Ministerstwo Finansów

ANEKS NR 2
SCENARIUSZE RYZYKA PRANIA PIENIĘDZY

1. Obszar - bankowość

Tabela nr 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.
Poziom podatności	2

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 daje pewne możliwości ukrycia danych rzeczywistych zleceniodawców transakcji – przy wykorzystywaniu tzw. słupów czy przedsiębiorstw symulujących do otwarcia rachunku. Zgodnie z opracowaniem Narodowego Banku Polski (NBP) p.t. *Porównanie wybranych elementów polskiego systemu płatniczego z systemami innych krajów Unii Europejskiej za 2017 r.*, liczba rachunków bankowych w Polsce wciąż rośnie (w 2017 r. wzrosła w stosunku do danych za 2016 r. o ponad o 6,6%, czyli o 4,5 mln rachunków).[1] Łączna ich liczba na 1 mieszkańca wynosi 1,9 i jest wyższa niż dla całej Unii Europejskiej (UE)[2]. Także łączna liczba transakcji zrealizowanych za pomocą kart płatniczych, czeków, poleceń zapłaty i przelewów wyniosła ponad 6,51 mld w 2017 r.[3] Przy czym w przypadku liczby poleceń przelewów na 1 mieszkańca Polska plasuje się powyżej średniej w UE, a w przypadku liczby poleceń zapłaty na 1 mieszkańca znacznie poniżej średniej w UE. 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. Posiadają świadomość swoich obowiązków z zakresu PPP/PFT.[4] Efektywnie analizują transakcje – najwięcej STR[5]/SAR[6], przekazywanych do Generalnego Inspektora Informacji Finansowej (GIIF), pochodzi od banków/oddziałów instytucji kredytowych/oddziałów banków zagranicznych (w 2017 r. było to ok. 94,9% SAR-ów od IO i ok. 97,8% STR-ów). 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 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	4
Uzasadnienie dla poziomu zagrożenia	Dokonywanie transakcji poprzez założone rachunki bankowe, zarówno rachunki firmowe jak i rachunki osób fizycznych, jest jedną z najprostszych w wykorzystaniu metod prania pieniędzy. Sposób ten jest szeroko dostępny i jego zastosowanie 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 są one omijane 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

[1] Porównanie wybranych elementów polskiego systemu płatniczego z systemami innych krajów Unii Europejskiej za 2017 r., NBP, grudzień 2018 r, s. 7, na: https://www.nbp.pl/home.aspx?f=/systemplatniczy/obrot_bezgotowkowy/obrot_bezgotowkowy.html.
[2] Tamże, s. 8.
[3] Tamże, s. 32.
[4] Jakkolwiek podczas wszystkich przeprowadzonych w 2018 r. przez Urząd Komisji Nadzoru Finansowego (UKNF) kontroli (m. in. w 12 bankach komercyjnych i 3 bankach spółdzielczych) ujawniono nieprawidłowości i uchybienia w badanych obszarach (głównie w zakresie oceny ryzyka i stosowania środków bezpieczeństwa finansowego, a także organizacji procesu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu i przekazywaniu informacji do GIIF). Natomiast GIIF podczas 4 na 5 kontroli banków przeprowadzonych w latach 2017-2018 ujawnił nieprawidłowości w wypełnianiu obowiązków dot. przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.
[5] Skrót od angielskiego pojęcia *suspicious transaction report* (tj. raport o podejrzanej transakcji).
[6] Skrót od angielskiego pojęcia *suspicious activity report* (tj. raport o podejrzanej aktywności).

	transferowania pieniędzy pochodzących z nielegalnych źródeł stwarza bardzo wysokie zagrożenie praniem pieniędzy.

Tabela nr 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	2
Uzasadnienie dla poziomu podatności	Dostęp do kredytów i pożyczek udzielanych przez banki jest prosty, jakkolwiek 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. Zgodnie z informacjami ze strony Biura Informacji Kredytowej (BIK) w 2018 r. stwierdzono wzrost udzielonych kredytów zarówno w ujęciu liczbowym, jak i w wartościowym. W 2018 r. banki oraz spółdzielcze kasy oszczędnościowo-kredytowe udzieliły łącznie 7,5 mln szt. kredytów konsumpcyjnych, tj. o 2,8% więcej niż w 2017 r. (w ujęciu wartościowym – wzrost wyniósł 6,7% w stosunku do roku poprzedniego).[7] Wzrost odnotowano także w liczbie i wartości udzielonych kredytów mieszkaniowych (odpowiednio o 10,3% i 20,1% więcej niż w 2017 r.). Niewielki spadek odnotowano jedynie w liczbie wydawanych kart kredytowych (o ok. 0,6% w stosunku do 2017 r.), jednak wartość ich limitów była o ok. 2,2% większa od wartości limitów kart kredytowych w 2017 r.[8] 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.[9] Efektywnie analizują transakcje – najwięcej STR/SAR, przekazywanych do GIIF, pochodzi od banków/oddziałów instytucji kredytowych/oddziałów banków zagranicznych (w 2017 r. było to ok. 94,9% SAR-ów od IO i ok. 97,8% STR-ów). 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.

[7] https://media.bik.pl/informacje-prasowe/420017/perspektywy-rynku-kredytowo-pozyczkowego-na-rok-2019, data odczytu 14.06.2019 r.

[8] https://media.bik.pl/publikacje/read/420072/newsletter-kredytowy-bik-grudzien-2018-r-i-podsumowanie-roku-kredytowe, data odczytu 14.06.2019 r.

[9] Jakkolwiek podczas wszystkich przeprowadzonych w 2018 r. przez UKNF kontroli (m. in. w 12 bankach komercyjnych i 3 bankach spółdzielczych) ujawniono nieprawidłowości i uchybienia w badanych obszarach (głównie w zakresie oceny ryzyka i stosowania środków bezpieczeństwa finansowego, a także organizacji procesu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu i przekazywaniu informacji do GIIF). Natomiast GIIF podczas 4 na 5 kontroli banków przeprowadzonych w latach 2017-2018 ujawnił nieprawidłowości w wypełnianiu obowiązków dot. przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.

Poziom zagrożenia	3
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie możliwości zawarcia umowy kredytowej bądź umowy pożyczki, a następnie ich spłata środkami pochodzącymi z nielegalnych źródeł jest postrzegane w Polsce jako dosyć 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 tę 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 praniem pieniędzy.

Tabela nr 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.
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[10]. 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 PPP/PFT (warto jednak pamiętać, że nie są one IO w myśl polskich przepisów, o ile nie działają one poprzez oddział ustanowiony w

[10] 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).

	Polsce). Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia[11] i analizowania informacji, jednak w dużej mierze jest w tym zakresie uzależniony od informacji uzyskanych od zagranicznych jednostek analityki finansowej. 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 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, nabywanych przez osoby fizyczne. Wymaga to od sprawców wiedzy na temat oferty zagranicznych instytucji pieniądza elektronicznego. Jakkolwiek z uwagi na relatywnie niskie limity określone w dyrektywie 2018/843 w związku z możliwością niestosowania środków bezpieczeństwa finansowego w odniesieniu do pieniądza elektronicznego, które każde z państw członkowskich UE ma obowiązek zastosować, ten sposób może wydać się sprawcom niezbyt atrakcyjny. Są informacje pochodzące głównie z zagranicy o wykorzystywaniu tego *modus operandi* do PP. WNIOSEK: Wykorzystanie kart przedpłaconych (wydawanych przez instytucje pieniądza elektronicznego z innych krajów UE) w celu utrudnienia identyfikacji sprawców prania pieniędzy jest aktualnie w Polsce na niskim poziomie zagrożenia praniem pieniędzy.

Tabela nr 4

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 w szczególności do banków ulokowanych w 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.
Poziom podatności	2
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. Zgodnie z opracowaniem NBP p.t. *Porównanie wybranych elementów*

[11] 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.

	polskiego systemu płatniczego z systemami innych krajów Unii Europejskiej za 2017 r., łączna liczba przelewów wyniosła w 2017 r. ok. 2,62 mld.[12] Przy czym w przypadku liczby poleceń przelewów na 1 mieszkańca Polska plasuje się powyżej średniej w UE. 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.[13] Efektywnie analizują transakcje – najwięcej STR/SAR, przekazywanych do GIIF, pochodzi od banków/oddziałów instytucji kredytowych/oddziałów banków zagranicznych (w 2017 r. było to ok. 94,9% SAR-ów od IO i ok. 97,8% STR-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 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.
Poziom zagrożenia	4
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie transferów do przekazywania środków finansowych do innych jurysdykcji jest jedną z najczęściej spotykanych metod prania pieniędzy (są informacje o jej stosowaniu przez przestępców). Jest to sposób szeroko dostępny, a jego zastosowanie relatywnie niewiele kosztuje. Jest postrzegany przez sprawców jako bardzo atrakcyjny. Wykorzystanie transferów do przekazywania środków finansowych do innych jurysdykcji nie wymaga specjalistycznej wiedzy ani umiejętności. Wykorzystywany często przez zorganizowaną przestępczość czasami może wiązać się ze skorumpowaniem pojedynczego pracownika banku lub z kontrolowaniem działalności całej filii bądź agencji. Środki bezpieczeństwa finansowego stosowane przez banki są omijane w tym *modus operandi* przez korupcje urzędników bankowych bądź fałszerstwo dokumentów, których weryfikacja dla banku jest utrudniona, np. faktur. WNIOSEK: Wykorzystanie transferów do przekazywania środków finansowych do innych jurysdykcji stwarza bardzo wysokie zagrożenie praniem pieniędzy.

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

Tabela nr 5

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.

[12] Porównanie wybranych elementów polskiego systemu płatniczego z systemami innych krajów Unii Europejskiej za 2017 r., NBP, grudzień 2018 r, s. 32, na: https://www.nbp.pl/home.aspx?f=/systemplatniczy/obrot_bezgotowkowy/obrot_bezgotowkowy.html.

[13] Jakkolwiek podczas wszystkich przeprowadzonych w 2018 r. przez UKNF kontroli (m. in. w 12 bankach komercyjnych i 3 bankach spółdzielczych) ujawniono nieprawidłowości i uchybienia w badanych obszarach (głównie w zakresie oceny ryzyka i stosowania środków bezpieczeństwa finansowego, a także organizacji procesu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu i przekazywaniu informacji do GIIF). Natomiast GIIF podczas 4 na 5 kontroli banków przeprowadzonych w latach 2017-2018 ujawnił nieprawidłowości w wypełnianiu obowiązków dot. przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.

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. IO z obszaru usług płatniczych Te podmioty posiadają pewną świadomość swoich obowiązków z zakresu PPP/PFT, choć wciąż ujawniane są braki w ich wypełnianiu.[14] Przekazują one relatywnie niewiele SAR-ów i STR-ów (w 2017 r. - 0,58% wszystkich otrzymanych SAR-ów od IO i 0,034% wszystkich otrzymanych STR-ów). 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	4
Uzasadnienie dla poziomu zagrożenia	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 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 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 praniem pieniędzy.

Tabela nr 6

Rodzaj wykorzystanych usług, produktów finansowych	internetowe usługi płatnicze
Ogólny opis ryzyka	korzystanie z internetowych usług płatniczych przez sprawców w celu transferowania środków pochodzących z nielegalnej działalności

[14] Podczas wszystkich przeprowadzonych w 2018 r. przez UKNF kontroli (m. in. w 16 krajowych instytucjach płatniczych) ujawniono nieprawidłowości i uchybienia w badanych obszarach (głównie w zakresie oceny ryzyka i stosowania środków bezpieczeństwa finansowego, a także organizacji procesu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu i przekazywaniu informacji do GIIF). Natomiast GIIF podczas wszystkich 3 kontroli instytucji płatniczych, przeprowadzonych w latach 2017-2018, ujawnił nieprawidłowości w wypełnianiu obowiązków dot. przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.

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. 3. Na rzecz klienta instytucji płatniczej wpływają stosunkowo drobne wpłaty od osób fizycznych i prawnych, będące wynikiem popełnienia przestępstwa bazowego dla prania pieniędzy. Wpłaty są realizowane zarówno w formie transakcji gotówkowych, jak i transferów bezgotówkowych, zlecanych za pośrednictwem instytucji obowiązanych, które umożliwiają przyjmowanie środków pieniężnych na rzecz ww. klienta instytucji płatniczej. Przekazane środki finansowe są następnie zbiorczo transferowane na rachunek bankowy lub płatniczy w innej instytucji finansowej, należący do ww. klienta instytucji płatniczej.
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 (np. jeden z portali daje możliwość realizowania 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. 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.[15] Przekazują one relatywnie niewiele SAR-ów i STR-ów (w 2017 r. - 0,58% wszystkich otrzymanych SAR-ów od IO i 0,034% wszystkich otrzymanych STR-ów). 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 części zakresowi analizowanego ryzyka.
Poziom zagrożenia	3
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 i inne organy zetknęły się w ramach realizacji swoich zadań ustawowych. Możliwe jest m.in. wprowadzenie rozdrobnionych wartości środków pieniężnych pochodzących z przestępstwa (w formie gotówkowej lub

[15] Podczas wszystkich przeprowadzonych w 2018 r. przez UKNF kontroli (m. in. w 16 krajowych instytucjach płatniczych) ujawniono nieprawidłowości i uchybienia w badanych obszarach (głównie w zakresie oceny ryzyka i stosowania środków bezpieczeństwa finansowego, a także organizacji procesu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu i przekazywaniu informacji do GIIF). Natomiast GIIF podczas wszystkich 3 kontroli instytucji płatniczych, przeprowadzonych w latach 2017-2018, ujawnił nieprawidłowości w wypełnianiu obowiązków dot. przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.

	bezgotówkowej), a następnie ich zbiorczy transfer za pośrednictwem instytucji płatniczej na docelowy rachunek bankowy lub płatniczy. Zbyt duży wolumen obrotów może zwrócić uwagę. Istnieją też limity łącznej wartości transakcji realizowanych w określonym czasie. Mogą występować też trudności w kontaktach z operatorem w razie nieprawidłowości. Warto jednak zwrócić uwagę, że liberalizacja przepisów wprowadzanych na podstawie dyrektywy 2015/2366[16] dopuszcza coraz szerszy wachlarz usług możliwych do świadczenia przez instytucje płatnicze oraz relatywnie niskie wymogi prowadzenia działalności, umożliwiając założenie instytucji płatniczej (zwłaszcza małej instytucji płatniczej) bez zbędnych nakładów finansowych, co może ułatwić działalność przestępcom. Ten *modus operandi* wymaga planowania, wiedzy i umiejętności na średnim poziomie zaawansowania. Wydaje się jednak, że może być on postrzegany przez sprawców jako coraz bardziej atrakcyjny. GIIF posiada informacje o wykorzystywanie tej metody do prania pieniędzy. WNIOSEK: Wykorzystywanie internetowych usług płatniczych stwarza wysokie zagrożenie praniem pieniędzy.

Tabela nr 7

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.
Poziom podatności	4
Uzasadnienie dla poziomu podatności	Usługi systemów typu Hawala znacznie ułatwiają dokonywanie szybkich i anonimowych transakcji. 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 PP w zakresie analizowanego ryzyka nie zostanie wykryty. 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

[16] Tj. *dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE* (Dz. Urz. L nr 337 z 23.12.2015 r., s. 35).

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 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/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 praniem pieniędzy.

3. Obszar – ubezpieczenia

Tabela nr 8

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)	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.
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 (w 2017 r. było to 0,12% wszystkich SAR-ów od IO i 0,16% wszystkich STR-ów). 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 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. W wypadku tego *modus operandi* potrzebne jest planowanie, wiedza i umiejętności do jego zastosowania. Wymaga przygotowania i aktualizowania dokumentacji na potrzeby ubezpieczenia. WNIOSEK: Wykorzystanie możliwości oferowanych przez ubezpieczenia na życie powiązane z funduszem inwestycyjnym do legitymizowania środków z przestępczej działalności stwarza średnie zagrożenie praniem pieniędzy.

4. Obszar – inne instytucje finansowe

Tabela nr 9

Rodzaj wykorzystanych usług, produktów finansowych	usługi na rynku walutowym FOREX
Ogólny opis ryzyka	wykorzystanie firmy brokerskiej działającej na rynku FOREX jako *market marker* do legitymizowania środków pochodzących z nielegalnych źródeł.
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	Firma działająca legalnie na rynku FOREX jako broker i *market maker*[17], jest kontrolowana przez osoby powiązane z przestępcami, którzy potajemnie finansują jej działalność. Przestępcy zakładają konta na platformie transakcyjnej prowadzonej przez tę 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.
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 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.[18] Relatywnie niewiele informacji o podejrzanych transakcjach/podejrzanej działalności jest przekazywanych przez domy maklerskie (w 2017 r. było to 0,49% wszystkich SAR-ów od IO i 0,42% wszystkich STR-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 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

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

[18] Podczas wszystkich przeprowadzonych w 2018 r. przez UKNF kontroli (m. in. w 6 domach/biurach maklerskich) ujawniono nieprawidłowości i uchybienia w badanych obszarach (głównie w zakresie oceny ryzyka i stosowania środków bezpieczeństwa finansowego, a także organizacji procesu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu i przekazywaniu informacji do GIIF). Natomiast GIIF podczas 1 kontroli domu maklerskiego, przeprowadzonej w 2017 r., ujawnił nieprawidłowości w wypełnianiu obowiązków dot. przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.

	analizowanego ryzyka.
Poziom zagrożenia	2
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. 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 praniem pieniędzy.

Tabela nr 10

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.[19] Relatywnie niewiele informacji o podejrzanych transakcjach/podejrzanej działalności jest przekazywanych przez TFI/FI (w 2017 r. było to 0% wszystkich SAR-ów od IO i 0,09% wszystkich STR-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 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.
Poziom zagrożenia	2
Uzasadnienie dla poziomu	Ponieważ fundusze inwestycyjne różnią się między sobą poziomem ryzyka i

[19] Podczas wszystkich 3 przeprowadzonych przez GIIF kontroli towarzystw funduszy inwestycyjnych, przeprowadzonych w latach 2017-2018, ujawnił nieprawidłowości w wypełnianiu obowiązków dot. przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.

zagrożenia	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 praniem pieniędzy.

Tabela nr 11

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.[20] Relatywnie niewiele informacji o podejrzanych transakcjach/podejrzanej działalności jest przekazywanych przez domy maklerskie (w 2017 r. było to 0,49% wszystkich SAR-ów od IO i 0,42% wszystkich STR-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 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

[20] Podczas wszystkich przeprowadzonych w 2018 r. przez UKNF kontroli (m. in. w 6 domach/biurach maklerskich) ujawniono nieprawidłowości i uchybienia w badanych obszarach (głównie w zakresie oceny ryzyka i stosowania środków bezpieczeństwa finansowego, a także organizacji procesu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu i przekazywaniu informacji do GIIF). Natomiast GIIF podczas 1 kontroli domu maklerskiego, przeprowadzonej w 2017 r., ujawnił nieprawidłowości w wypełnianiu obowiązków dot. przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.

	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 specjalistycznej wiedzy, umiejętności i planowania. 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 praniem pieniędzy.

5. Obszar – wymiana walut

Tabela nr 12

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 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. Wszystkie podmioty oferujące te usługi są IO. Posiadają one świadomość swoich obowiązków z zakresu PPP/PFT.[21] Relatywnie mało informacji o podejrzanych transakcjach/podejrzanej działalności przekazywanych jest przez podmioty zajmujące się wymianą walut[22] (w 2017 r. było to ok. 0,03% wszystkich SAR-ów od IO i ok. 0,0064% wszystkich STR-ów, co oznacza spadek w stosunku do danych za 2016 r., kiedy było to ok. 0,64% wszystkich SAR-ów i ok. 7,66% wszystkich STR-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 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 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 praniem pieniędzy.

Tabela nr 13

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 ryzyka)	Wymiana banknotów EUR o niskich nominałach na banknoty o nominale 500 EUR[23] w celu zmniejszenia objętości przenoszonych środków pieniężnych.
Poziom podatności	2

[21] W kontroli prowadzonych przez NBP udział przedsiębiorców prowadzących działalności kantorową, u których wykryto nieprawidłowości w zakresie realizacji obowiązków dotyczących PPP/PFT, w stosunku do wszystkich skontrolowanych przedsiębiorców prowadzących działalność kantorową był relatywnie niewielki, w 2018 r. wyniósł on 4,87%, w 2017 r. – 4,14%. Natomiast w przypadku wszystkich 3 kontroli przeprowadzonych przez GIIF w 2017 r. w IO zajmujących się wymianą walut, wykryto pewne nieprawidłowości.

[22] Abstrahując od usług świadczonych przez banki.

[23] W dniu 4 maja 2016 r. Europejski Bank Centralny podjął decyzje o zaprzestaniu wydawania banknotów o nominale 500 EUR. Większość krajowych banków centralnych strefy euro wydawały je do stycznia 2019 r., natomiast Deutsche Bundesbank i Österreichische Nationalbank – do kwietnia 2019 r. Banknoty wydane do tego czasu pozostają w obiegu.

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.[24] Relatywnie mało informacji o podejrzanych transakcjach/podejrzanej działalności przekazywanych jest przez podmioty zajmujące się wymianą walut[25] (w 2017 r. było to ok. 0,03% wszystkich SAR-ów od IO i ok. 0,0064% wszystkich STR-ów, co oznacza spadek w stosunku do danych za 2016 r., kiedy było to ok. 0,64% wszystkich SAR-ów i ok. 7,66% wszystkich STR-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 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 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 praniem pieniędzy.

Tabela nr 14

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)	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.
Poziom podatności	3

[24] W kontroli prowadzonych przez NBP udział przedsiębiorców prowadzących działalności kantorową, u których wykryto nieprawidłowości w zakresie realizacji obowiązków dotyczących PPP/PFT, w stosunku do wszystkich skontrolowanych przedsiębiorców prowadzących działalność kantorową był relatywnie niewielki, w 2018 r. wyniósł on 4,87%, w 2017 r. – 4,14%. Natomiast w przypadku wszystkich 3 kontroli przeprowadzonych przez GIIF w 2017 r. w IO zajmujących się wymianą walut, wykryto pewne nieprawidłowości.

[25] Abstrahując od usług świadczonych przez banki.

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 bezgotówkowo. Wszystkie podmioty oferujące te usługi są IO. Posiadają one pewną świadomość swoich obowiązków z zakresu PPP/PFT.[26] Relatywnie mało informacji o podejrzanych transakcjach/podejrzanej działalności przekazywanych jest przez podmioty zajmujące się wymianą walut[27] (w 2017 r. było to ok. 0,03% wszystkich SAR-ów od IO i ok. 0,0064% wszystkich STR-ów, co oznacza spadek w stosunku do danych za 2016 r., kiedy było to ok. 0,64% wszystkich SAR-ów i ok. 7,66% wszystkich STR-ów). 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 części zakresowi analizowanego ryzyka.[28]
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 jedną z metod prania pieniędzy. Według szacunków dostępnych w Internecie, w I półroczu 2017 r. ok. 35% transakcji wymiany walut odbywało się w sieci.[29] Dynamicznie wzrasta wolumen obrotów kantorów internetowych, a pojedyncze transakcje sięgają już nawet kilku milionów złotych. Bezgotówkowa wymiana waluty połączona z transferem środków stosunkowo niewiele kosztuje i jako *modus operandi* może być jest postrzegana przez sprawców jako atrakcyjny i szeroko dostępny sposób 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). 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 praniem pieniędzy.

6. Obszar – waluty wirtualne

Tabela nr 15

Rodzaj wykorzystanych usług,	zdecentralizowane i wymienialne waluty wirtualne (tzw. kryptowaluty)

[26] W przypadku wszystkich 3 kontroli przeprowadzonych przez GIIF w 2017 r. w IO zajmujących się wymianą walut, wykryto pewne nieprawidłowości.

[27] Abstrahując od usług świadczonych przez banki.

[28] 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.

[29] Polacy wymieniają waluty w Internecie. Raport - trendy w wymianie walut pierwsze półrocze 2017 r., Xchanger i Fintek.pl, 2017 r., s. 2, na: https://fintek.pl/najnowszy-raport-kantorach-internetowych-polsce/.

produktów finansowych	
Ogólny opis ryzyka	wykorzystanie kryptowalut do transferowania wartości pochodzących z nielegalnych źródeł
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Wykorzystywanie kryptowalut (np. Bitcoinów) 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 (np. Monero) 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*.
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 PP 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[30] 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 pewne informacje o możliwości wykorzystywania kryptowalut do transferowania wartości majątkowych pochodzących z nielegalnych źródeł. WNIOSEK: Wykorzystanie kryptowalut do transferowania wartości majątkowych pochodzących z nielegalnych źródeł stwarza wysokie zagrożenie praniem pieniędzy.

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

Tabela nr 16

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 (np. *Webmoney*, *Perfectmoney*) w jednym z internetowych kantorów 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 na zagraniczny rachunek bankowy.
Poziom podatności	3
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 PP 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	2
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 jednak tylko jednostkowe 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 średnie zagrożenie praniem pieniędzy.

7. Obszar - usługi telekomunikacyjne powiązane z płatnościami mobilnymi

Tabela nr 17

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 możliwość gromadzenia i analizowania informacji dot. tego typu usług. Istnieje prawdopodobieństwo, że przypadek PP 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 legitymizowania środków z przestępczej działalności 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 ryzykowny. 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. 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 praniem pieniędzy.

8. Obszar – fizyczny przewóz wartości majątkowych przez granicę

Tabela nr 18

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

	nieznacznie 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 może nie zostać rozpoznane przez organy administracji publicznej na granicy. 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). 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.
Poziom zagrożenia	4
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie osób fizycznych do przewozu pieniędzy pochodzących z nielegalnych źródeł poprzez granice państwowe jest jedną z najczęściej spotykanych metod prania pieniędzy. Jest to sposób szeroko dostępny, jego zastosowanie relatywnie niewiele kosztuje i jest postrzegany przez sprawców jako bardzo atrakcyjny. Wykorzystanie osób fizycznych do przewozu pieniędzy pochodzących z nielegalnych źródeł poprzez granice państwowe nie wymaga posiadania specjalistycznej wiedzy ani umiejętności, a zapewnia anonimowość dla grupy przestępczej, która organizuje proceder. Metoda jest wykorzystywana często przez zorganizowaną przestępczość, może wiązać się z korupcją wśród funkcjonariuszy służb granicznych. GIIF otrzymywał informacje, zwłaszcza od jednostek współpracujących, o możliwości wykorzystania tej metody do prania pieniędzy. WNIOSEK: Wykorzystanie osób fizycznych do przewozu pieniędzy pochodzących z nielegalnych źródeł poprzez granice państwowe stwarza bardzo wysokie zagrożenie praniem pieniędzy.

Tabela nr 19

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. 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 PP 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 nielegalne wykorzystanie tych usług do przekazywania pieniędzy pochodzących z nielegalnych źródeł. W celu ukrycia beneficjenta rzeczywistego częstokroć wykorzystywane są słupy. 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 praniem pieniędzy.

9. Obszar – gry hazardowe

Tabela nr 20

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. Przestępca wpłaca środki (wykorzystując kryptowaluty lub pieniądze zgromadzone już na rachunku bankowym, kontrolowanym przez siebie) na odpowiedni rachunek powiązany z platformą hazardową. Środki przekazywane są z powrotem do omawianego klienta platformy pod postacią "wygranej".
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. 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*. Płatności w nim można dokonywać jedynie poprzez przelewy online lub BLIKIEM. 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.[31] Relatywnie niewiele – w porównaniu z innymi IO – informacji o podejrzanych transakcjach/podejrzanej działalności przekazywanych jest przez podmioty prowadzące działalność w zakresie gier hazardowych (w 2017 r. było to 0,00% wszystkich SAR-ów od IO i 0,008% wszystkich STR-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 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.
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 sieć Internet, z wyjątkiem zakładów wzajemnych i loterii promocyjnych jest objęte monopolem państwa. Od grudnia 2018 r. działa jedno legalne kasyno gier *online*. Przepisy prawne zakazują zarówno urządzania nielegalnych gier hazardowych przez sieć Internet przez podmioty nieuprawnione, jak i uczestniczenie w tych grach. Pomimo zakazu GIIF jednak otrzymywał nieliczne informacje o możliwości wykorzystywania takiego *modus operandi*, ale ten sposób, z uwagi na uwarunkowania prawne, jest postrzegany 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*. Nie jest to też sposób tani. WNIOSEK: Wykorzystanie internetowych gier hazardowych do prania środków pochodzących z nielegalnych źródeł stwarza średnie zagrożenie praniem pieniędzy.

Tabela nr 21

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

[31] W latach 2017-2018 w 6 na 10 kontrolach przeprowadzonych przez GIIF w podmiotach oferujących gry hazardowe stwierdzono nieprawidłowości w zakresie wypełniania obowiązków w obszarze przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.

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 łatwe jest ukrycie danych identyfikacyjnych nielegalnego gracza, zwłaszcza w przypadku korzystania z internetowych platform płatniczych. Istnieje możliwość realizacji transakcji o charakterze międzynarodowym, szczególnie w przypadku dokonywania transakcji finansowych, w przypadku gdy rachunki podmiotu prowadzącego internetowe gry hazardowe są ulokowane za granicą. Z szacunków Ministerstwa Finansów wynika, iż „szara strefa" w sektorze internetowych zakładów wzajemnych w 2018 r. wyniosła ok. 51%.[32] 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.[33] Relatywnie niewiele – w porównaniu z innymi IO – informacji o podejrzanych transakcjach/podejrzanej działalności przekazywanych jest przez podmioty prowadzące działalność w zakresie gier hazardowych (w 2017 r. było to 0,00% wszystkich SAR-ów od IO i 0,008% wszystkich STR-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 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. Obecnie dyskutowane są propozycje nowelizacji Kodeksu karnego skarbowego, które powinny zmniejszyć udział szarej strefy w rynku. Zmiany dotyczą wprowadzenia sankcji karnoskarbowych dla operatorów usług finansowych, którzy pośredniczą w transferowaniu środków pieniężnych od polskich graczy do nieposiadających zezwolenia Ministra Finansów bukmacherów.[34]
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 nielegalne wpływają na wyniki obstawianych przez nich zdarzeń, np. wydarzeń sportowych (bądź innych obstawianych zdarzeń). W celu ukrycia beneficjenta rzeczywistego częstokroć wykorzystywane są też „słupy". 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 praniem pieniędzy.

[32] https://www.senat.gov.pl/download/gfx/senat/pl/senatoswiadczenia/2045/09_071_2053_1_odp.pdf, data odczytu 24.06.2019 r.
[33] W latach 2017-2018 w 6 na 10 kontrolach przeprowadzonych przez GIIF w podmiotach oferujących gry hazardowe stwierdzono nieprawidłowości w zakresie wypełniania obowiązków w obszarze przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.
[34] https://gazetalubuska.pl/drobne-zmiany-w-kodeksie-karnym-skarbowym-to-miliardy-dla-budzetu-panstwa/ar/13900516, dostęp 21.06.2019 r.

Tabela nr 22

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 musza 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 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.[35] Relatywnie niewiele – w porównaniu z innymi IO – informacji o podejrzanych transakcjach/podejrzanej działalności przekazywanych jest przez podmioty prowadzące działalność w zakresie gier hazardowych (w 2017 r. było to 0,00% wszystkich SAR-ów od IO i 0,008% wszystkich STR-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 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.
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. 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 praniem pieniędzy.

[35] W latach 2017-2018 w 6 na 10 kontrolach przeprowadzonych przez GIIF w podmiotach oferujących gry hazardowe stwierdzono nieprawidłowości w zakresie wypełniania obowiązków w obszarze przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.

Tabela nr 23

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 legalnie gry hazardowe są IO. Posiadają pewną świadomość swoich obowiązków z zakresu PPP/PFT, choć wciąż ujawniane są braki w ich wypełnianiu.[36] Relatywnie niewiele – w porównaniu z innymi IO – informacji o podejrzanych transakcjach/podejrzanej działalności przekazywanych jest przez podmioty prowadzące działalność w zakresie gier hazardowych (w 2017 r. było to 0,00% wszystkich SAR-ów od IO i 0,008% wszystkich STR-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 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
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. 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 praniem pieniędzy.

10. Obszar – organizacje typu *non-profit*

Tabela nr 24

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)	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.
Poziom podatności	3

[36] W latach 2017-2018 w 6 na 10 kontrolach przeprowadzonych przez GIIF w podmiotach oferujących gry hazardowe stwierdzono nieprawidłowości w zakresie wypełniania obowiązków w obszarze przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.

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.[37] Nie przekazują lub przekazują relatywnie mało informacji o podejrzanych transakcjach/podejrzanej działalności do GIIF (w 2017 r.[38] nie było żadnych STR-ów lub SAR-ów od nich). 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.
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. WNIOSEK: Zakładanie fundacji i stowarzyszeń by przekazywać poprzez nie środki pochodzące z nielegalnych źródeł stanowi wysokie zagrożenie praniem pieniędzy.

11. Obszar – finansowanie społecznościowe

Tabela nr 25

Rodzaj wykorzystanych usług, produktów finansowych	finansowanie społecznościowe
Ogólny opis ryzyka	organizowanie akcji *crowdfundingowej* w celu legitymizowania posiadanych lub

[37] W latach 2017-2018 w 3 na 3 kontrole przeprowadzone przez GIIF w fundacjach stwierdzono nieprawidłowości w zakresie wypełniania obowiązków w obszarze przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.

[38] W tamtym czasie IO były wszystkie fundacje, bez względu na przyjmowanie lub dokonywanie płatności w gotówce, a także stowarzyszenia, posiadające osobowość prawną, przyjmujące płatności w gotówce o wartości równej lub przekraczającej równowartość 15 tys. EUR, również w drodze więcej niż jednej operacji

	przekazywanych środków pieniężnych
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	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.
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. 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 PP 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	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 nie posiada informacji o możliwości wykorzystania tej metody do prania pieniędzy, z wyjątkiem pochodzących od zagranicznych partnerów (w szczególności zawartych w ponadnarodowej ocenie ryzyka prania pieniędzy oraz finansowania terroryzmu, przygotowanej w 2017 r. przez Komisję Europejską). WNIOSEK: Wykorzystanie mechanizmu crowdfundingu stwarza średnie zagrożenie praniem pieniędzy.

12. Obszar - handel dobrami o wysokiej wartości

Tabela nr 26

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.
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. 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 w Polsce działalnością reglamentowaną prawnie. 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.
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. W uzasadnieniu, dołączonym w 2018 r. do ówczesnego projektu *ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu*, wskazano, że ryzyko prania pieniędzy lub finansowania terroryzmu związane z działalnością podmiotów prowadzących działalność w zakresie obrotu metalami lub kamieniami szlachetnymi i półszlachetnymi dotyczy przede wszystkim transakcji gotówkowych. 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 praniem pieniędzy.

Tabela nr 27

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)	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.
Poziom podatności	3
Uzasadnienie dla poziomu podatności	Kupno/sprzedaż antyków czy dzieł sztuki są relatywnie łatwe. Istnieje wiele firm handlujących tego typu towarami, na podstawie przepisów *ustawy - Prawo przedsiębiorców* (domy aukcyjne, antykwariaty). Łatwo jest 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. Obecnie domy aukcyjne czy antykwariaty 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. 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.
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 teju metody do prania pieniędzy. WNIOSEK: Wykorzystanie mechanizmu inwestowania środków pochodzących z nielegalnych źródeł w zakup antyków i dzieł sztuki stwarza średnie zagrożenie praniem pieniędzy.

13. Obszar – obrót nieruchomościami

Tabela nr 28

Rodzaj wykorzystanych usług, produktów finansowych	kupno/sprzedaż nieruchomości
Ogólny opis ryzyka	inwestowanie środków pochodzących z nielegalnych źródeł w nieruchomości

Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Nieruchomość zakupiona za legalne lub wyprane środki po cenie rynkowej przez przestępców zostaje wniesiona aportem do nowoutworzonej spółki. Jej wartość zostaje przy tym zawyżona, a co za tym idzie wzrasta również wartość samej spółki. Potem sprawcy odsprzedają udziały w tej firmie podstawionej osobie, która w rzeczywistości płaci tylko tyle, ile wynosi cena rynkowa nieruchomości. 2. Nieruchomość zostaje zakupiona przez przestępców po zaniżonej cenie za legalne lub wyprane środki. Różnica pomiędzy ceną nabycia a ceną rynkową zostaje zapłacona sprzedawcy nieoficjalnie za pomocą środków pochodzących z nielegalnych źródeł.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Kupno/sprzedaż nieruchomości jest utrudniona przepisami wymagającymi dokonywanie takich transakcji w formie aktów notarialnych (art. 158 *Kodeksu cywilnego*). Ponadto nabywanie nieruchomości w Polsce przez cudzoziemców może być dokonywane zgodnie z dodatkowymi obostrzeniami (po uzyskaniu zezwolenia ministra właściwego do spraw wewnętrznych). Trudno ukryć dane identyfikacyjne kupującego i sprzedającego. Transakcje o charakterze międzynarodowym są możliwe w przypadku, gdy dotyczą nieruchomości położonych poza granicami kraju lub towarzyszące transakcje finansowe są realizowane za pośrednictwem rachunków prowadzonych za granicą. IO są podmioty pośredniczące w dokonywaniu transakcji (notariusze, pośrednicy w obrocie nieruchomościami). IO nie są deweloperzy sprzedający nieruchomości na rynku pierwotnym. IO z tego obszaru nie przekazują lub przekazują relatywnie mało informacji o podejrzanych transakcjach/podejrzanej działalności do GIIF (w 2017 r. nie było żadnych STR-ów lub SAR-ów od pośredników w obrocie nieruchomościami; notariusze przekazali 0,0032% wszystkich STR-ów, a wraz z adwokatami i radcami prawnymi - 0,61% wszystkich SAR-ów od 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 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.
Poziom zagrożenia	3
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie mechanizmu polegającego na inwestowaniu środków pochodzących z nielegalnych źródeł w nieruchomości może być postrzegane w Polsce jako dosyć atrakcyjna metoda prania pieniędzy. Zawyżanie lub zaniżanie wartości nieruchomości w transakcjach prowadzonych między powiązanymi ze sobą osobami czy przedsiębiorstwami i wykorzystywanie różnicy między realną/rynkową ceną nieruchomości a ceną na fakturze/umowie (zawyżoną) stanowi dla kupującego/sprzedającego „zysk" w postaci legalizacji tej części środków. Swoboda zawierania umów i duża ilość czynników różnicujących potencjalnie wartość podobnych nieruchomości 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. WNIOSEK: inwestowanie środków pochodzących z nielegalnych źródeł w nieruchomości stanowi wysokie zagrożenie praniem pieniędzy.

14. Obszar – skrytki sejfowe

Tabela nr 29

Rodzaj wykorzystanych usług, produktów finansowych	skrytki sejfowe

Ogólny opis ryzyka	ukrywanie środków pochodzących z nielegalnych źródeł w skrytkach sejfowych
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	Wynajmowanie przez sprawców licznych skrytek sejfowych do przechowywania środków pochodzących z nielegalnych źródeł do czasu ich wprowadzenie do systemu finansowego. Systematyczne wprowadzanie w niewielkich kwotach środków przechowywanych w tych skrytkach do systemu bankowego.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Część banków świadczy usługi w zakresie udostępniania klientom skrytek sejfowych, choć nie we wszystkich filach i oddziałach są one dostępne. Teoretycznie każdy może wynająć skrytkę. Koszt wynajmu skrytki sejfowej, w porównaniu z kosztami związanymi z posiadaniem rachunku bankowego, jest relatywnie duży - przeważnie kilkaset złotych rocznie. Oprócz banków również inni przedsiębiorcy, działający na podstawie przepisów *ustawy z dnia 6 marca 2018 r. - Prawo przedsiębiorców*, oferują usługi w tym zakresie. Skrytka sejfowa umożliwia tylko przechowywanie wartości majątkowych. W celu realizacji transakcji klient musi skorzystać z innych produktów i usług oferowanych przez banki i inne instytucje finansowe. Ukrycie danych klienta jest trudne. Wszystkie podmioty oferujące wyżej wymienione produkty/usługi są IO. Banki stosują środki bezpieczeństwa finansowego. Cechują się dobrą świadomością ryzyka PP/FT. Efektywnie analizują transakcje. Najwięcej STR/SAR, przekazywanych do GIIF, pochodzi od banków/oddziałów instytucji kredytowych/oddziałów banków zagranicznych (w 2017 r. było to ok. 94,9% SAR-ów od IO i ok. 97,8% STR-ów). Jeśli chodzi o przedsiębiorców w rozumieniu *ustawy z dnia 6 marca 2018 r. - Prawo przedsiębiorców* prowadzący działalność polegającą na udostępnianiu skrytek sejfowych, oraz oddziały przedsiębiorców zagranicznych prowadzące taką działalność na terytorium Rzeczypospolitej Polskiej, to są one nową kategorią instytucji obowiązanych, zobowiązaną do stosowania obowiązków wynikających z przepisów o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu od 13 lipca 2018 r. 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	3
Uzasadnienie dla poziomu zagrożenia	Skrytki sejfowe umożliwiają przechowywanie niektórych rodzajów wartości majątkowych związanych z nielegalną działalnością i tym samym dają możliwość ukrycia ich przed organami ścigania Część banków oferuję tę usługę. Skorzystanie z niej wymaga podpisania umowy z bankiem, co powoduje, że wszystkie dane deponenta są dostępne również dla organów prowadzących postępowanie karne w stosunku do najemcy bądź dla komornika. Należy jednak pamiętać, że przestępcy mogą wykorzystywać też skrytki depozytowe udostępniane nie tylko przez banki, ale i wyspecjalizowanych przedsiębiorców. Ten *modus operandi* jest stosunkowo prosty, nie wymaga skomplikowanego planowania. GIIF nie otrzymywał wielu informacji o ukrywaniu środków pochodzących z nielegalnych źródeł w skrytkach sejfowych, zarówno jeśli chodzi o rezydentów, jak i nierezydentów. WNIOSEK: Ukrywanie środków pochodzących z nielegalnych źródeł w skrytkach sejfowych w Polsce stanowi wysokie zagrożenie praniem pieniędzy.

15. Obszar – działalność gospodarcza (ogólnie)

Tabela nr 30

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.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Założenie spółki prawa handlowego czy też rozpoczęcie działalności jako osoba fizyczna prowadząca działalność gospodarczą jest w pewnymi 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 tez 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 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.
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 praniem pieniędzy.

Tabela nr 31

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 tez 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 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.
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 tez mieć charakter końcowego ogniwa w łańcuchu transakcyjnym. Przedsiębiorstwo symulujące działalność gospodarczą może być podmiotem krajowym, ale tez 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 praniem pieniędzy.

Tabela nr 32

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 (często bez świadomości rzeczywistego celu) w przeprowadzaniu transakcji zakupu nieruchomości i towarów o wysokiej wartości, tworzeniu i prowadzeniu podmiotów gospodarczych, fundacji i trustów, a także realizacji transakcji finansowych poprzez użyczanie swoich rachunków bankowych.
Poziom podatności	3
Uzasadnienie dla poziomu podatności	Dostęp do usług prawniczych i doradztwa podatkowego jest stosunkowo łatwy. Mogą one wspomagać 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. IO z tego obszaru nie przekazują lub przekazują relatywnie mało informacji o podejrzanych transakcjach/podejrzanej działalności do GIIF (w 2017 r. przekazali ok. 0,034% wszystkich STR-ów oraz ok. 0,98% wszystkich SAR-ów od IO[39]). Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma ograniczoną 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 niewielkiej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	4
Uzasadnienie dla poziomu zagrożenia	Korzystanie z pośrednictwa innych podmiotów (często bez ich świadomości rzeczywistego celu), aby transferować i legitymizować środki pochodzące z nielegalnych źródeł jest jedną z rozpoznanych metod prania pieniędzy. GIIF posiada informacje o wykorzystywaniu tego *modus operandi*. Podmioty świadczący ww. usługi mogą zapewnić dostęp przestępcom do specjalistycznej wiedzy prawnej i 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 tego typu pośredników, 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 tego rodzaju pośrednictwa jest istotne również dlatego, że te usługi są niekiedy niezbędne do realizacji konkretnej transakcji. Sam dostęp do ww. usług jest dosyć łatwy i nie wymaga szczególnych kompetencji ani wiedzy specjalistycznej. Ten *modus operandi* może być postrzegany przez sprawców jako dosyć atrakcyjna i bezpieczna forma prania pieniędzy. WNIOSEK: Wykorzystanie pośrednictwa innych podmiotów (w celu transferowania i legitymizowania środków pochodzących z nielegalnych źródeł stwarza bardzo wysokie zagrożenie praniem pieniędzy.

[39] Wraz z biegłymi rewidentami i księgowymi.