczej firmy, posługują się kilkoma rachunkami, które funkcjonują tylko jako pasy transmisyjne dla przesyłu środków finansowych na rzecz organizacji terrorystycznych. Dokonywane na rzecz firmy wpłaty gotówkowe bądź przelewy mają służyć zaciemnieniu pochodzenia środków, które są przekazywane dalej, często na rachunki innych podmiotów ulokowanych już w rejonach wrażliwych z punktu widzenia zwalczania terroryzmu. Częstokroć te pozornie tylko działające firmy zajmujące się przepływem środków związanych z finansowaniem terroryzmu są prowadzone przez członków jednej grupy etnicznej, co wpływa na trudności w rozpoznaniu tego procederu. Wykorzystanie spółek nieprowadzących w praktyce działalności gospodarczej dla przesyłu środków związanych z finansowaniem działalności terrorystycznej jest sposobem stosunkowo łatwym i szeroko dostępnym, a jego zastosowanie niewiele kosztuje i może być postrzegany przez sprawców raczej jako w miarę atrakcyjne. Wykorzystanie funkcjonujących podmiotów gospodarczych do finansowania terroryzmu z reguły nie wzbudza podejrzeń, choć zagrożeniem jest czasem widoczna niestandardowość tych firm w podejściu biznesowym. W celu ukrycia beneficjenta rzeczywistego częstokroć wykorzystuje się sfałszowaną dokumentację transakcji. Zastosowanie tego *modus operandi* wymaga jednak zaplanowania, wiedzy o rachunkowości i umiejętności logistycznych. GIIF otrzymywał nieliczne informacje o możliwości wykorzystania tej metody do finansowania działalności terrorystycznej. WNIOSEK: Wykorzystanie spółek nieprowadzących w praktyce działalności gospodarczej do finansowania terroryzmu stwarza w Polsce średnie zagrożenie.

Podstawową zasadą wprost wyrażoną w *ustawie z dnia 6 marca 2018 r. – Prawo przedsiębiorców* jest zasada wolności prowadzenia działalności gospodarczej. Oznacza to, iż podejmowanie, wykonywanie i zakończenie działalności gospodarczej jest wolne dla każdego na równych prawach. Jedynie do wykonywania działalności gospodarczej w dziedzinach mających szczególne znaczenie ze względu na bezpieczeństwo państwa lub obywateli albo inny ważny interes publiczny, gdy działalność ta nie może być wykonywana jako wolna, wymagane jest uzyskanie odpowiedniej koncesji, zezwolenia albo uzyskanie wpisu do rejestru działalności regulowanej. Polskie prawo za przedsiębiorcę uznaje wykonującą działalność gospodarczą osobę fizyczną, osobę prawną lub jednostkę organizacyjną niebędącą osobą prawną, której

odrębna ustawa przyznaje zdolność prawną, jak również wspólników spółki cywilnej w zakresie wykonywanej przez nich działalności gospodarczej. Działalność gospodarczą można podjąć w dniu złożenia wniosku o wpis do Centralnej Ewidencji i Informacji o Działalności Gospodarczej albo po dokonaniu wpisu do rejestru przedsiębiorców Krajowego Rejestru Sądowego, chyba że przepisy szczególne stanowią inaczej. Ale spółka kapitałowa w organizacji może podjąć działalność gospodarczą przed wpisem do rejestru przedsiębiorców.

W Polsce działalność gospodarczą można prowadzić w postaci różnych form prawnych. W przypadku indywidualnej działalności gospodarczej i spółek cywilnych miejscem rejestracji działalności jest Centralna Ewidencja Informacji o Działalności Gospodarczej. W przypadku pozostałych form prawnych miejscem rejestracji jest Krajowy Rejestr Sądowy. Krajowy Rejestr Sądowy składa się z rejestru przedsiębiorców; rejestru stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz publicznych zakładów opieki zdrowotnej; oraz z rejestru dłużników niewypłacalnych.

Na koniec grudnia 2022 r. Główny Urząd Statystyczny szacował liczbę podmiotów prowadzących działalność gospodarczą na 4 986 256[95]. Nie oznacza to jednak, iż w Polsce jest obecnie aktywnych prawie 5 mln firm. W statystykach GUS znajdują się bowiem podmioty, które zawiesiły wykonywanie działalności, podmioty które zakończyły działalność lecz informacja o tym fakcie nie dotarła do GUS oraz podmioty, które nie są przedsiębiorcami (fundacje, stowarzyszenia). Rejestr przedsiębiorców stosuje się do następujących podmiotów: spółek jawnych; europejskich zgrupowań interesów gospodarczych; spółek partnerskich; spółek komandytowych; spółek komandytowo-akcyjnych; spółek z ograniczoną odpowiedzialnością; spółek akcyjnych; spółek europejskich; spółdzielni; przedsiębiorstw państwowych; jednostek badawczo-rozwojowych; przedsiębiorców określonych w przepisach o zasadach prowadzenia na terytorium Rzeczypospolitej Polskiej działalności gospodarczej w zakresie drobnej wytwórczości przez zagraniczne osoby prawne i fizyczne; towarzystw ubezpieczeń wzajemnych; innych osób prawnych, jeżeli wykonują działalność gospodarczą i podlegają obowiązkowi wpisu do rejestru; oddziałów przedsiębiorców zagranicznych działających na terytorium Rzeczypospolitej Polskiej; głównych oddziałów zagranicznych zakładów ubezpieczeń.

Podmiot obowiązany do złożenia wniosku o wpis do Rejestru nie może powoływać się wobec osób trzecich działających w dobrej wierze na dane, które nie zostały wpisane do Rejestru lub uległy wykreśleniu z Rejestru.

Jednocześnie z analiz przeprowadzonych przez Centralny Ośrodek Informacji Gospodarczej[96] wynika, iż na dzień 11 sierpnia 2022 r. działało w Polsce 93 258 spółek z udziałem kapitału zagranicznego lub których beneficjentami rzeczywistymi są obywatele innych państw. Wśród nowych spółek co roku powstaje od 6 000 do 10 000 nowych firm z kapitałem zagranicznym.

W 2015 r. takich spółek powstało 6 706, w 2016 r. 7122, w 2017 r. 7 282, w 2018 r. 7 878 spółek, w 2019 r. 8 820 spółek, w 2020 r. 6 924, w 2021 10 494, a do końca czerwca 2022 r. 5 581 spółek. Co roku też 3 500 – 4 000 spółek zmienia właścicieli z polskich na zagranicznych. Ponadto blisko 60% wszystkich aktywnych spółek zagranicznych powstało w ostatnich 5

[95]https://stat.gov.pl/obszary-tematyczne/podmioty-gospodarcze-wyniki-finansowe/zmiany-strukturalne-grup-podmiotow/miesieczna-informacja-o-podmiotach-gospodarki-narodowej-w-rejestrze-regon-grudzien-2022,4,65.html dostęp 30.01.2023 r.
[96] https://www.coig.com.pl/inwestorzy-zagraniczni-w-polsce.php dostęp 30.01.2023 r.

latach. Najwięcej z tych spółek powstało z udziałem obywateli Ukrainy (23 259), Niemiec (8 936) i Białorusi (4 025).

Z analiz przeprowadzonych przez Centralny Ośrodek Informacji Gospodarczej wynika, iż w 2022 r. zarejestrowano 55 447 podmiotów w Rejestrze Przedsiębiorców KRS. Jest to mniej o 1,51% niż w 2021 r. Jednocześnie w 2022 r. opublikowano w Monitorze Sądowym i Gospodarczym oraz Krajowym Rejestrze Zadłużonych 360 upadłości firm.

Najwięcej w Polsce aktywnych firm z kapitałem zagranicznym posiada formę prawną spółki z ograniczoną odpowiedzialnością, procentowo jest ich 94,14%[97]. Jako główny przedmiot działalności najwięcej firm wskazało transport drogowy towarów - 4 553 spółki; roboty budowlane związane ze wznoszeniem budynków - 3 759 firm; pozostałe doradztwo - 3462 spółki; sprzedaż hurtowa - 3374 firmy. Najwięcej firm z kapitałem zagranicznym ma siedzibę w Warszawie.

W 2021 r. przedsiębiorstwa niefinansowe osiągnęły[98] 6 287,7 mld zł przychodów ogółem, wytworzyły 1 448,7 mld zł wartości dodanej, a wartość ich produkcji wyniosła 4 662,0 mld zł. Blisko połowę wartości powyższych kategorii wygenerowały jednostki duże. W stosunku do roku 2020 wartość przychodów ogółem przedsiębiorstw niefinansowych zwiększyła się o 19,6%. Ze względu na rodzaj prowadzonej działalności, 72,9% przychodów ogółem przypadało łącznie na przedsiębiorstwa przemysłowe i handlowe. Wynik finansowy brutto przedsiębiorstw niefinansowych w 2021 r. wyniósł 569,3 mld zł i był wyższy w porównaniu do roku 2020 o 210,3 mld zł (tj. o 58,6%). Najwyższy wynik finansowy brutto w 2021 r. wygenerowały przedsiębiorstwa przemysłowe (185,4 mld zł, z czego 145,2 mld zł zanotowano w podmiotach zajmujących się przetwórstwem przemysłowym), zaś pod względem lokalizacji – podmioty mające siedzibę w województwie mazowieckim (29,0% udziału).

Podatność sektora

Przestępstwo prania pieniędzy jest procederem legalizowania wartości majątkowych pochodzących z nielegalnych bądź nieujawnionych źródeł przez ich wprowadzanie do obrotu gospodarczego, powodujące zagrożenie dla jego prawidłowego funkcjonowania. Jako pewien proces rozciągnięty w czasie proceder ten obejmuje często kolejne fazy czynności, których ostatecznym celem jest asymilacja bezprawnie uzyskanych środków przez kapitał pochodzący z legalnych źródeł, a dzięki temu pojawia się możliwość legalnego skorzystania z „oczyszczonych" środków. Przestępstwo prania pieniędzy zostało uznane przez ustawodawcę za przestępstwo odrębne od przestępstwa bazowego (będącego potencjalnym źródłem bezprawnie legalizowanych korzyści), a ustawodawca opatrzył to przestępstwo surową sankcją karną, nierzadko przewyższającą zagrożenie przewidziane dla czynów zabronionych bazowych. Pranie pieniędzy stanowi samodzielny typ czynu zabronionego. Artykuł 299 kodeksu karnego penalizujący proceder prania pieniędzy umiejscowiony jest w rozdziale XXXV kodeksu, obejmującym przestępstwa przeciwko obrotowi gospodarczemu (również pierwotne ulokowanie penalizacji prania pieniędzy znalazło się w *ustawie z dnia 12 grudnia 1994 r. o ochronie obrotu gospodarczego i zmianie niektórych przepisów prawa karnego*. Choć w kodeksowych znamionach przestępstwa prania pieniędzy nie wskazuje się wprost na

[97] Tamże

[98] Analiza GUS pt. Działalność przedsiębiorstw niefinansowych w 2021 r., Warszawa 2022 r. - https://stat.gov.pl/obszary-tematyczne/podmioty-gospodarcze-wyniki-finansowe/przedsiebiorstwa-niefinansowe/dzialalnosc-przedsiebiorstw-niefinansowych-w-2021-roku,2,18.html dostęp 02.02.2023 r.

naruszenie tego dobra prawnego, to najważniejszym przedmiotem ochrony stypizowanego w art. 299 § 1 kk przestępstwa prania pieniędzy jest prawidłowość obrotu gospodarczego[99].

Jedną z najpowszechniej stosowanych metod prania pieniędzy jest tzw. blending. Polega ta metoda na zmieszaniu pieniędzy pochodzących z czynu zabronionego z dochodami legalnymi. W tym celu przestępcy zakładają działalność gospodarczą, która powinna się charakteryzować pewnymi cechami, takimi jak obrotem gotówkowym, trudnością stwierdzenia wysokości rzeczywistych przychodów, możliwością dużej dynamiki zmian w wysokości przychodów i liczby klientów. Ponadto powinna to być działalność usługowa, aby nie trzeba się było wykazać konkretną, łatwo wyliczalną produkcją. Najlepiej do tego celu nadają się restauracje, kawiarnie, punkty skupu złomu, dyskoteki i solaria. Często sam transfer środków odbywa się za pomocą rachunku bankowego osób fizycznych prowadzących działalność gospodarczą bądź innych podmiotów gospodarczych. Rachunki bankowe podmiotów gospodarczych są zasilane drobnymi i większymi kwotami, po czym zostają przekazywane na rachunki innych podmiotów, często mających swoje siedziby w tzw. rajach podatkowych. Charakter operacji finansowych na rachunkach podmiotów gospodarczych związanych z praniem pieniędzy co do zasady nie wykazuje istotnych różnic w porównaniu ze zwykłymi i legalnymi czynnościami finansowymi i handlowymi realizowanymi w obrocie gospodarczym.

Należy jednak zwrócić uwagę na fakt, że ze względu na istniejące uregulowania dotyczące obowiązków informacyjnych spółek notowanych na giełdach, w wypadku takich spółek trochę niższa jest podatność takich spółek zarówno na pranie pieniędzy, jak i na finansowanie terroryzmu. Obowiązek publikacji raportów okresowych ma swoje umocowanie w przepisach ogólnie obowiązujących w Polsce oraz regulaminach giełd. W każdym wypadku treść raportów okresowych jest szczegółowo określona, a każdy rodzaj raportu zawiera zarówno dane finansowe, jak też informacje opisowe, które przedstawiają działalność i otoczenie biznesowe danej spółki w raportowanym okresie. Raporty okresowe powinny odzwierciedlać aktualną sytuację rynkową danej spółki i być sporządzane w sposób prawdziwy, rzetelny i kompletny.

Często w wypadku działalności podmiotów gospodarczych podejrzanych o pranie pieniędzy należy brać pod uwagę fakt istnienia pokrewieństwa między członkami władz spółek prawa handlowego. Może dochodzić do transakcji między podmiotami zależnymi. Efektem może być np. działanie na szkodę spółki przez prezesa zarządu, w wyniku czego część aktywów zostanie przelana na konto spółki zależnej. Do najbardziej typowych oznak występowania ww. metody można zaliczyć:

- częste transakcje na stosunkowo niewielkie sumy między firmami należącymi do każdego z małżonków, krewnych,
- powtarzające się zasilenia rachunku bankowego tytułem „darowizna", „pożyczka", „zwrot pożyczki", „zwrot długu",
- transakcje między rachunkami osób o tych samych nazwiskach lub też między rachunkami, których analiza prowadzi do wniosku, że właściciele lub pełnomocnicy są ze sobą spokrewnieni.

Pomimo zasady, że operacje finansowe na rachunkach podmiotów gospodarczych związanych z praniem pieniędzy są podobne bądź tożsame z transakcjami w normalnym obrocie gospodarczym, to charakterystyczne dla prania pieniędzy są formy wykorzystywanych

[99] UCHWAŁA składu siedmiu sędziów Sądu Najwyższego Dnia 18 grudnia 2013 r., Sygn. akt i KZP 19/13.

dodatkowych podmiotów gospodarczych. Należą do nich spółki offshore oraz przedsiębiorstwa symulujące. Z odpowiedzi jednostek współpracujących do ankiety GIIF, przeprowadzonej w sierpniu 2021 r. dla instytucji obowiązanych i jednostek współpracujących wynika, że wśród 5 najczęściej wymienianych przez jednostki współpracujące produktów i usług oferowanych poza rynkiem finansowym jako trzecie najbardziej narażone na pranie pieniędzy zostały uznane podmioty gospodarcze z siedzibą w tzw. rajach podatkowych lub finansowych.

Spółka offshore to spółka, z reguły kapitałowa lub o takim charakterze, zarejestrowana w kraju, w którym nie prowadzi ona żadnej działalności gospodarczej. Zazwyczaj spółki offshore rejestruje się w rajach podatkowych. Rejestrację można przeprowadzić zdalnie i nie jest wymagane osobiste stawiennictwo w urzędzie. Korzyści z zarejestrowania takiej spółki to przede wszystkim poufność informacji, korzyści podatkowe oraz ochrona aktywów. Nazwiska właścicieli spółek offshore podlegają tajemnicy i są trudne do wyśledzenia. Należy zauważyć, że spółka offshore nie musi być nielegalna, jeśli jej istnienie zostanie zgłoszone odpowiednim organom państwa. W jurysdykcjach offshore opodatkowany jest zwykle wyłącznie dochód uzyskany na terytorium tego państwa. Ponieważ nie ma tam podatków od zysków kapitałowych, nieruchomości, darowizn bądź spadków, utworzenie spółki offshore z reguły pozwala na uniknięcie takich podatków. Utworzenie tego typu firmy nie napotyka większych przeszkód oprócz opłat administracyjnych, wynajęcia osób zarządzających/pełnomocników rejestrowych itp. Skoro spółki te nie prowadzą żadnej działalności gospodarczej w kraju rejestracji, nie muszą organizować zgromadzeń wspólników ani zatrudniać pracowników. Z reguły też nie ma obowiązku przedstawiania rocznych sprawozdań finansowych.

Oprócz spółek offshore formą przestępczego wykorzystania podmiotów do przestępstw bazowych, ale i prania pieniędzy są tzw. przedsiębiorstwa symulujące. Są to takie przedsiębiorstwa, w których w zamian za stosunkowo niewielkie korzyści majątkowe osoby fizyczne (figuranci, „słupy") wyrażają zgodę na wykorzystanie ich danych osobowych do zarejestrowania tych podmiotów gospodarczych, a następnie założenia rachunków bankowych, wykorzystywanych dalej do prania pieniędzy. W przypadku przedsiębiorstw symulujących istotnym elementem takiego działania jest umożliwienie dostępu do rachunków bankowych za pomocą elektronicznych kanałów łączności (w szczególności przez Internet). Zlecanie transakcji i rzeczywiste inne dyspozycje gospodarcze w imieniu firmy są faktycznie podejmowane przez osoby nieuprawnione do działania w jej imieniu. Działania przedsiębiorstw symulujących ułatwiają ukrycie danych rzeczywistych zleceniodawców transakcji i uniemożliwiają zastosowanie na czas odpowiednich środków bezpieczeństwa finansowego przez instytucje obowiązane. Szczególnie narażone na działalność przedsiębiorstw symulujących były przestępstwa paliwowe i złomowe, oszustwa typu „znikający podatnik", oszustwa karuzelowe, wystawianie „pustych faktur" czy zaciąganie kredytów i pożyczek.

Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w zakresie przedmiotowego sektora. GIIF ma ograniczone możliwości gromadzenia i analizowania informacji dotyczących tego typu usług. Istnieje duże prawdopodobieństwo, że przypadek dotyczący prania pieniędzy czy finansowania terroryzmu zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców.

Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie.

Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.

Zagrożenia w sektorze

Sektor działalności gospodarczej pod względem oceny zagrożenia praniem pieniędzy, ale też zagrożenia finansowania terroryzmu, jest sektorem potencjalnie mogącym być wykorzystanym w związku z przestępstwami źródłowymi dla prania pieniędzy oraz finansowania terroryzmu. Spółki offshore uczestniczące w obrocie gospodarczym stanowią szczególne zagrożenie z punktu widzenia zarówno prania pieniędzy, jak i finansowania terroryzmu. Ich wykorzystanie w łańcuchu transakcji powoduje, że gubiony jest (zwłaszcza w transakcjach handlu międzynarodowego) ślad transakcyjny podejrzanych transakcji. Wysoki poziom poufności czy nawet anonimowości beneficjenta rzeczywistego podmiotów, do których należą spółki offshore powoduje, że utrudnione jest bądź niemożliwe zbadanie prawdziwych relacji gospodarczych konkretnego podmiotu czy ustalenie jego prawdziwej struktury, a także celu i zamierzonego charakteru przeprowadzanych transakcji. Na uwagę z punktu widzenia zagrożenia zasługuje również fakt, że spółki offshore z reguły posiadają szybkie procedury rejestracyjne oraz stosunkowo niskie opłaty. Ich założenie i wdrożenie do obrotu gospodarczego to kwestia dni, jeśli nie godzin. Jak wskazuje doświadczenie, wiele spółek offshore było wykorzystywanych do ukrywania funduszy pochodzących z działalności przestępczej, zarówno przestępczości zorganizowanej, jak i terroryzmu.

Podobne zagrożenie z punktu widzenia prania pieniędzy i finansowania terroryzmu stanowią przedsiębiorstwa symulujące. Ukrycie danych rzeczywistych zleceniodawców transakcji powoduje, że nieprzejrzyste stają się relacje pomiędzy rzeczywistymi właścicielami legalnych środków będących przedmiotem obrotu gospodarczego, a wprowadzanymi do obrotu środkami pochodzącymi z czynu zabronionego. Wykorzystanie w obrocie gospodarczym łańcucha spółek legalnych oraz przedsiębiorstw symulujących, ich rachunków bankowych, a także pośrednictwo wielu instytucji obowiązanych w transakcjach powoduje, że bardzo utrudniona jest weryfikacja transakcji pod kątem ustalenia beneficjenta rzeczywistego przez instytucje obowiązane i uprawnione organy. Pogłębia się jeszcze taki stan w wypadku przeprowadzenia transakcji gospodarczych w obrębie kilku jurysdykcji.

Sektor działalności gospodarczej pod względem oceny zagrożenia praniem pieniędzy, ale też zagrożenia finansowania terroryzmu, jest sektorem potencjalnie mogącym być wykorzystanym w związku z przestępstwami źródłowymi dla prania pieniędzy oraz finansowania terroryzmu. Sposobów wykorzystania działalności gospodarczej do prania pieniędzy czy finansowania terroryzmu jest naprawdę wiele i mogą one być generowane w kilku obszarach.

Może to być np. prosty transfer środków z wykorzystaniem rachunków bankowych, należących do podmiotów gospodarczych. Zasilenie rachunku bankowego następuje gotówką (np. z firm usługowych. Zastosowanie znajdą tu: structuring - czyli dzielenie wpłat na rachunki bankowe poniżej wartości ponadprogowych; smurfing - czyli rozdrabnianie wpłat przez wykorzystanie wielu podstawionych osób oraz blending - czyli mieszanie pieniędzy czystych i brudnych). Druga faza prania pieniędzy to udostępnienie zgromadzonych środków właściwym beneficjentom za granicę. W takich wypadkach dla ukrycia pochodzenia środków oraz ich przeznaczenia do transferu za granicę wykorzystywane są rachunki słupów czy podmiotów symulujących. Taki schemat działania jest wysoce utrudniony w wypadku spółek giełdowych z uwagi na obowiązki informacyjne takich spółek. Publikacja raportów biznesowych odbywa się w terminach określonych prawem i wynosi np. 4 miesiące w przypadku raportów rocznych,

3 miesiące w przypadku raportów półrocznych i 60 dni w przypadku raportów kwartalnych - liczonych od końca okresu sprawozdawczego.

Jako podmiot gospodarczy piorący pieniądze może też wystąpić kantor wymiany walut, który prowadzi zarówno sprzedaż waluty, jak i jej skup. Kantor można prowadzić właściwie w każdej formie prawnej, którą przewidziano w polskich przepisach, ale prowadzenie kantoru wymaga uzyskania wpisu do rejestru działalności kantorowej prowadzonego pod nadzorem Narodowego Banku Polskiego. Dla działającej na rynku firmy założenie i prowadzenie kantoru nie jest zbyt trudne. Istnieje możliwość założenia kantoru w celu stworzenia pralni dla pieniędzy pochodzących z działalności przestępczej. Powstały kantor prowadzący działalność gospodarczą polegającą na handlu walutą, mógłby jednocześnie legalizować środki pochodzące z czynów zabronionych poprzez wykazywanie ich jako przychód z działalności.

Zorganizowane grupy przestępcze mogą prać pieniądze również z wykorzystaniem darowizn i pożyczek opisanych w Kodeksie cywilnym. Polega to na tym, że osoba prawna, która osiąga zyski z nielegalnych przedsięwzięć, chcąc je zalegalizować, porozumiewa się z innymi osobami w celu sporządzenia fikcyjnej umowy pożyczki lub darowizny, a następnie rejestruje je w urzędzie skarbowym, opłacając należny podatek. Ta metoda prania pieniędzy w formie pożyczki czy darowizny pomiędzy podmiotami często jest wykorzystywana przez podmioty, które są zarejestrowane w tzw. rajach podatkowych.

Działalność gospodarcza do prania pieniędzy może być też wykorzystana w przypadku umów faktoringu. W takim wypadku grupy przestępcze np. zakładają w większości przypadków legalne firmy, które z kolei prowadzą fikcyjną działalność sprowadzającą się do fikcyjnego fakturowania sprzedaży, która nigdy nie miała miejsca, zaciągania fikcyjnych zobowiązań stwarzających formalną podstawę do egzekwowania należności.

Z danych GIIF, dotyczących zawiadomień o podejrzeniu popełnienia przestępstwa prania pieniędzy, skierowanych przez GIIF do prokuratur w okresie styczeń 2019 r. – sierpień 2022 r. wynika, że ponad 39 % osób fizycznych prowadzących działalność gospodarczą w Polsce będących podmiotami wymienionymi w zawiadomieniach GIIF, to obywatele polscy. Największą, bo ponad 50% grupę w przedmiotowej statystyce stanowiły osoby prowadzące działalność gospodarczą bez przyporządkowanego obywatelstwa. Wśród innych narodowości zarejestrowanych w CEIDG obywatele Ukrainy stanowili 2,75%, obywatele Wietnamu stanowili 1,65%, a obywatele Łotwy 0,82%.

W ogólnej liczbie zawiadomień o podejrzeniu popełnienia przestępstwa prania pieniędzy, skierowanych przez GIIF do prokuratur w okresie styczeń 2019 r. – sierpień 2022 r. największy udział miały osoby fizyczne, których udział wynosił 48,44%. Wśród innych podmiotów, które były przedmiotem ww. zawiadomień GIIF, największy udział miały spółki z ograniczoną odpowiedzialnością - 28,78%, następnie przedsiębiorstwa zagraniczne - 9,33%, osoby fizyczne prowadzące działalność gospodarczą - 4,59%.

Działalność gospodarcza może też być jednym ze sposobów finansowania terroryzmu. Same środki finansowe mogą pochodzić zarówno z legalnej działalności, jak i z szarej strefy. Dochody przeznaczane na finansowanie terroryzmu z legalnej działalności pochodzą przede wszystkim z tych sektorów działalności gospodarczej, w których przy rozpoczęciu działalności nie występują wymagania formalne dotyczące kwalifikacji do konkretnego zawodu bądź działalności i w których rozpoczęcie działalności nie wymaga znaczących inwestycji. Ryzyko,

że firma będzie przekierowywać fundusze na wsparcie terroryzmu jest większe, gdy relacja między wykazywaną sprzedażą a faktyczną sprzedażą jest trudna do weryfikacji oraz w przypadku działalności kapitałochłonnej. Najbardziej znanym i opisanym w literaturze przypadkiem finansowania terroryzmu z dochodów pochodzących z działalności gospodarczej była międzynarodowa sieć firm należących do Osamy bin Ladena. Według raportu Europolu TESAT 2022[100] organizacje terrorystyczne i ekstremistyczne aktywnie finansują się poprzez organizacje imprez komercyjnych (jest to forma działalności gospodarczej). Choć było to utrudnione w okresie pandemii COVID-19, niektóre grupy zbierały środki właśnie w ten sposób. Dotyczyło to przede wszystkim grup prawicowych, lewicowych, etniczno-nacjonalistycznych oraz separatystycznych grup ekstremistycznych. Dochód stanowią w takim wypadku zyski ze sprzedaży biletów wstępu, akcje promocyjne i darowizny. Ocena autorów raportu TESAT 2022 jest taka, że wielkość dochodów ww. grup nie jest jednak znacząca. Ponadto ekstremiści lewicowi tradycyjnie już sprzedają książki i dedykowane czasopisma w celu zbierania funduszy. Wśród innych sposobów generowania dochodu występuje sprzedaż online towarów na platformach handlu elektronicznego (t-shirty z wizerunkami zespołów, płyty CD i gadżety nazistowskie z okresu II wojny światowej w kontekście prawicowym).

Dochody z wykonywanej pracy (zarówno legalnej, jak i nielegalnej), których przeznaczeniem jest finansowanie terroryzmu, również w Polsce są elementem postępowań prowadzonych przez ABW. Według posiadanych przez GIIF informacji ABW prowadząc działania operacyjne i analityczne odnotowała w Polsce tą metodę gromadzenia i przekazywania środków finansowych w celu wsparcia organizacji terrorystycznych.

Uśredniony poziom zagrożenia sektora działalności gospodarczej – ML – 4,0 i FT – 2,0

Uśredniony poziom podatności sektora działalności gospodarczej – ML – 2,5 i FT – 2,0

Oszacowany poziom prawdopodobieństwa dla sektora – ML – 3,10 i FT - 2,00

Poziom ryzyka jest ostatecznie określany przez kombinację zagrożenia i podatności. Macierz ryzyka określająca ten poziom ryzyka opiera się na wadze 40% (zagrożenie) + 60% (podatność) – przy założeniu, że komponent podatności ma większą zdolność określania poziomu ryzyka. Zakłada się, że poziom podatności może zwiększyć atrakcyjność, a tym samym zamiary przestępców/terrorystów, aby użyć danego modus operandi – wpływając w ten sposób ostatecznie na poziom zagrożenia. Poziom ryzyka sektora, z uwzględniem prawdopobieństwa i konsekwencji (współczynnik 2,5 dla PP i 1,5 dla FT), jest ustalany zgodnie z metodyką krajowej oceny ryzyka – aneks nr 1.

Ryzyko FT sektora działalności gospodarczej – 1,80	
1 – 1,5	Niskie
1,6 – 2,5	Średnie
2,6 – 3,5	Wysokie
3,6 – 4	Bardzo wysokie

[100] https://www.europol.europa.eu/publications-events/main-reports/tesat-report dostęp 02.02.2023 r.

Ryzyko ML sektora działalności gospodarczej – 2,86	
1 – 1,5	Niskie
1,6 – 2,5	Średnie
2,6 – 3,5	Wysokie
3,6 – 4	Bardzo wysokie

WNIOSEK 1: Poziom ryzyka wykorzystania sektora działalności gospodarczej do finansowania terroryzmu w Polsce znajduje się na poziomie średnim.

WNIOSEK 2: Poziom ryzyka wykorzystania sektora działalności gospodarczej do prania pieniędzy w Polsce znajduje się na poziomie wysokim.

Mitygacja zidentyfikowanych ryzyk:

W celu ograniczenia prawdopodobieństwa wykorzystania podmiotów prowadzących działalność gospodarczą do prania pieniędzy lub finansowania terroryzmu, zasadne jest podjęcie odpowiednich działań. Przedsiębiorcy nieujęci we wcześniejszych punktach, częściowo pozostają instytucjami obowiązanymi. Dotyczy to w szczególności przedsiębiorców prowadzących działalność w obszarze świadczenia pomocy prawnej, obsługi notarialnej, doradztwa podatkowego, czy też obrotu nieruchomościami. Ich świadomość zagrożeń związanych z praniem pieniędzy oraz finansowaniem terroryzmu jest na zróżnicowanym poziomie. Stosowanie zaproponowanych działań mitygujących powinno następować z uwzględnieniem rozpoznanego przez daną instytucję obowiązaną ryzyka.

W zakresie działalności instytucji obowiązanych zajmujących się świadczeniem szeroko pojętych usług prawnych, istnieje ryzyko związane z niechęcią instytucji obowiązanej do przełamania pewnego rodzaju lojalności przedsiębiorcy względem klienta. Ograniczenie przedmiotowego ryzyka wiąże się z koniecznością opracowania dedykowanych programów szkoleniowych dla instytucji obowiązanych z wymienionych branż.

Instytucje obowiązane zajmujące się świadczeniem szeroko pojętych usług prawnych, powinny zwracać szczególną uwagę na weryfikację źródła pochodzenia wartości majątkowych klienta.

Instytucje obowiązane powinny zwracać szczególną uwagę na stosunki gospodarcze powiązane z jurysdykcjami charakteryzującymi się wyższym ryzykiem prania pieniędzy oraz finansowania terroryzmu. Instytucje obowiązane zajmujące się świadczeniem szeroko pojętych usług prawnych, powinny analizować zasadność nawiązywania przez klientów stosunków gospodarczych z kontrahentami z państw trzecich. Instytucje obowiązane zajmujące się świadczeniem usług notarialnych powinny weryfikować źródło pochodzenia wartości majątkowych, w szczególności w przypadku przeprowadzania transakcji z kontrahentami z państw trzecich.

Instytucje obowiązane powinny położyć szczególny nacisk na uzyskanie od klienta informacji na temat celu i zamierzonego charakteru stosunków gospodarczych oraz powinny na bieżąco monitorować stosunki gospodarcze i w uzasadnionych sytuacjach występować do klienta o przekazanie informacji i dokumentów dotyczących źródła pochodzenia wartości majątkowych. W szczególności w przypadku realizowania przez instytucje obowiązane z branży notarialnej usług obejmujących zbywanie przedsiębiorstw, czy też wnoszenia wkładów do spółek kapitałowych, zasadne jest przeprowadzenie oceny gospodarczego uzasadnienia przeprowadzenia czynności. Instytucje obowiązane powinny zwracać szczególną uwagę na pozyskanie odpowiednich, aktualnych informacji o kliencie, a w trakcie stosunków gospodarczych również o transakcjach przeprowadzanych na rzecz klienta oraz przez klienta. Instytucje obowiązane powinny podejmować działania wzmacniające poziom świadomości narażenia na przestępstwo prania pieniędzy oraz finansowania terroryzmu, jak również podnoszące poziom wyszkolenia pracowników w analizie sygnałów ostrzegawczych wynikających z transakcji podejrzanych. Instytucje obowiązane zajmujące się obsługą księgową, czy też doradztwem podatkowym, powinny zwracać uwagę na identyfikowanie granic pomiędzy racjonalną optymalizacją kosztów przez klientów, a stanowiącym przestępstwo wyłudzeniem podatku, jak również późniejszymi działaniami stanowiącymi pranie pieniędzy uzyskanych poprzez wyłudzenia podatkowe.

Zalecane jest rozwijanie zaawansowanych narzędzi i systemów informatycznych, wspomagających realizację celów przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu oraz wdrażanie takich rozwiązań przez podmioty dotychczas z nich niekorzystające.

Kontynuowane powinny być szkolenia dla instytucji obowiązanych, podczas których będą przekazywane teoretyczne i praktyczne wskazówki dotyczące ustalania beneficjenta rzeczywistego oraz struktury własności i kontroli klientów a także raportowania rozbieżności do organu właściwego w sprawie CRBR. Zalecane jest uczestnictwo przedstawicieli instytucji obowiązanych w szkoleniach podnoszących świadomość AML/CTF, organizowanych zarówno przez GIIF, jak i przez UKNF w ramach Programu CEDUR.

Instytucje obowiązane powinny przykładać szczególną wagę do czynników geograficznych mogących wskazywać na wyższe ryzyko prania pieniędzy czy też finansowania terroryzmu, takich jak niestabilna sytuacja polityczna czy konflikt zbrojny, czego najdobitniejszym przykładem w ostatnich latach jest wojna prowadzona przez Rosję przeciwko Ukrainie. Z uwagi na wysokie ryzyko transferowania środków pochodzących z nielegalnego handlu, przemytu ludzi, handlu bronią, czy też działań zmierzających do omijania sankcji gospodarczych, szczególnie istotne jest analizowanie przez instytucje obowiązane nie tylko danych dotyczących samych stron transakcji, ale również beneficjentów rzeczywistych, czy też faktycznych celów przeprowadzania danych transakcji.

Instytucje obowiązane powinny zwracać szczególną uwagę na podstawę przeprowadzenia danej transakcji, w szczególności w celu potwierdzenia, że transakcje są zgodne z wiedzą instytucji obowiązanej o kliencie. Dotyczy to również instytucji obowiązanych należących do sektora wyznaczonych niefinansowych przedsiębiorców i zawodów, które nie przeprowadzają danej transakcji, a świadczą usługi na rzecz klienta, w ramach których przykładowo obsługują daną transakcję pod kątem prawnym lub księgowym.

W odniesieniu do instytucji obowiązanych należących do sektora wyznaczonych niefinansowych przedsiębiorców i zawodów, zasadnym jest rozwinięcie zakresu działań

szkoleniowych, celem zwiększenia poziomu świadomości znaczenia tych instytucji dla całokształtu systemu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.

14. Obszar – Nieruchomości

Opis sektora – zawarty jest w podrozdziale 2.2 „Rynek pozafinansowy" oraz w podrozdziale 7.2.2. „Podatność rynku pozafinansowego".

Scenariusze wystąpienia ryzyka (tj. możliwe przykłady wystąpienia ryzyka) dotyczyły wykorzystania do prania pieniędzy różnych form czynności przeniesienia własności nieruchomości, form zabezpieczeń majątkowych na nieruchomości oraz wnoszenia wkładów niepieniężnych do spółek, a do finansowania terroryzmu dotyczyły wykorzystania sprzedaży nieruchomości oraz wynajmu posiadanych nieruchomości. Opis scenariuszy znajduje się poniżej.

Pranie pieniędzy

Tabela 61

Rodzaj wykorzystanych usług, produktów finansowych	Przeniesienie własności nieruchomości
Ogólny opis ryzyka	Wykorzystanie różnych form czynności przeniesienia własności nieruchomości do prania pieniędzy
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Zakup przez spółkę środków trwałych zabezpieczony został wpisem do hipoteki nieruchomości. Ponieważ spółka była spółką zależną, raty były spłacane przez spółkę matkę, należącą faktycznie do członków grupy przestępczej. W wyniku umowy pomiędzy spółkami zakupione środki trwałe zostały zostały wywiezione z Polski. 2. Podmiot dokonuje zakupu nieruchomości po cenie zaniżonej w stosunku do ceny rynkowej. Różnica kwot w stosunku do ceny rynkowej zostaje wypłacona sprzedającemu poza umową. Następnie po pewnym czasie następuje sprzedaż nieruchomości po cenie rynkowej z wykazanym zyskiem. 3. Dokonywanie transakcji kupna/sprzedaży tej samej nieruchomości w ramach operacji dokonywanych wśród grupy powiązanych osób. Zawyżone ceny nieruchomości są finansowane ze środków pochodzących z korzyści związanych z popełnieniem czynu zabronionego. Zawyżanie ceny nieruchomości staje się sposobem wprowadzania do legalnego obrotu środków pochodzących z nielegalnej działalności. 4. Kupno nieruchomości za środki pozyskane z bankowego kredytu hipotecznego. Raty kredytu są spłacane pieniędzmi pochodzącymi z nielegalnej działalności. 5. Zamiana jednej nieruchomości na kilka innych, których prawidłową wycenę trudno ustalić. Różnica wartości zamienianych nieruchomości przy następującej niedługo potem transakcji sprzedaży służy wprowadzaniu do legalnego obrotu środków pochodzących z nielegalnej działalności. 6. Nabycie nieruchomości za środki pochodzące z czynu zabronionego. Kupno/sprzedaż nieruchomości dochodzi do skutku poprzez złożenie notariuszowi przez strony transakcji nieprawdziwych oświadczeń i dokumentów, dotyczących formy przekazania środków finansowych. Zamiast wpłaty na rachunek bankowy dewelopera cała kwota bądź jej większa część została uiszczona przez kupującego gotówką pochodzącą z czynu zabronionego.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Przeniesienie własności nieruchomości odbywa się w wielu formach: sprzedaży, zamiany, darowizny, dziedziczenia czy dożywocia. Aby przeniesienie własności nieruchomości było skuteczne, potrzebny jest akt notarialny. Bez aktu notarialnego zawierana umowa nie będzie miała mocy prawnej. Sprzedaż jest zawsze odpłatną formą przeniesienia własności nieruchomości. Natomiast przez umowę zamiany każda ze stron zobowiązuje się przenieść na drugą stronę własność rzeczy w zamian za zobowiązanie się do przeniesienia własności innej rzeczy. Szczególne procedury obowiązują podczas nabywania nieruchomości od dewelopera, gdy nabywający zobowiązuje się do zakupu mieszkania jeszcze

	przed fizycznym powstaniem budynku. Sporządza się wtedy notarialnie dwie umowy (deweloperską i przyrzeczoną). Księga wieczysta jest podstawowym dowodem na istnienie prawa własności do nieruchomości. GIIF ma odpowiedni dostęp do systemu Elektronicznych Ksiąg Wieczystych. Oprócz notariusza przy czynności przeniesienia własności nieruchomości mogą być zaangażowani pośrednicy w obrocie nieruchomościami oraz adwokaci, radcowie prawni i prawnicy zagraniczni w zakresie, w jakim świadczą na rzecz klienta pomoc prawną lub czynności doradztwa podatkowego, dotyczące kupna lub sprzedaży nieruchomości. Podmioty te powinny realizować wszelkie obowiązki dotyczące przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu nałożone ustawą. Notariusze sporządzający akt notarialny dotyczący przeniesienia własności nieruchomości, pośrednicy w obrocie nieruchomościami oraz adwokaci, radcowie prawni i prawnicy zagraniczni w zakresie, w jakim świadczą na rzecz klienta pomoc prawną lub czynności doradztwa podatkowego, dotyczące kupna lub sprzedaży nieruchomości są IO. Natomiast deweloperzy sprzedający nieruchomości na rynku pierwotnym nie posiadają statusu IO. W.w IO posiadają pewną świadomość swoich obowiązków z zakresu PPP/PFT, choć wciąż ujawniane są braki w ich wypełnianiu. Poziom świadomości jest nierówny, w szczególności zależny od wielkości danego podmiotu. O zwiększony poziom świadomości notariuszy dbają Izby Notarialne. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek prania pieniędzy w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	3
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie różnych form przeniesienia własności nieruchomości w celu skutecznego prania pieniędzy jest jedną z najczęściej spotykanych metod prania pieniędzy. Jest to sposób szeroko dostępny, jego zastosowanie niewiele kosztuje i sposób ten jest postrzegany przez sprawców jako bardzo atrakcyjny. Wykorzystanie różnych form przeniesienia własności nieruchomości do prania pieniędzy nie wymaga specjalistycznej wiedzy o systemie bankowym ani szczególnych, specjalistycznych umiejętności. Istnieją wyspecjalizowane zawody, których przedstawiciele za stosunkowo niewielką kwotę pomogą w przygotowaniu transakcji przeniesienia własności nieruchomości i zapewnią odpowiednią obsługę. Ten sposób prania pieniędzy jest często wykorzystywany przez zorganizowaną przestępczość. Zorganizowane grupy przestępcze korzystają często z systemu pożyczek, kredytów, manipulują wyceną wartości majątkowych, korzystają z wehikułów korporacyjnych a także wykorzystują gotówkę w celu prania pieniędzy pochodzących z nielegalnej działalności. Niejednokrotnie zakupione nieruchomości są odbudowywane bądź remontowane za środki pochodzące z czynów zabronionych, a następnie odsprzedawane po znacznie wyższej cenie. Kreatywna księgowość pozwala zalegalizować nielegalne środki. GIIF otrzymuje informacje o wykorzystywaniu metody przeniesienia własności nieruchomości do prania pieniędzy. WNIOSEK: Wykorzystanie różnych form przeniesienia własności nieruchomości do prania pieniędzy stwarza wysokie zagrożenie prania pieniędzy.

Tabela 62

Rodzaj wykorzystanych usług, produktów finansowych	Zabezpieczenie na nieruchomości oraz wnoszenie nieruchomości jako aport do spółek
Ogólny opis ryzyka	Wykorzystanie form zabezpieczeń majątkowych na nieruchomości oraz wnoszenia wkładów niepieniężnych do spółek w celu prania pieniędzy
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Zakup przez spółkę środków trwałych zabezpieczony został kredytem i wpisem do hipoteki nieruchomości. Ponieważ spółka była spółką zależną, raty były spłacane przez spółkę dominującą, mającą siedzibę w raju podatkowym, ze środków pochodzących z działalności przestępczej. Pozyskane przez spółkę środki trwałe pochodziły już jednak z czystych środków kredytu bankowego. 2. Spółka zagraniczna z siedzibą w jednym z rajów podatkowych uzyskuje kredyty pod zabezpieczeniem na hipotece posiadanej nieruchomości inwestycyjnej. Hipoteka tej nieruchomości jest zabezpieczeniem również dla kredytów i pożyczek dla innych osób. Zyski z przestępczej działalności są transferowane za granicę na rzecz przedmiotowej firmy zagranicznej, a następnie powracają do Polski jako przelewy na rachunek tejże firmy w polskim banku lub jako wkłady inwestycyjne (np. na zakup nieruchomości). Uzyskane z banku kredyty mają walor środków pozyskanych legalnie. Natomiast spłata uzyskanych kredytów i pożyczek może być dokonywana m.in. poprzez przejęcie przez bank nieruchomości stanowiącej zabezpieczenie. 3. Zawarcie umowy przedwstępnej zobowiązującej do przeniesienia własności nieruchomości. Elementem umowy była wysoka kara umowna za odstąpienie od umowy. Ponieważ strony (członkowie zorganizowanej grupy przestępczej) są w zmowie i do realizacji umowy nie dochodzi, wypłacana kara umowna jest formą legalizacji korzyści pochodzących z czynu zabronionego. 4. Członek zorganizowanej grupy przestępczej nabywa nieruchomość po cenie odpowiadającej jej cenie rynkowej, a następnie wnosi ją aportem do spółki prawa handlowego, zawyżając jej wartość. W związku z zawyżeniem wartości nieruchomości wzrasta również wartość samej spółki. Otrzymane w związku z aportem nieruchomości do spółki udziały są sprzedawane następnie podstawionemu inwestorowi lub inwestorom.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Mając już nieruchomość można zaciągnąć kredyty bądź pożyczkę, zabezpieczając te umowy wpisem do hipoteki ustanowionej na tej nieruchomości. Uzyskane np. od banku środki finansowe mają walor legalności, uzyskane są ze znanego źródła. Natomiast same raty kredytu czy pożyczki spłacać można już środkami pochodzącymi z niekoniecznie legalnych źródeł. Dopuszczalne w wielu przypadkach są płatności gotówkowe. Hipoteka polega na możliwości zabezpieczenia oznaczonej wierzytelności na nieruchomości i obciążenia tej nieruchomości prawem, na mocy którego wierzyciel może dochodzić zaspokojenia z nieruchomości bez względu na to, czyją stała się własnością, i z pierwszeństwem przed wierzycielami osobistymi właściciela nieruchomości. Hipoteka powstaje dopiero z chwilą wpisu do księgi wieczystej – wpis ten ma więc charakter konstytutywny. Hipotekę ujawnia się w dziale IV księgi wieczystej. GIIF ma odpowiedni dostęp do systemu Elektronicznych Ksiąg Wieczystych. Sam kredyt pod hipotekę może dostać osoba pełnoletnia, która jest właścicielem lub współwłaścicielem nieruchomości, albo posiada zgodę właściciela na obciążenia hipoteką nieruchomości, która stanie się zabezpieczeniem kredytu. Hipoteką można obciążyć prawo własności nieruchomości (w tym gruntów), spółdzielcze prawo do lokalu, prawo do użytkowania wieczystego, prawo do domu jednorodzinnego (w spółdzielni mieszkaniowej). Hipoteka zabezpiecza kredyt hipoteczny do oznaczonej sumy. Jest to określona kwota pieniężna ujawniona w księdze wieczystej. Suma hipoteki to maksymalna kwota, w jakiej wierzyciel może zaspokoić swoje roszczenia z nieruchomości obciążonej hipoteką. Pożyczkę może udzielić każdy

	podmiot mający zdolność do czynności prawnych. Natomiast kredyty mogą być udzielane wyłącznie przez banki oraz SKOK-i. Banki udzielające kredytu zabezpieczonego na hipotece są IO. Nie wszystkie jednak podmioty udzielające pozyczek są IO. Banki posiadają świadomość swoich obowiązków z zakresu PPP/PFT, stosują środki bezpieczeństwa finansowego, choć wciąż ujawniane są podczas kontroli braki w tym obszarze. W związku z trwającym konfliktem wojennym na Ukrainie szczególnym wyzwaniem związanym z prawidłowym stosowaniem środków bezpieczeństwa stanowi prawidłowa identyfikacja i weryfikacja tożsamości uchodźców z Ukrainy, zainteresowanych skorzystaniem z funkcjonujących na rynku finansowym produktów. Z uwagi na trwający konflikt zbrojny utrudnione jest pozyskanie szerszego spektrum dokumentów potwierdzających tożsamość lub wiarygodność klienta. Występują poważne problemy z identyfikacją i weryfikacją osób, które albo w ogóle nie miały żadnych dokumentów, albo miały dokumenty w rodzaju paszportu wewnętrznego pisanego cyrylicą. Właściwa transkrypcja takich dokumentów na alfabet łaciński jest niezwykle utrudniona. Poza tym istniejąca bariera językowa i kulturowa pomiędzy pracownikami instytucji obowiązanych, a uchodźcami korzystającymi z rachunku bankowego utrudnia rozpoznanie nietypowych zachowań klienta, zarówno klienta pragnącego założyć np. rachunek bankowy, jak i klienta dokonującego transakcji. Bariera językowa i kulturowa w istotny sposób wpływa na prawidłowe rozpoznanie czynników zwiększonego ryzyka. Stanowi ona ten czynnik behawioralny, który utrudnia prawidłową ocenę odpowiedzi klientów-uchodźców w kwestiach problematycznych, które wymagają dodatkowych informacji czy dokumentów.. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek prania pieniędzy w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka
Poziom zagrożenia	3
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie form zabezpieczeń majątkowych na nieruchomości oraz wnoszenia wkładów niepieniężnych do spółek w celu skutecznego prania pieniędzy jest jedną z najczęściej spotykanych metod prania pieniędzy. Jest to sposób szeroko dostępny, jego zastosowanie niewiele kosztuje i sposób ten jest postrzegany przez sprawców jako bardzo atrakcyjny. Wykorzystanie form zabezpieczeń majątkowych na nieruchomości oraz wnoszenie wkładów niepieniężnych do spółek w celu prania pieniędzy nie wymaga specjalistycznej wiedzy o systemie bankowym, prawie handlowym ani szczególnych, specjalistycznych umiejętności. Istnieją wyspecjalizowane zawody, których przedstawiciele za stosunkowo niewielką kwotę pomogą w przygotowaniu wniosku kredytowego z wykorzystaniem form zabezpieczeń majątkowych na nieruchomości czy wniosków o wniesienie wkładów niepieniężnych do spółki i zapewnią odpowiednią obsługę. Ten sposób prania pieniędzy jest często wykorzystywany przez zorganizowaną przestępczość. Zorganizowane grupy przestępcze często z niego korzystają, a także do spłaty rat wykorzystują gotówkę w celu prania pieniędzy pochodzących z nielegalnej działalności. Niejednokrotnie jako przyjęty element prania pieniędzy, zabezpieczone na hipotece nieruchomości są przejmowane przez bank. GIIF otrzymuje informacje o wykorzystywaniu metody zabezpieczeń majątkowych na nieruchomości oraz wnoszenia wkładów niepieniężnych do spółek do prania pieniędzy. WNIOSEK: Wykorzystanie różnych form przeniesienia własności nieruchomości do prania pieniędzy stwarza wysokie zagrożenie prania pieniędzy.

Finansowanie terroryzmu

Tabela 63

Rodzaj wykorzystanych usług, produktów finansowych	Przeniesienie własności nieruchomości i wynajem nieruchomości
Ogólny opis ryzyka	Wykorzystanie sprzedaży nieruchomości oraz wynajmu posiadanych nieruchomości do finansowania terroryzmu.
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Należąca do spółki prowadzonej przez członków jednej z grup etnicznych nieruchomość zostaje sprzedana. Część kwoty sprzedaży poprzez zabiegi księgowe w spółce zostaje przekazana na działalność związaną z terroryzmem. 2. Członkowie jednej z grup etnicznych w Polsce za środki otrzymane z zagranicy zakupili nieruchomość, która została przeznaczona na wynajem. Dochody z wynajmu w przeważającej części są przeznaczane na rzecz organizacji terrorystycznych, działających w ojczyźnie członków tej grupy.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Przeniesienie własności nieruchomości odbywa się w formie aktu notarialnego. Bez aktu notarialnego zawierana umowa nie będzie miała mocy prawnej. Księga wieczysta jest podstawowym dowodem na istnienie prawa własności do nieruchomości. GIIF ma odpowiedni dostęp do systemu Elektronicznych Ksiąg Wieczystych. Oprócz notariusza przy czynności przeniesienia własności nieruchomości mogą być zaangażowani pośrednicy w obrocie nieruchomościami oraz adwokaci, radcowie prawni i prawnicy zagraniczni w zakresie, w jakim świadczą na rzecz klienta pomoc prawną lub czynności doradztwa podatkowego, dotyczące kupna lub sprzedaży nieruchomości. Podmioty te powinny realizować wszelkie obowiązki dotyczące przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu nałożone ustawą. Notariusze sporządzający akt notarialny dotyczący przeniesienia własności nieruchomości, pośrednicy w obrocie nieruchomościami oraz adwokaci, radcowie prawni i prawnicy zagraniczni w zakresie, w jakim świadczą na rzecz klienta pomoc prawną lub czynności doradztwa podatkowego, dotyczące kupna lub sprzedaży nieruchomości są IO. W/w IO posiadają pewną świadomość swoich obowiązków z zakresu PPP/PFT, choć wciąż ujawniane są braki w ich wypełnianiu. Poziom świadomości jest nierówny, w szczególności zależny od wielkości danego podmiotu. O zwiększony poziom świadomości notariuszy dbają Izby Notarialne. Natomiast wynajmujący nieruchomość nie musi być jego właścicielem. Wynajmującemu nie musi także przysługiwać ograniczone prawo rzeczowe do wynajmowanego lokalu. Wynajmujący nie musi być właścicielem przedmiotu najmu, ponieważ zawarcie umowy najmu nie jest rozporządzeniem prawem własności. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji w przypadku sprzedaży nieruchomości. W wypadku najmu taka wiedza jest mało dostępna. Istnieje niewielkie prawdopodobieństwo, że przypadek finansowania terroryzmu w zakresie analizowanych scenariuszy zostanie wykryty przez GIIF, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Możliwość taką mają jednak monitorujące środowiska radykalne JW. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka
Poziom zagrożenia	3

Uzasadnienie dla poziomu zagrożenia	Wykorzystanie sprzedaży własności nieruchomości oraz wynajmu posiadanych nieruchomości do finansowania terroryzmu jest jedną z metod finansowania terroryzmu. Jest to sposób szeroko dostępny, jego zastosowanie niewiele kosztuje i sposób ten jest postrzegany przez sprawców jako raczej atrakcyjny. Wykorzystanie sprzedaży własności nieruchomości bądź wynajmu posiadanych nieruchomości do finansowania terroryzmu nie wymaga specjalistycznej wiedzy o systemie bankowym czy finansowym ani szczególnych, specjalistycznych umiejętności. Istnieją wyspecjalizowane zawody, których przedstawiciele za stosunkowo niewielką kwotę pomogą w przygotowaniu transakcji przeniesienia własności nieruchomości i zapewnią odpowiednią obsługę. Ten sposób finansowania terroryzmu jest metodą często wykorzystywaną. Kreatywna księgowość pozwala ukryć przekazanie części kwoty sprzedaży nieruchomości na cele związane z finansowaniem terroryzmu. GIIF otrzymuje niewiele informacji o wykorzystywaniu tej metody przeniesienia własności nieruchomości bądź wynajmu do finansowania terroryzmu. WNIOSEK: Wykorzystanie sprzedaży własności nieruchomości oraz wynajmu posiadanych nieruchomości do finansowania terroryzmu stwarza wysokie zagrożenie.

Sektor nieruchomości jest nie tylko jednym z podstawowych rynków inwestycji dla krajowych i światowych podmiotów gospodarczych, ale sektor ten, z uwagi na swoje cechy, przyciąga również zorganizowane grupy przestępcze, które wykorzystują ten sektor do nielegalnej działalności lub do prania zysków pochodzących z przestępstwa. Sytuacja na rynku nieruchomości ma istotne znaczenie z punktu widzenia stabilności systemu finansowego państwa i jego stabilności makroekonomicznej[101]. Ważna jest sytuacja ekonomiczna oraz finansowa firm deweloperskich i budowlanych, kształtowanie się cen ofertowych i transakcyjnych na rynkach pierwotnych i wtórnych nieruchomości, sytuacja na rynku nieruchomości komercyjnych, rynku biurowym i handlowym, relacje pomiędzy cenami mieszkań a dochodami gospodarstw domowych. Działalność przestępcza ulokowana w sektorze nieruchomości może destabilizować przedmiotowy sektor, a w konsekwencji gospodarkę państwa. W niektórych krajach taka destabilizacja przyczynia się do wzrostu cen nieruchomości, czyniąc mieszkania niedostępnymi dla wielu osób, co z kolei ma wpływ na społeczeństwo i podważa praworządność.

Publikowany co roku przez NBP „Raport o sytuacji na rynku nieruchomości mieszkaniowych i komercyjnych w Polsce" w edycji za 2021 r. podał dane statystyczne dotyczące polskiego sektora nieruchomości. Zgodnie z tymi danymi szacowana wartość majątku nieruchomości mieszkaniowych w Polsce na koniec 2021 r. wyniosła ok. 5,6 bln zł, wobec 4,9 bln zł w 2020 r. Szacowana wartość nieruchomości komercyjnych stanowiła około 355 mld zł, przy 314 mld zł w 2020 r. Wartość nieruchomości mieszkaniowych na koniec 2021 r. odpowiadała ok. 215% PKB, a komercyjnych ok. 14% PKB (w 2020 r. odpowiednio 211% i 13%). Zgodnie z szacunkami NBP w 2021 r. zasób mieszkań w Polsce wynosił ok. 15,3 mln lokali. Zwiększyła się w kraju liczba mieszkań w zasobie na 1 000 ludności (wyniosła ok. 400 wobec 392 w 2020 r.) oraz przeciętna powierzchnia użytkowa mieszkania na osobę (ok. 30,0 mkw. wobec 29,2 mkw. w 2020 r.). Zmalała przeciętna liczba osób przypadająca na mieszkanie (2,50 w 2021 r. wobec 2,55 w 2020 r.). W 2021 r. oddano do użytkowania w Polsce 97,5 tys. domów jednorodzinnych jednomieszkaniowych, tj. o 18,5% więcej niż rok wcześniej. Firmy deweloperskie, zwłaszcza duże, finansowały się średnio kwartalnie w 2021 r. głównie

[101] Raport o sytuacji na rynku nieruchomości mieszkaniowych i komercyjnych w Polsce w 2021 r., NBP 2022 r.

kapitałem własnym (ok. 43%), przedpłatami klientów (ok. 20%) i zobowiązaniami wobec wykonawców (ok. 24%), natomiast kredyty stanowiły ok. 6%, a dłużne papiery wartościowe ok. 7%.

Sektor finansowy ma kluczowe znaczenie dla sektora nieruchomości, gdyż zapewnia płynność tego rynku oraz wycenę wartości nieruchomości. Z kolei, sektor finansowy ma znaczną ekspozycję na rynek nieruchomości. Na koniec 2021 r. aktywa sektora bankowego w postaci kredytów dla gospodarstw domowych na nieruchomości mieszkaniowe wyniosły ok. 38,8% kredytów ogółem (tj. wzrosły o 0,8 p.p. w porównaniu do 2020 r.) oraz stanowiły ok. 20,0% aktywów banków (tj. spadły o 0,4 p.p. w porównaniu do 2020 r.). Według danych BIK w I półroczu 2022 r. Polacy skorzystali z kredytów i pożyczek na łączną kwotę 79,8 mld zł, czyli pożyczyli o 8,7 mld złotych mniej niż w analogicznym okresie rok wcześniej. Największe spadki odnotowały kredyty hipoteczne, których sprzedano o około 30% mniej[102].

Zgodnie z polskimi przepisami przeniesienie własności nieruchomości następuje w tym samym momencie, w którym kupujący podpisuje umowę zakupu tej nieruchomości. Jednak prawo wymaga, że aby umowa przeniesienia własności nieruchomości była formalnie ważna, musi zostać zawarta w formie aktu notarialnego. Wpis do księgi wieczystej, po podpisaniu umowy, ma charakter deklaratoryjny.

Wśród instytucji obowiązanych, które działają profesjonalnie na rynku nieruchomości i rozpoznają ryzyko prania pieniędzy oraz finansowania terroryzmu związane ze stosunkami gospodarczymi lub z transakcją okazjonalną oraz oceniają poziom rozpoznanego ryzyka, działają następujące podmioty. Są to notariusze - w zakresie czynności dokonywanych w formie aktu notarialnego, obejmujących m.in. przeniesienie własności wartości majątkowej, w tym sprzedaż, zamianę lub darowiznę ruchomości lub nieruchomości; zawarcie umowy działu spadku, zniesienia współwłasności, dożywocia, renty w zamian za przeniesienie własności nieruchomości oraz o podział majątku wspólnego, […] wniesienie wkładu niepieniężnego po założeniu spółki. Są nimi również adwokaci, radcowie prawni, prawnicy zagraniczni, doradcy podatkowi w zakresie, w jakim świadczą na rzecz klienta pomoc prawną lub czynności doradztwa podatkowego dotyczące kupna lub sprzedaży nieruchomości, przedsiębiorstwa lub zorganizowanej części przedsiębiorstwa. Od dnia 31 lipca 2021 r. został przez ustawodawcę rozszerzony katalog instytucji obowiązanych poprzez zapis, że instytucją obowiązaną jest pośrednik w obrocie nieruchomościami w rozumieniu *ustawy z dnia 21 sierpnia 1997 roku o gospodarce nieruchomościami*, z wyłączeniem czynności pośrednictwa w obrocie nieruchomościami zmierzających do zawarcia umowy najmu lub dzierżawy nieruchomości lub ich części, w której miesięczny czynsz został określony w wysokości mniejszej niż równowartość 10 000 euro.

Podatność sektora

Transakcje będące transakcjami prania pieniędzy na rynku nieruchomości formalnie nie różnią się od przeprowadzanych na tym rynku transakcji w pełni legalnych. Przestępczy charakter transakcji prania pieniędzy wynika dopiero z ujawnienia celu tych transakcji oraz ujawnienia nielegalnych źródeł pochodzenia użytych w transakcji środków finansowych.

[102] https://direct.money.pl/artykuly/porady/kredyt-a-pozyczka-czym-sie-roznia,128,0,1658496 dostęp w dniu 03.09.2023 r.

Z uwagi na swoje cechy, uwzgledniające wielkość rynku (sama wartość majątku nieruchomości mieszkaniowych w Polsce na koniec 2021 r. wyniosła ok. 5,6 bln zł), międzynarodowy charakter transakcji, podział geograficzny oraz liczne czynniki kształtujące lokalną cenę nieruchomości - sektor nieruchomości jest uważany za dosyć podatny na pranie pieniędzy. Ta podatność sektora nieruchomości wynika m.in. z wysokiej nominalnej wartości przeprowadzanych na tym rynku transakcji. Wysoka wartość będących w obrocie handlowym nieruchomości sprawia, że nieruchomości są atrakcyjne dla osób bądź organizacji przestępczych próbujących ukryć duże ilości pieniędzy pochodzących z przestępstw. Na rynku nieruchomości może dochodzić do manipulacji wyceny nieruchomości. Wprowadzenie do znanego algorytmu wyceny nieruchomości w modelu statystycznym sfingowanych niektórych danych, pozwala na dowolne oszacowanie wartości nieruchomości. W ten sposób można zaniżyć szacunkową wartość nabywanej nieruchomości i nabyć tą nieruchomość taniej, niż prawdziwa wartość rynkowa. Nie oznacza to jednak w przypadku prania pieniędzy, że zbywca nieruchomości jest nieświadomy bądź oszukiwany co do faktycznej wartości nieruchomości. Po prostu rozliczenie transakcji nabycia nieruchomości ma dwa etapy. W pierwszym etapie płacona jest oficjalna zaniżona wartość nieruchomości oraz w drugim etapie cena przeniesienia własności nieruchomości jest uzupełniana np. gotówką, poza oficjalnym obiegiem, do wartości rynkowej. W ten sposób piorący pieniądze na rynku nieruchomości staje się właścicielem nieruchomości o dużo większej wartości, niż oficjalnie zapłacona cena. Dalsze dyspozycje dotyczące nieruchomości jak np. sprzedaż czy zamiana, następują już po wartościach rynkowych. W ten sposób zostają zalegalizowane wykorzystane (poza oficjalnym obiegiem) do zakupu nieruchomości środki finansowe.

Wycena wartości nieruchomości w Polsce jest sporządzana w formie operatu szacunkowego. Operat szacunkowy to opinia o wartości nieruchomości sporządzana przez licencjonowanego rzeczoznawcę majątkowego. Operat szacunkowy ma wartość dokumentu urzędowego i jest oficjalnie uwzględniany w różnych sytuacjach administracyjnych. Jego formę i treść określa „Rozporządzenie Rady Ministrów w sprawie wyceny mienia nieruchomego i sporządzania operatu szacunkowego.” Dokument ten jest ważny przez okres 12 miesięcy od daty jego sporządzenia. Operat szacunkowy zawiera informacje istotne przy dokonywaniu wyceny przez rzeczoznawcę majątkowego – opis mienia pod względem fizycznym, prawnym i funkcjonalnym. Do operatu dołącza się istotne dokumenty wykorzystane przy jego sporządzaniu. Ma formę pisemną i musi być podpisany przez sporządzającego. Operat szacunkowy może sporządzić jedynie licencjonowany rzeczoznawca majątkowy.

Na zwiększoną podatność sektora nieruchomości w zakresie prania pieniędzy oraz finansowania terroryzmu wpływa też możliwość używania w płatnościach gotówki. W wypadku płatności gotówkowych występujących przy przeniesieniu prawa własności nieruchomości w każdym wypadku zwiększa się podatność na pranie pieniędzy z uwagi na utrudnienie możliwości śledzenia źródła środków finansowych użytych w transakcji. Tym niemniej należy zauważyć, że w każdej sytuacji, gdy przedsiębiorca dokona płatności za towar (w tym wypadku nieruchomość) w formie gotówkowej lub przyjmie taką płatność w kwocie przekraczającej równowartość 10 000 euro, stanie się instytucją obowiązaną w rozumieniu *ustawy o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu*. Powstanie po jego stronie obowiązek wyznaczenia osoby odpowiedzialnej za wdrażanie obowiązków nałożonych ustawą, wykonania analizy ryzyka, wdrożenia odpowiednich procedur oraz stosowania środków bezpieczeństwa finansowego, polegających m.in. na identyfikacji klienta, beneficjenta rzeczywistego, osób zajmujących eksponowane stanowiska polityczne, a także polegających

na ocenie stosunków gospodarczych klienta. Ponadto instytucje obowiązane zobligowane zostały do przekazywania informacji o transakcjach do GIIF. Gotówka jest również wykorzystywana, gdy zakupione w celu prania pieniędzy nieruchomości są odbudowywane bądź remontowane za środki pochodzące z czynów zabronionych, a następnie odsprzedawane po znacznie wyższej cenie.

Niektóre z transakcji przeniesienia własności nieruchomości mogą mieć bardziej złożony charakter, wynikający np. z faktu, że zakupu nieruchomości dokonuje większa liczba osób bądź podmiotów. Wprowadzone elementy anonimizacyjne, utrudniające monitorowanie relacji biznesowych czy rodzinnych i służbowych podmiotów dokonujących transakcji, zwiększają podatność transakcji przeniesienia prawa własności nieruchomości na pranie pieniędzy czy finansowanie terroryzmu. Monitoring transakcji oraz sprawdzanie istnienia ewentualnych więzi kapitałowych, organizacyjnych lub personalnych pomiędzy stronami transakcji może być utrudnione, zwłaszcza w wypadku uczestnictwa w transakcji podmiotów zależnych od podmiotów z innych jurysdykcji. Instytucje obowiązane obsługujące transakcje przeniesienia własności nieruchomości w wypadku istnienia kontrahentów mają bardzo utrudnione monitorowanie stosunków gospodarczych klientów, w tym analizę transakcji przeprowadzanych w ramach stosunków gospodarczych w celu zapewnienia, że transakcje te są zgodne z wiedzą instytucji obowiązanej o kliencie, rodzaju i zakresie prowadzonej przez niego działalności oraz zgodne z ryzykiem prania pieniędzy oraz finansowania terroryzmu związanym z tym klientem.

Na podatność sektora nieruchomości do celów prania pieniędzy oraz finansowania terroryzmu mają wpływ uregulowania *ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*. Nakładają one na instytucje obowiązane uczestniczące w obsłudze transakcji przeniesienia własności nieruchomości szereg obowiązków, dotyczących stosowania środków bezpieczeństwa finansowego w obrocie nieruchomościami. Podejmowane przez te instytucje obowiązane środki bezpieczeństwa finansowego powinny być adekwatne do wielkości podmiotu i zakresu prowadzonej działalności. Wśród środków bezpieczeństwa finansowego w obszarze AML stosowanych przez pracowników instytucji obowiązanych wyróżnia się m.in. identyfikację klienta; weryfikację tożsamości klienta; identyfikację beneficjenta rzeczywistego w CRBR; monitorowanie rozbieżności między CRBR a ustaleniami instytucji obowiązanej, ustalenie struktury własności i kontroli w przypadku klienta będącego osobą prawną albo jednostką organizacyjną nieposiadającą osobowości prawnej; dokonanie oceny stosunków gospodarczych klienta; bieżące monitorowanie stosunków gospodarczych klienta; stałe monitorowanie transakcji i stosunków gospodarczych łączących instytucję obowiązaną z jego klientami.

Na podatność sektora nieruchomości do celów prania pieniędzy oraz finansowania terroryzmu wpływa też odpowiednie stosowanie podejścia opartego na ryzyku w ramach KYC. Ponieważ w niektórych jurysdykcjach możliwy jest pewien stopień anonimowości w transakcjach zakupu nieruchomości bez ujawniania tożsamości właściciela lub za pośrednictwem spółek celowych, nie jest też w niektórych jurysdykcjach wymagane dokładne ujawnienie źródła finansowania zakupu nieruchomości, to należy w Polsce przykładać wagę do stosowanych przez kontrahentów w transakcjach elementów inżynierii podatkowej i prawnej, mającej na celu ukrycie pochodzenia pieniędzy. Identyfikacja beneficjenta rzeczywistego transakcji przeniesienia prawa własności nieruchomości jest w niektórych przypadkach dosyć prosta, ale w niektórych przypadkach jest to proces niezwykle skomplikowany. Zastosowanie w

transakcjach np. wehikułów inwestycyjnych w postaci często wielopiętrowych spółek offshore, trustów czy spółek fasadowych powoduje, że pranie pieniędzy może się odbywać poprzez inwestycje w nieruchomości, stające się w takich wypadkach nośnikiem nielegalnie zdobytych środków finansowych.

Na rynku nieruchomości ważną role odgrywają banki, udzielające kredytów na zakup nieruchomości. Z punktu widzenia podatności sektora nieruchomości na pranie pieniędzy, ale także z punktu widzenia bezpieczeństwa działalności banku, jedną ze szczególnie istotnych kwestii jest rozważna polityka finansowania transakcji na rynku nieruchomości, a zwłaszcza ocena wartości zabezpieczenia na nieruchomości. W celu ograniczenia skutków potencjalnych sytuacji kryzysowych, skutecznego zarządzania przez banki ryzykiem związanym z przyjmowaniem zabezpieczeń hipotecznych ustanowionych na nieruchomościach oraz potrzeby wiarygodnej i kompletnej informacji o rynku nieruchomości, aktualnych oraz historycznych danych, które pokazywałyby zmiany zachodzące na tym rynku w ujęciu długo- i krótkookresowym, KNF wydał w marcu 2023 r. nową Rekomendację J. Rekomendacja J dotyczy dobrych praktyk w zakresie gromadzenia i przetwarzania przez banki danych o rynku nieruchomości zawartych w wewnętrznych (własnych) i zewnętrznych (międzybankowych) bazach danych, wspomagających proces zarządzania ryzykiem związanym z ekspozycjami kredytowymi zabezpieczonymi hipotecznie. Bank, dostosowując swoją działalność do Rekomendacji J, uwzględnia przepisy prawa, w szczególności *ustawy z dnia 29 sierpnia 1997 r. o listach zastawnych i bankach hipotecznych* oraz *ustawy z dnia 21 sierpnia 1997 r. o gospodarce nieruchomościami*. Rekomendacja J ma zastosowanie do wszystkich kredytów zabezpieczonych hipotecznie udzielonych od daty rozpoczęcia jej stosowania.

Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w zakresie przedmiotowego sektora. GIIF ma możliwości gromadzenia i analizowania informacji dotyczących tego typu usług. Istnieje duże prawdopodobieństwo, że przypadek dotyczący prania pieniędzy czy finansowania terroryzmu zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców.

Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie.

Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.

Zagrożenia w sektorze

Pranie pieniędzy w sektorze nieruchomości posiada zagrożenia nie tylko na poziomie krajowym, ale też i globalnym. Ponieważ ta forma prania pieniędzy nie wymaga jakiejś szczególnej wiedzy specjalistycznej, istnieją zawody obsługujące transakcje na rynku nieruchomości, koszty transakcyjne ponoszone przez kontrahentów są stosunkowo niewielkie, to zgodnie z kryminalistyczną teorią racjonalnego wyboru inwestycja na rynku nieruchomości w celu zalegalizowania pochodzenia nielegalnych środków finansowych jest niezwykle atrakcyjna. Z takich też powodów ten sposób prania pieniędzy znajduje się w kręgu zainteresowania międzynarodowych grup przestępczości zorganizowanej.

Pranie pieniędzy na rynku nieruchomości może mieć też negatywny skutek dla rynku nieruchomości konkretnego państwa, powodując jego niestabilność poprzez niekontrolowane zmiany cen nieruchomości czy materiałów budowlanych, rozwój bądź stagnację przemysłu materiałów budowlanych, zmiany aktywności gospodarczej spółek sektora budowlanego, a tym

samym ma wpływ na rozwój danego kraju. Inwestycje w nieruchomości powodują napływ środków finansowych do konkretnego kraju, co znacząco wpływa na decyzje inwestycyjne podejmowane przez potencjalnych nabywców i sprzedawców nieruchomości. Oddziałuje to też na decyzje inwestycyjne organów państwowych i samorządowych. Takie decyzje gospodarcze podejmowane w wyniku dużej ekspozycji nielegalnych środków na rynek nieruchomości, obarczone błędem inwestycyjnym, są groźne dla interesów każdego państwa.

Zagrożeniem jest tworzenie dla celów przeprowadzenia transakcji na rynku nieruchomości skomplikowanych struktur kapitałowych, które mają utrudnić, bądź nawet uniemożliwić dotarcie do ich rzeczywistych właścicieli (beneficjentów rzeczywistych). Umiędzynarodowienie tego typu struktur kapitałowych i częściowo lub całkowicie umiejscowienie ich w mało przejrzystych jurysdykcjach utrudnia ich rozpoznanie poprzez procedury KYC. W niektórych przypadkach dopiero działania wyspecjalizowanych organów nadzorczych czy organów ścigania, informacje od sygnalistów czy działania operacyjne pozwalają na ujawnienie prawdziwych dysponentów środków finansowych i wykrycie śladów prania pieniędzy na rynku nieruchomości. Takie nieprzejrzyste struktury kapitałowe wprowadzają element anonimowości w sferę transakcji na rynku nieruchomości.

Element anonimowości jako element zagrożenia w transakcjach na rynku nieruchomości wprowadza też możliwość wykorzystania gotówki w transakcjach na tym rynku. Zorganizowane grupy przestępcze na rynku nieruchomości wykorzystują dla celów prania pieniędzy gotówkę pochodzącą z nielegalnej działalności nie tylko w formie zapłaty za nieruchomość. Niejednokrotnie zakupione w celu prania pieniędzy nieruchomości są w złym stanie technicznym. Po zakupie są one odbudowywane bądź remontowane za środki pochodzące z czynów zabronionych, a następnie odsprzedawane po znacznie wyższej cenie. Uczestniczące w pracach budowlanych firmy budowlane, sklepy sprzedaży materiałów budowlanych, pracownicy budowlani – są to podmioty które chętnie przyjmują płatności w gotówce. Często część działalności tych podmiotów mieści się w szarej strefie. Kreatywna księgowość pozwala natomiast zalegalizować środki pochodzące z czynów zabronionych. Zagrożenie w sektorze nieruchomości podnosi również fakt, że wartość nieruchomości podlegających procederowi prania pieniędzy, zwłaszcza w atrakcyjnych lokalizacjach, jest niezwykle wysoka. Inwestycje w nieruchomości środków finansowych pochodzących z czynów zabronionych mogą być traktowane jako stosunkowo łatwo dostępna forma lokowania czy przechowywania dużych sum pieniędzy w formie bezpiecznego, choć czasem trudno zbywalnego aktywa.

Na ocenę zagrożenia rynku nieruchomości na pranie pieniędzy oraz finansowanie terroryzmu wpływa również brak odpowiedniego nadzoru i kontroli nad tym rynkiem. Generalnie niedostateczna jest w wypadku rynku nieruchomości typowa kontrola wykonywania przez instytucje obowiązane obowiązków w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu. Jedynie w wypadku notariuszy kontrolę taką sprawują prezesi sądów apelacyjnych. W przypadku innych zawodów kontrolę sprawują naczelnicy urzędów celno-skarbowych i GIIF.

Wykorzystanie sprzedaży nieruchomości oraz wynajmu posiadanych nieruchomości może też być jednym ze sposobów finansowania terroryzmu. Środki finansowe w takim wypadku mogą pochodzić przede wszystkim z legalnej umowy sprzedaży nieruchomości czy z legalnej umowy najmu, zawieranych przez osoby bądź inne podmioty wspierające środowiska radykalne bądź

terrorystyczne. Według posiadanych przez GIIF informacji ABW prowadząc działania operacyjne i analityczne odnotowała w Polsce przypadki inwestowania na terytorium RP środków pozyskanych przez członków i sympatyków ugrupowań terrorystycznych, w tym w powiązane z nimi podmioty gospodarcze (lub celem założenia kolejnych), z których dochody przeznaczane są następnie na daną organizację, jak również na zakup przez te osoby nieruchomości (w tym bez uzasadnienia ekonomicznego - np. w złym stanie technicznym).

Uśredniony poziom zagrożenia sektora nieruchomości – ML – 3,0 i FT – 3,0

Uśredniony poziom podatności sektora nieruchomości – ML – 2,0 i FT – 2,0

Oszacowany poziom prawdopodobieństwa dla sektora – ML – 2,40 i FT - 2,40

Poziom ryzyka jest ostatecznie określany przez kombinację zagrożenia i podatności. Macierz ryzyka określająca ten poziom ryzyka opiera się na wadze 40% (zagrożenie) + 60% (podatność) – przy założeniu, że komponent podatności ma większą zdolność określania poziomu ryzyka. Zakłada się, że poziom podatności może zwiększyć atrakcyjność, a tym samym zamiary przestępców/terrorystów, aby użyć danego modus operandi – wpływając w ten sposób ostatecznie na poziom zagrożenia. Poziom ryzyka sektora, z uwzględniem prawdopobieństwa i konsekwencji (współczynnik 2,5 dla PP i 1,5 dla FT), jest ustalany zgodnie z metodyką krajowej oceny ryzyka – aneks nr 1.

Ryzyko FT sektora nieruchomości – 2,04	
1 – 1,5	Niskie
1,6 – 2,5	Średnie
2,6 – 3,5	Wysokie
3,6 – 4	Bardzo wysokie
Ryzyko ML sektora nieruchomości – 2,44	
1 – 1,5	Niskie
1,6 – 2,5	Średnie
2,6 – 3,5	Wysokie
3,6 – 4	Bardzo wysokie

WNIOSEK 1: Poziom ryzyka wykorzystania sektora nieruchomości do finansowania terroryzmu w Polsce znajduje się na poziomie średnim.

WNIOSEK 2: Poziom ryzyka wykorzystania sektora nieruchomości do prania pieniędzy w Polsce znajduje się na poziomie średnim.

Mitygacja zidentyfikowanych ryzyk:

W celu ograniczenia prawdopodobieństwa wykorzystania sektora nieruchomości do prania pieniędzy lub finansowania terroryzmu, zasadne jest podjęcie odpowiednich działań lub zastosowanie środków mających na celu zmniejszenie ryzyka prania pieniędzy oraz finansowania terroryzmu. Dotyczy to w szczególności podmiotów obsługujących transakcje na rynku nieruchomość, będących IO. Stosowanie właściwych mitygantów w ramach procesu przeciwdziałania praniu pieniędzy jest jednym z podstawowych aspektów zapewnienia skutecznej ochrony tych instytucji przed ryzykiem prawnym, finansowym i reputacyjnym.

W sektorze nieruchomości poziom świadomości ryzyka prania pieniędzy i finansowania terroryzmu jest bardzo zróżnicowany, w szczególności zależy on od wielkości konkretnego podmiotu rynkowego oraz jego struktury. Czynniki te warunkują dostęp pracowników IO obsługujących rynek nieruchomości do nowoczesnych narzędzi informacyjnych i szkoleniowych. Powyższe wymaga większej koncentracji tych IO ukierunkowanej na weryfikację źródła pochodzenia wartości majątkowych klienta, użytych w transakcji przeniesienia własności nieruchomości oraz prawidłową identyfikację beneficjenta rzeczywistego. Podjęcie przez IO niezbędnych działań w celu weryfikacji tożsamości klienta oraz ustalenie struktury własności i kontroli w przypadku klienta będącego osobą prawną albo jednostką organizacyjną nieposiadającą osobowości prawnej jest niezbędne właściwie w każdym przypadku transakcji przeniesienia własności nieruchomości na rynku.

Instytucje obowiązane działające na rynku nieruchomości powinny zwracać szczególną uwagę w tych wypadkach, gdy z monitoringu stosunków gospodarczych klienta wynikają jego związki/powiązania gospodarcze z jurysdykcjami charakteryzującymi się wyższym ryzykiem prania pieniędzy oraz finansowania terroryzmu, a zwłaszcza gdy ma miejsce zastosowanie w transakcjach tzw. wehikułów inwestycyjnych obejmujących spółki offshore, trusty itp.

Instytucje obowiązane powinny położyć szczególny nacisk na uzyskanie od klienta informacji na temat celu i zamierzonego charakteru stosunków gospodarczych oraz powinny na bieżąco monitorować stosunki gospodarcze i w uzasadnionych sytuacjach występować do klienta o przekazanie informacji i dokumentów dotyczących źródła pochodzenia wartości majątkowych. W szczególności w przypadku realizowania przez instytucje obowiązane z branży notarialnej usług obejmujących zbywanie przedsiębiorstw (obejmujących też nieruchomości), czy też wnoszenia wkładów do spółek kapitałowych (w postaci nieruchomości), zasadne jest przeprowadzenie oceny gospodarczego uzasadnienia przeprowadzenia czynności. Instytucje obowiązane powinny zwracać szczególną uwagę na pozyskanie odpowiednich, aktualnych informacji o kliencie, a w trakcie stosunków gospodarczych również o transakcjach przeprowadzanych na rzecz klienta oraz przez klienta.

W sytuacji, gdy w sektorze nieruchomości poziom świadomości ryzyka prania pieniędzy i finansowania terroryzmu jest bardzo zróżnicowany, IO działające na tym rynku powinny podejmować wszelkie działania wzmacniające poziom tej świadomości, przede wszystkim podnosząc poziom wyszkolenia pracowników w analizie sygnałów ostrzegawczych wynikających z transakcji podejrzanych. Przeszkolenie pracowników w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu pomaga zrozumieć i identyfikować potencjalne zagrożenia znajdujące się w sektorze, którego są ważnym elementem.

Zalecane jest rozwijanie zaawansowanych narzędzi i systemów informatycznych, wspomagających realizację celów przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu oraz wdrażanie takich rozwiązań przez podmioty dotychczas z nich niekorzystające.

Na rynku nieruchomości ważne jest ustanowienie i udokumentowanie jasnych procedur przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, ustalających progi ostrzegawcze, które wskazują na konieczność dalszego badania transakcji i stosowania środków bezpieczeństwa finansowego. Szczególną wagę należy przykładać do czynników geograficznych i geopolitycznych mogących wskazywać na wyższe ryzyko prania pieniędzy czy też finansowania terroryzmu, takich jak niestabilna sytuacja polityczna w danym kraju czy konflikt zbrojny, czego najdobitniejszym przykładem w ostatnich latach jest wojna prowadzona przez Rosję przeciwko Ukrainie.

Z uwagi na fakt, że w sektorze nieruchomości poziom świadomości ryzyka prania pieniędzy i finansowania terroryzmu jest bardzo zróżnicowany, istotne jest regularne przeprowadzanie audytów i testów wewnętrznych, oceniających skuteczność stosowanych przez IO programów KYC i pozwalających identyfikować obszary wymagające poprawy.

Potwierdzam zgodność kopii z dokumentem elektronicznym:

Identyfikator dokumentu	7842598.29494334.19336329
Nazwa dokumentu	ANEKS NR 2 final_4.pdf
Tytuł dokumentu	ANEKS NR 2 final_4
Sygnatura dokumentu	IF10.033.1.2023
Data dokumentu	2023-11-27 10:38:13
Skrót dokumentu	9553E3E6FB56AE1D05F2DF67B48D85C52D5D100F
Wersja dokumentu	1.3
Data podpisu	2023-11-27
Sygnatariusz	Magdalena Rzeczkowska
Rodzaj certyfikatu	Certyfikat kwalifikowany podpisu elektronicznego
	EZD 3.116.9.9.
Data wydruku:	2023-12-04 23:09:01
Autor wydruku:	Pajewska Anna