Aktywa wirtualne – wskaźniki ryzyka ML/TF

TABELA SKRÓTÓW:

AML/CFT	Przeciwdziałanie praniu pieniędzy i finansowaniu terroryzmu	(ang. Anti-Money Laundering and Combating the Financing of Terrorism)
CDD	Środki bezpieczeństwa finansowego	(ang. Customer Due Diligence)
FATF	Grupa Specjalna ds. Przeciwdziałania Praniu Pieniędzy	(ang. Financial Action Task Force)
JAF	Jednostka Analityki Finansowej	
KYC	Poznaj Swojego Klienta	(ang. Know Your Customer)
ML/TF	Pranie pieniędzy i finansowanie terroryzmu	(ang. Money Laundering and Terrorist Financing)
STR	Raport o podejrzanej transakcji	(ang. Suspicious Transaction Report)
TOR	Anonimowa sieć komputerowa	(ang. The Onion Router)
VA	Aktywa wirtualne	(ang. Virtual Assets)
VASP	Podmioty świadczących usługi związane z VA	(ang. Virtual Asset Service Providers)

Aktywa wirtualne (VA) pozwalają na szybki i anonimowy transfer środków bez względu na odległość i granice państw. To czyni je narzędziem narażonym na wykorzystanie do finansowania nielegalnej działalności jak również prania dochodów z takiej działalności. W październiku 2018 r. Grupa Specjalna ds. Przeciwdziałania Praniu Pieniędzy (FATF) zaktualizowała swoje standardy, aby były lepiej dopasowane do szczególnego charakteru VA. W czerwcu 2019 r. FATF przyjęła Notę Interpretacyjną do Rekomendacji 15 w celu dalszego doprecyzowania wymagań wobec podmiotów zajmujących się VA. Z kolei we wrześniu 2020 r. ukazał się raport FATF, opisujący wskaźniki podwyższonego ryzyka (tzw. czerwone flagi) prania pieniędzy lub finansowania terroryzmu (ML/TF) z wykorzystaniem VA[1].

Poniżej prezentujemy najważniejsze informacje ze wspomnianego raportu FATF. **Dokument ten jest w szczególności skierowany do instytucji obowiązanych i powinien ukierunkować stosowanie przez nie środków bezpieczeństwa finansowego wobec podmiotów wykorzystujących aktywa wirtualne.** Jednocześnie informacje zebrane w raporcie mogą być użyteczne dla organów ścigania, w szczególności mogą pomóc w skutecznym wykrywaniu i ściganiu przestępstw związanych z VA.

[1] FATF (wrzesień 2020), *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*.

Zachęcamy do zapoznania się z całym raportem FATF, który zawiera szczegółowe wyliczenie wszystkich zidentyfikowanych czerwonych flag. W poniższym omówieniu prezentujemy zbiorcze opisy poszczególnych grup flag wraz z przykładami faktycznych spraw. Jednocześnie zwracamy uwagę, że sama obecność czerwonej flagi nie jest wystarczającym powodem do podejrzenia popełnienia przestępstwa, ale wskaźnikiem do dalszego badania i monitoringu. Zatem pojawienie się czerwonych flag nie powinno automatycznie powodować wysłania raportu o transakcji podejrzanej czy raportu o podejrzanych działaniach przez instytucje obowiązane, ale dopiero potwierdzenie, że w danym przypadku zachodzi podejrzenie ML/TF.

1. Czerwone flagi związane z transakcjami

Czerwone flagi tradycyjnie kojarzone z transakcjami z wykorzystaniem bardziej konwencjonalnych środków płatniczych pozostają istotne dla wykrywania potencjalnych nielegalnych działań związanych z VA, takich jak **podział transakcji na wiele przekazów poniżej progu raportowania** lub **liczne duże transakcje w małym odstępie czasu (np. 24 godzin)**. Takim wskaźnikiem może być także **transferowanie VA do wielu podmiotów świadczących usługi związane z VA (VASP)** – w szczególności, jeżeli są wśród nich VASP-y z innych jurysdykcji – lub **zdeponowanie VA w VASP-ie, a następnie ich wycofanie lub wymiana na inne VA, pomimo kosztów transakcyjnych**.

Przykład: Wielokrotne natychmiastowe transfery dużych kwot VA do zagranicznych VASP-ów (Republika Południowej Afryki)

Lokalny VASP wysłał do JAF STR w związku z podejrzeniami dotyczącymi zakupu dużych ilości VA przez różne osoby oraz ich natychmiastowego przekazania do VASP-u w zagranicznej jurysdykcji. W wielu przypadkach osoby te miały ten sam adres zamieszkania, dostępy do większości adresów VA pochodziły z tego samego adresu IP, co może wskazywać na wykorzystanie mułów pieniężnych w celu wyprania nielegalnych dochodów.

Ponadto dokonano wielokrotnego maskowania (ang. *layering*) funduszy, zanim zorganizowano zakup VA przez muły. Aby ukryć ich pochodzenie, gotówka była najpierw zdeponowana na różnych rachunkach w różnych instytucjach finansowych w całym kraju. Następnie środki te były przekazywane dalej na różne rachunki w różnych jurysdykcjach. Płatności elektroniczne zostały wprowadzone do ksiąg rachunkowych w mniejszych kwotach. Później pieniądze zostały przeniesione na inną grupę rachunków, zanim trafiły na rachunki mułów w różnych lokalnych VASP-ach. VA zostały natychmiast zakupione i przeniesione do zagranicznych VASP-ów. Zaangażowanych w ten proceder było ponad 150 osób. W sumie do dwóch zagranicznych VASP-ów wytransferowano około 108 352 900 USD (lub 11 960 Bitcoinów).

2. Czerwone flagi związane ze schematami transakcyjnymi

Na wykorzystanie VA do celów ML/TF mogą wskazywać nietypowe schematy transakcji. W przypadku nowych klientów VASP-ów może to być **złożenie depozytu nieproporcjonalnie dużego do profilu klienta** oraz **wykorzystanie jego dużej części do przeprowadzania transakcji od razu po otwarciu rachunku** lub **wycofanie depozytu wkrótce po złożeniu**. Wskaźnikami dla nowych, jak i stałych klientów mogą być: **używanie wielu rodzajów VA i wielu kont bez biznesowego uzasadnienia**, **dokonywanie regularnych transferów (np. każdego dnia, tygodnia) przy użyciu tego samego konta,**

wymiana VA na gotówkę przy prawdopodobnej stracie czy **wymiana dużej ilości jednego rodzaju VA na inny bez logicznego uzasadnieni**a.

Przykład: Wpłata początkowa niezgodna z profilem klienta (Czechy)

Bank wysłał STR na bazie następujących podejrzanych okoliczności:

1) transakcje niezgodne z profilem posiadacza rachunku - w ciągu pierwszych dwóch dni po założeniu konta osobistego dla młodej osoby rachunek otrzymał wysokie wpłaty o charakterze handlowym od różnych osób prawnych;

2) schemat transakcji - zdeponowane środki zostały natychmiast przekazane na rachunki kilku VASP-ów (w ciągu jednego dnia) w celu zakupu Bitcoinów;

3) profil klienta - jeden z zamawiających był znany bankowi jako zamieszany w sprawę o oszustwo.

Dochodzenie wykazało, że właściciel konta jest tzw. mułem pieniężnym, to jest osobą zwerbowaną przez przestępców przy pomocy mediów społecznościowych, aby otrzymywać płatności za towary sprzedawane online. Pieniądze przelewane na konto pochodziły od oszukanych firm. Środki były natychmiast przelewane z osobistego konta bankowego poprzez kilka dzielonych wpłat na inny rachunek prowadzony przez spółkę akcyjną w Czechach, a następnie były wymieniane na Bitcoiny przechowywane w kilku lokalnych VASP-ach, skąd bardzo szybko były wycofywane. Oprócz wysłania STR bank wstrzymał także podejrzane przelewy, co umożliwiło późniejszą konfiskatę środków.

Także VASP zauważył nieprawidłowości i dostarczył cennych dla śledztwa informacji. Obejmowały one okoliczności zakupu VA, informacje dotyczące transakcji oraz środków bezpieczeństwa finansowego (CDD), takie jak adres portfela VA, kopia dokumentu identyfikacyjnego użytego do zakupu oraz nazwisko domniemanego nabywcy. Dzięki tym danym organy ścigania mogły zwrócić się do banków o dodatkowe informacje (np. wyciągi bankowe).

3. Czerwone flagi związane z anonimowością

Ten zestaw wskaźników jest związany ze specyfiką technologii leżących u podstaw funkcjonowania VA. Najważniejszą jej cechą, z punktu widzenia ryzyka ML/TF, jest ułatwione zachowanie anonimowości przez posiadaczy VA. Jest to główna przyczyna atrakcyjności VA dla przestępców, którzy używają ich do ukrywania swoich dochodów. Anonimowość VA utrudnia prowadzenie śledztw i wykrywanie sprawców przestępstw przez organy ściągania. Uwagę instytucji obowiązanych prowadzących działalność związaną z VA powinny zwracać zlecane przez klientów **wymiany VA opartych na publicznych łańcuchach bloków (*blockchain*) na takie, które zapewniają zwiększoną anonimowość z racji wykorzystywania prywatnych łańcuchów bloków**[2]. Dotyczy to w szczególności przypadków, dla których trudno znaleźć biznesowe uzasadnienie. Także **klienci działający jako niezarejestrowane VASP-y na stronach umożliwiających wymianę *peer-to-peer*** należą do grupy podwyższonego ryzyka, a ponadto **każdy inny klient korzystający z takich stron w celu spieniężenia znacznej ilości VA, gdy trudno znaleźć racjonalne wytłumaczenie dla tego typu działania**.

[2] Mowa tu o tzw. AEC (*anonymity enhanced cryptocurrencies*). Należą do nich takie kryptowaluty jak Monero, Zcash czy Dash.

Przykład: Wykorzystanie adresu IP związanego z Darknet Marketplace - AlphaBay (USA)

Zlikwidowany przez władze USA w 2017 r. AlphaBay był największym przestępczym rynkiem darknetowym. Był on wykorzystywany przez setki tysięcy osób do kupna i sprzedaży narkotyków, skradzionych i sfałszowanych dokumentów identyfikacyjnych, podrabianych towarów, broni palnej i toksycznych chemikaliów, złośliwego oprogramowania i narzędzi do włamywania się do komputerów. Strona działała jako usługa w sieci TOR, aby ukryć lokalizacje serwerów, na których się znajdowała, jak również tożsamość jej administratorów, moderatorów i użytkowników. W latach 2015-2017 sprzedawcy AlphaBay korzystali z wielu różnych rodzajów VA i mieli około 200 tys. użytkowników i 250 tys. ofert. Na platformie zawarto transakcje o wartości ponad 1 mld USD.

W lipcu 2017 r. rząd Stanów Zjednoczonych z pomocą zagraniczną zlikwidował serwery, na których znajdował się AlphaBay. Administrator został aresztowany, a fizyczne jak i wirtualne aktywa z samego rynku zostały przejęte (w tym te, które stanowiły przychody samego AlphaBay).

4. Czerwone flagi dotyczące nadawców i odbiorców

Ten rodzaj wskaźników dotyczy profilu i nietypowego zachowania nadawcy lub odbiorcy przekazów VA. Będą to: nietypowe zachowania przy okazji zakładania konta, na przykład - **zakładanie wielu kont pod różnymi imionami w celu ominięcia limitów nałożonych przez dany VASP**, **wielokrotne otwieranie nowego konta w tym samym VASP-ie przy użyciu tego samego adresu IP**; nietypowe zachowania przy wykonywaniu środków bezpieczeństwa finansowego, takie jak **brak wiedzy lub niepełna informacja klienta na temat źródła jego funduszy lub jego kontrahentów**; wątpliwości dotyczące profilu klienta takie jak **podanie przez niego danych identyfikacyjnych identycznych jak dla istniejącego już konta** lub **niezgodność adresu IP przypisanego do konta klienta oraz adresu, z którego zainicjowana została transakcja**; okoliczności wskazujące na to, że klient jest mułem pieniężnym lub ofiarą machinacji (naciągniętą na współpracę przestępczą bez swojej wiedzy) - m.in. **małe obeznanie z technologią VA**, **znacząco starszy wiek niż przeciętny dla użytkowników platformy**, **zakupy przekraczające możliwości finansowe klienta wynikające z historii konta**; a także inne nietypowe zachowania, takie jak **częsta zmiana danych identyfikacyjnych konta** czy **częste łączenie się z VASP-em z różnych adresów IP**.

Przykład: Profil klienta nieodpowiadający regularnym transakcjom VA o wysokiej wartości (Włochy)

Giełda kryptowalut oraz instytucja płatnicza wysłały do JAF STR-y dotyczące wysokiej wartości obrotu VA na pewnym rachunku tuż po jego otwarciu. Posiadacz rachunku przeprowadzał różne transakcje kupna i sprzedaży VA na kwotę ponad 180 000 EUR, co nie odpowiadało jego profilowi (w tym zawodowi i wynagrodzeniu).

Analiza przepływu środków wykazała, że VA były następnie wykorzystywane do: (i) transakcji na rynku w darknecie; (ii) zakładów online; (iii) transakcji z VASP-ami, które nie były objęte odpowiednią kontrolą AML/CFT lub które były przedmiotem dochodzeń w sprawie prania pieniędzy; (iv) operacji na platformach, które oferowały transakcje VA typu "peer-to-peer"; oraz (v) "miksowania". W tym samym czasie posiadacz rachunku wyprowadzał ze swojego konta za pomocą różnych metod (przelewów pieniężnych, bankowości internetowej oraz kart przedpłaconych) duże kwoty.

Środki wpływające na konto okazały się pochodzić od osób, które kupiły VA (Bitcoiny) za gotówkę. Osoby te znajdowały się w różnych państwach w Azji i Europie (w tym we Włoszech), a pieniądze przekazywały przy użyciu przelewów bankowych. Posiadacz konta otrzymywał również środki za pośrednictwem swoich przedpłaconych kart od podmiotów z Afryki i Bliskiego Wschodu, które z kolei zbierały środki od osób zamieszkałych we Włoszech i w innych krajach. Środki te były następnie wykorzystywane do przelewów transgranicznych i gier hazardowych on-line oraz wypłacane w gotówce z bankomatów we Włoszech.

Przykład: Ofiary oszustwa wykorzystane w roli mułów pieniężnych (Finlandia)

Obcokrajowcy kontaktowali się z emerytami i osobami starszymi za pomocą bezpośrednich rozmów telefonicznych, e-maili lub mediów społecznościowych i oferowali im inwestycje w Bitcoiny lub inne VA, obiecując duże zyski dzięki rosnącym popularności i cenom VA. Początkowe inwestycje o niewielkich kwotach (najczęściej poniżej 250 euro) były dokonywane z bankowych kont ofiar, kart kredytowych lub za pomocą innych metod i trafiały do rąk przestępców. W innych przypadkach ofiary zostały poinstruowane, aby wymienić gotówkę na Bitcoin przy użyciu bankomatu VA i wysłać środki na adres wskazany przez przestępców.

Ofiary nie były obeznane z technologią VA i nie rozumiały, w co inwestują. Przestępcy poprosili je o zainstalowanie na swoich urządzeniach aplikacji zdalnego pulpitu, rzekomo w celu pomocy w prawidłowym przekazaniu środków na konkretne konta. Dzięki temu przestępcy mogli dokonywać nieautoryzowanych przekazów pieniężnych bez wiedzy ofiary, dopóki nie zauważyła ona brakujących na koncie pieniędzy. W niektórych przypadkach przestępcy pokazywali ofiarom sfabrykowane artykuły prasowe, w których znane osoby, zamożni biznesmeni lub dziennikarze promowali inwestycje w VA. W ten sposób łatwiej było im zdobyć zaufanie oszukanych przez siebie osób.

5. Czerwone flagi dotyczące źródeł funduszy i majątku

Niezgodne z prawem wykorzystanie VA często wiąże się z działalnością przestępczą, taką jak nielegalny handel narkotykami i substancjami psychotropowymi, oszustwa, kradzieże i wymuszenia (w tym przestępstwa popełniane w cyberprzestrzeni). Czerwone flagi związane z przestępczymi źródłami środków finansowych lub majątku obejmują, m.in. **ponadprzeciętnie wysokie depozyty na kontach VA o nieznanych źródłach pochodzenia, które wymieniane są następnie na gotówkę**, **transakcje VA z internetowymi serwisami hazardowymi**, **pochodzenie większej części funduszy klienta z inwestycji w VA** – w szczególności, jeśli dokonano ich za pośrednictwem giełd nie poddanych kontroli AML/CFT.

Przykład: Korzystanie z wielu giełd VA, fałszywych dokumentów identyfikacyjnych i kart przedpłaconych (USA)

Oskarżeni w tej sprawie mieli zorganizować schemat prania pieniędzy pochodzących z cyberwłamania do giełdy VA, podczas którego skradziono VA o wartości 250 milionów dolarów. Dwóch oskarżonych miało wyprać około 91 milionów dolarów ze skradzionych VA, a także 9,5 miliona dolarów z innej cyberkradzieży.

Skradzione VA były transferowane w setkach zautomatyzowanych transakcji z wykorzystaniem wielu różnych giełd VA. Podczas poddawania się procedurom KYC piorący posługiwali się przerobionymi zdjęciami i sfałszowanymi dokumentami. Około 35 milionów dolarów zostało przekazanych na

zagraniczne rachunki bankowe i było również wykorzystywane do zakupu kart przedpłaconych, które mogły być wymienione na VA. Oskarżeni działali za pośrednictwem niezależnych, jak i połączonych rachunków, świadcząc usługi wymiany VA na gotówkę. Oskarżeni prowadzili również działalność gospodarczą w USA, ale nigdy nie trafili do rejestru amerykańskiej jednostki analityki finansowej.

6. Czerwone flagi związane z ryzykiem geograficznym

Ten zestaw wskaźników jest związany z wykorzystywaniem przez przestępców faktu, że poszczególne kraje są na różnym etapie wdrażania standardów FATF dotyczących VA i VASP-ów. Częstą praktyką jest **przenoszenie nielegalnych dochodów do VASP-ów działających w krajach, których przepisy AML/CFT posiadają istotne luki** (np. nie nakładają na VASP-y obowiązku raportowania lub rejestracji działalności). Pod uwagę należy wciąć kraj, w którym zainicjowana została transakcja, kraj docelowy transakcji, a także tranzytowy. Istotne są zarówno pochodzenie klienta, jego miejsce zamieszkania jak i miejsce prowadzenia działalności gospodarczej.

Przykład: **Sprzedawca Bitcoinów prowadzący bez licencji działalność w zakresie przekazywania środków pieniężnych (USA)**

W kwietniu 2019 r. oskarżony otrzymał karę dwóch lat więzienia za świadczenie usług przekazów pieniężnych bez licencji. Sprzedawał on Bitcoiny warte setki tysięcy dolarów ponad tysiącowi klientów w USA. Wyrok obejmował także przepadek 823 357 dolarów zysku.

Oskarżony reklamował swoje usługi na stronach internetowych dla użytkowników VA. Gotówkę w zamian za VA przyjmował od klientów osobiście. Niektórzy klienci płacili za pomocą ogólnokrajowych sieci bankomatów lub przekazów pieniężnych. Oskarżony otrzymywał 5% premii od bieżącego kursu wymiany. Po raz pierwszy nabył Bitcoiny na amerykańskiej giełdzie kryptowalut, jednak gdy jego działania wzbudziły podejrzenia, a jego konto zostało zamknięte, zaczął korzystać z giełdy w Azji, gdzie kupił Bitcoiny warte 3,29 miliona dolarów w setkach oddzielnych transakcji między marcem 2015 r. i kwietniem 2017 r. Oskarżony przyznał również, że wymienił 1 mln dolarów przechowywany w sąsiadującej z USA jurysdykcji na metale szlachetne, które sukcesywnie transportował do USA w porcjach poniżej 10 000 USD niewymagających zaraportowania.