• F I N A N S E I P R A W O F I N A N S O W E •
• Journal of Finance and Financial Law •

Wrzesień/September 2015 • vol. II, no. 3 ISSN 2353-5601

https://doi.org/10.18778/2391-6478.2.3.10

RYZYKO AML I JEGO ZNACZENIE W DZIAŁANOŚCI BANKÓW

Weronika Zielińska*

Streszczenie:

Artykuł obejmuje teoretyczne przedstawienie problemu prania pieniędzy i finansowania terroryzmu, a także zwięźle przedstawia wybrane metody statystyczne pozwalające wykrywać nietypowe transakcje, które potencjalnie niosą za sobą ryzyko wykorzystania banku do wyżej wspomnianego problemu. Temat ten został wybrany, ponieważ globalne instytucje finansowe coraz więcej uwagi przywiązują do ryzyka AML (ang. *Anti-Money-Laundering*), czyli ryzyka związanego z wykorzystaniem instytucji finansowych do procesu prania pieniędzy oraz oszustw finansowych. Banki zobligowane są do monitorowania transakcji, poprzez różne akty prawne w Azji, w USA (*FACTA– Foreign Account Tax Compliance Act* oraz *US Patriot Act 2001*), czy wkrótce obowiązującymi czterech europejskich dyrektyw (4MLD).

Słowa kluczowe: AML, ryzyko operacyjne, pranie pieniędzy, oszustwa finansowe, międzynarodowe regulacje prawne.

JEL Class: A, C, G, P.

Przyjęto/Accepted : 15.08.2015 Opublikowano/Published: 30.09.2015

WPROWADZENIE

Proces prania pieniędzy polega na tworzeniu skomplikowanych operacji finansowych w celu oddzielenia środków finansowych od ich nielegalnego źródła pochodzenia. Środki, najczęściej w formie gotówki, pochodzącej z nielegalnych

* Magister, absolwentka Katedry Statystyki, Uniwersytet Łódzki, Wydział Ekonomiczno-Socjologiczny.

Wrzesień/September 2015 • vol. II, no. 3 ISSN 2353-5601

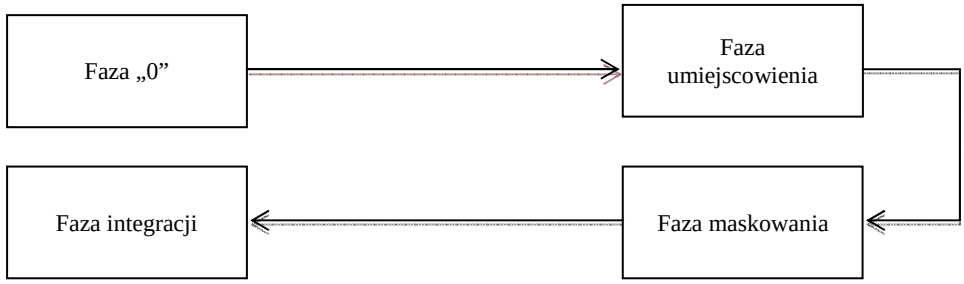
źródeł, jak sprzedaż narkotyków, handel ludźmi czy bronią, oszustwa gospodarcze czy podatkowe, są wprowadzane do obiegu finansowego w celu zamaskowania ich prawdziwego pochodzenia, a następnie posługiwania się tym środkami, tak jak ze źródeł legalnych. Proces prania pieniędzy składa się z czterech faz [Savla 2001: 10–11]:

– faza zerowa, czyli wygenerowanie środków pieniężnych wynikiem działalności przestępczej,

– faza umiejscawiania, czyli faza pierwszego wprowadzenie środków do systemu finansowego. Jest to etap przygotowawczy do oddzielenia pochodzenia środków od ich nielegalnego źródła,

– faza maskowania, czyli wykonywanie różnego rodzaju operacji finansowych poprzez liczne produkty finansowe w celu zgubienia śladu ich oryginalnego pochodzenia oraz przygotowanie nielegalnych środków do ostatniej fazy,

– faza integracji, czyli etapu w którym środki są asymilowane, a niekiedy nawet łączone są z tymi o legalnych korzeniach.



Rysunek 1. Proces prania pieniędzy

Źródło: opracowanie własne na podstawie na postawie: Savla [2001: 10–11].

Opisany proces zostanie zobrazowany przez krótki przykład: pewna grupa przestępcza zebrała gotówkę ze sprzedaży broni z okolicznych miejscowości w Afryce. Gotówka ta została przeliczona i złożona w jednym miejscu w pewnym magazynie (faza zero). W celu uniknięcia rejestru oraz identyfikacji osób wchodzących w skład grupy przestępczej, zostaje ona podzielona na mniejsze części (>10 tys. $) oraz wprowadzona do banków przez tak zwane „słupy” lub „smurfy” (ang. *smurfing*), a następnie jest wypłacana czekami (faza umiejscawiania). W tym miejscu również zaczyna się faza maskowania. Wspominane czeki realizowane są na jednym koncie w jednym z afrykańskich oddziałów Banku X z siedzibą w Nowym Jorku, a następnie poprzez transfery elektroniczne, pieniądze wysyłane są do Banku Y w Chicago. Dalej z części środków na koncie w Banku Y zakładana jest lokata krótkoterminowa, a reszta funduszy przekazywana jest przelewem do Banku Z w Londynie. Z rachunku w Londynie środki zamieniane są na certyfikaty depozytowe, stanowiące zabezpieczanie

Wrzesień/September 2015 • vol. II, no. 3 ISSN 2353-5601

kredytu dla firmy na Kajmanach, a stamtąd przelewane na inne konto w Banku X w Nowym Jorku. Dalej wykonywane są transfery elektroniczne do Waszyngtonu, gdzie pieniądze trafiają na konta szefów grupy przestępczej. Pieniądze na prywatnych kontach szefów mogą być teraz swobodnie dysponowane na rynku (faza integracji) [Kuijlen i Migut 2004: 71–80].

1. METODY PRANIA PIENIĘDZY

Pranie pieniędzy może przyjąć różne formy, choć większość z metod stosowanych przez przestępców można podzielić na jeden z kilku typów. Są to tak zwane „metody bankowe" jak *Smurfing* (znany również jako *Structuring*), zamiana walut, polegająca na przyniesieniu gotówki i jej zamianie na inną walutę czy fikcyjne kredyty. Przykłady najpopularniejszych metod zostaną przytoczone poniżej [Savla 2001: 10–11].

Structuring (tłumaczenie z ang. konstruowanie/strukturyzowanie) jest to metoda fazy umieszczania, w której gotówka jest podzielone na mniejsze części i poprzez depozyty gotówkowe wprowadzana do banku, aby uniknąć wymagań dokumentacyjnych jakie należy dostarczyć bankom w ramach regulacji AML. Często dalej na kontach bankowych następują zakupy instrumentów finansowych na okaziciela, nie wymagające podawania danych osobowych oraz omijające wymogi rejestracyjne [Lawrence 2005: 78].

Fikcyjne kredyty, metoda wykorzystywana, gdy „brudne" środki pieniężne mają być wykorzystywane do prywatnych celów. W takim wypadku są one przechowywane najczęściej w domach. Aby wykorzystać zgromadzone środki, kryminaliści zaciągają kredyty (lub wyrabiają kartę kredytową), wykorzystując je na prywatny użytek i spłacają zobowiązania ze środków pochodzących z nielegalnych źródeł.

Masowy przemyt środków pieniężnych (ang. *smuggling*), metoda, która polega na fizycznym przemycie gotówki do innego kraju, a następnie zdeponowaniu jej w instytucji finansowej, najlepiej w banku zapewniającym większą tajemnicą bankową i mniej rygorystyczną polityką egzekwowania dokumentacji w celach AML [*National Money Laundering Threat Assessment*, 2011: 33].

Zakładanie **firm operujących głównie gotówką** (ang. *cash intensive business*), jest to metoda, w której wspomniane firmy są zaangażowane w otrzymanie dużych ilości gotówki oraz wykorzystują swoje konta bankowe do dokonywania nielegalnych wpłat gotówkowych, uzasadniając wysokie wolumeny gotówkowe przychodami z ich profilu działalności. Przykładami tego typu przedsiębiorstw są budynki parkingowe, kluby, solaria, myjnie czy kasyna [*National Money Laundering Threat Assessment*, 2011: 33].

Zakładanie **firm „krzaków", trusty oraz biura nieruchomości**, jest to kolejna metoda mająca ukryć prawdziwą tożsamość osób zaangażowanych w pra-

Wrzesień/September 2015 • vol. II, no. 3 ISSN 2353-5601

nie pieniędzy. Często takie firmy są rejestrowane w krajach o liberalnym podejściu do podawania danych osobowych właścicieli spółki (np. Kajmany, Brytyjskie Wyspy Dziewicze), co utrudnia odnalezienie źródeł pochodzenia funduszy. W przypadku nieruchomości, maskowanie pochodzenia zasobów finansowych polega na kupnie pewnej nieruchomości za pieniądze z nielegalnych źródeł, szybką jej sprzedaż, a fundusze ze sprzedaży są następnie wprowadzane do systemu finansowego jako „legalne".

2. WYTYCZNE WSPOMAGAJĄCE PROCES ZARZĄDZANIA RYZYKIEM AML

Ze względu na fakt, że różne kraje mają odrębne systemy administracyjne i rozporządzenia prawne, a wiele banków działa w skali międzynarodowej, FATF (*Financial Action Task Force*) wyznacza standardy w walce przeciw praniu pieniędzy i finansowaniu terroryzmu. Standardy wyznaczane przez FAFT stanowią rekomendowane rozwiązania mające zapewnić [*UKNF*, *Międzynarodowe Standardy Przeciwdziałania Praniu Pieniędzy*...]:

– właściwą identyfikację ryzyka AML,

– wyznaczenie obowiązków i odpowiedzialności odpowiednim organom nadzorczym oraz organom ścigania,

– ułatwienie współpracy międzynarodowej i wiedzy o klientach instytucji finansowych,

– stosowanie środków zapobiegawczych w stosunku do sektora finansowego oraz środków ścigania przestępców dopuszczających się działalności związanej z praniem pieniędzy.

2.1. Ocena ryzyka na postawie analizy ryzyka

Aby poprawnie identyfikować ryzyko prania pieniędzy i finansowania terroryzmu, należy zrozumieć mechanizmy związane z tym rodzajem ryzyka. W tym celu należy stosować analizę opartą o ryzyko (ang. *risk base approach*) we wszystkich obszarach, w którym to ryzyko występuje. W obszarach, w których zostanie wykryte podwyższone ryzyko, czyli w których bank jest bardziej narażany na jego wykorzystanie do wyprowadzenia nielegalnych środków, należy zapewnić takie systemy przeciwdziałania praniu pieniędzy, które takie ryzyko będą regulowały we właściwy sposób. Natomiast, w obszarach, w których zostanie wykryte obniżone ryzyko, można dopuścić uproszczone procedury w części zaleceń FATF, jeśli określone warunki zostaną spełnione. Jednakże sam sposób, w jaki bank będzie monitorował ryzyko AML pozostawiono w gest banku, pod warunkiem, że procedury bankowe będą zgodne z standardami wytyczonymi przez FATF dotyczącymi między innymi przechowywania dokumentacji, oceny opartej o ryzyko, tajemnicy bankowej czy badania klienta [UKNF, *Międzynarodowe Standardy Przeciwdziałania Praniu Pieniędzy*...].

Wrzesień/September 2015 • vol. II, no. 3 ISSN 2353-5601

2.2. Tajemnica bankowa i badanie klienta

Instytucje finansowe, niezależnie od kraju działalności czy kraju macierzystego instytucji finansowej, powinny przestrzegać przepisów dotyczących tajemnicy bankowej oraz starannego przechowywania danych osobowych klientów, przy jednoczesnym badaniu klienta z zastosowaniem odpowiedniego podejścia zależnego od ryzyka związanego z danym klientem. Żadna instytucja finansowa nie może prowadzić rachunków anonimowych ani też rachunków założonych na fikcyjne osoby. Badanie klienta powinno odbywać się przynajmniej na niżej wymienianych etapach [*UKNF, Międzynarodowe Standardy Przeciwdziałania Praniu Pieniędzy*...]:

– nawiązywania pierwszej relacji z danym klientem,

– przy każdej transakcji klienta, która jednorazowo przekracza 15 tys. EUR lub 10 tys. USD,

– w momencie, kiedy wystąpi podejrzenie, że klient jest zamieszany w pranie pieniędzy lub jest związany z finansowaniem terroryzmu,

– w chwili, gdy dana instytucja finansowa uzna, że wcześniej dostarczone informacje indentyfikacyjne o kliencie mogą być nieprawdziwe.

Zalecane jest przez FATF, aby badanie klienta składało się z weryfikacji jego tożsamości, identyfikacji relacji klienta z rzeczywistym odbiorcą funduszy i na odwrót. W przypadku, gdy jest to konieczne, należy zweryfikować także cel transakcji, aby sprawdzić czy przepływ pieniędzy ma logiczny sens [*UKNF*, *Międzynarodowe Standardy Przeciwdziałania Praniu Pieniędzy*...].

Ponadto instytucje finansowe powinny posiadać odpowiednie mechanizmy zarządzania ryzykiem AML, które pozwolą na identyfikacje osób zajmujących stanowiska publiczne (ang. PEP – *Politically Exposed Persons*), jako klientów lub jako rzeczywistych odbiorców przekazywanych środków. Nawiązanie oraz kontynuowanie relacji z taką osoba wymaga również zgody kadry zarządczej wyższego szczebla banku. Transakcje, gdzie stroną są osoby publiczne powinny zawsze być monitorowane ze szczególną ostrożnością [*UKNF*, *Międzynarodowe Standardy Przeciwdziałania Praniu Pieniędzy*...].

Również banki powinny zachować szczególną ostrożność, gdy stroną transakcji jest organizacja *non-profit*. Jest to uwarunkowane tym, że podmioty te mogą być wykorzystane do finansowania terroryzmu. Wyróżnia się kilka zjawisk, które sprawiają, że organizacje non-profit są podmiotami podwyższonego ryzyka [*UKNF, Międzynarodowe Standardy Przeciwdziałania Praniu Pieniędzy*...]:

– ugrupowania terrorystyczne mogą podszywać się pod legalne podmioty, jak np. organizacje charytatywne,

– legalne podmioty mogą zostać wykorzystane jako pośrednicy finansowi.

FATF stworzył też listę krajów podwyższonego ryzyka prania pieniędzy oraz finansowania terroryzmu. Kraje znajdujące się na tej liście charakteryzują się często społeczną aprobatą dla organizacji, które głoszą ekstremizm religijny,

Wrzesień/September 2015 • vol. II, no. 3 ISSN 2353-5601

lub są to kraje, które posiadają wysoki odsetek transakcji gotówkowych, przy których identyfikacja pochodzenia środków finansowych jest szczególnie utrudniona. Z tego też powodu przepływ pieniędzy, badanie klienta oraz relacji miedzy stronami transakcji czy cel operacji bankowych powinien być monitorowany z zastosowaniem podwyższonych norm oceny ryzyka [*UKNF*, *Międzynarodowe Standardy Przeciwdziałania Praniu Pieniędzy*...].

3. WYKRYWANIE NADUŻYĆ

Mimo, że ryzyko prania pieniędzy oraz oszustw finansowych dotyczy każdej instytucji finansowej niezależnie od jej rozmiarów, najbardziej narażone na ryzyko AML są duże, międzynarodowe banki. Dzieje się tak, ponieważ globalne banki oferują mnogość oddziałów na całym świecie oraz dostępność do różnych produktów finansowych, także w skali światowej. Daje to możliwość przestępcom na szybką transmisję środków finansowych z jednego kraju do drugiego, a także wachlarz ogromnych możliwości budowania złożonych procesów prania pieniędzy w oparciu oszeroką ofertę produktową.

W celu przeciwdziałania praniu pieniędzy tworzy się systemy, które mają za zadanie wykrywać potencjalnie podejrzane transakcje oraz identyfikować osoby zajmujące się wprowadzaniem nielegalnych funduszy do systemu finansowego. Wymaga to wielowymiarowej analizy, nie tylko samych zapisów bankowych, ale także analiz asocjacji między transferami, a osobami zaangażowanymi w wykonywanie tych transferów. Jest to ogromne wyzwanie dla instytucji finansowych, gdyż posiadają one ogromną ilość klientów, a każdy z nich może posiadać praktycznie nieograniczoną ilość produktów oferowanych przez bank (będziemy mówili nawet o miliardach różnego rodzaju kont bankowych). Duża liczba klientów pociąga za sobą ogromną liczbę transakcji, a co za tym idzie, olbrzymią ilość danych. Metody statystyczne, w tym coraz bardziej popularne *data mining*, mogą w znacznym stopniu zautomatyzować analizy transakcji w poszukiwaniu tych operacji, które są dokonywane w celu przeprania pieniędzy. Metody te pomagają w segregacji klientów, jak i transakcji na te o niskim, przeciętnym oraz wysokim stopniu ryzyka. Takie zautomatyzowane systemy oczywiście muszą być wspierane przez wyspecjalizowanych analityków, którzy ostatecznie zdecydują czy transakcje i klienci wytypowani przez odpowiednie algorytmy rzeczywiście są prawidłowe, a pieniądze mogą pochodzić z działalności przestępczej.

Systemy dedykowane wykrywaniu transakcji, mogących mieć nielegalne pochodzenie, są oparte na regułach rejestrujących różnego rodzaju anomalie. Do takich anomalii można zaliczyć przykładowo zmianę zachowania klienta poprzez analizę typowych dla niego transakcji lub same transakcje, czyli np. te przekraczające ustaloną kwotę, powyżej której alert powinien wygenerować się. Aby móc przeciwdziałać praniu pieniędzy najpierw trzeba posiadać odpo-

Wrzesień/September 2015 • vol. II, no. 3 ISSN 2353-5601

wiednio duże bazy danych na temat zdarzeń operacyjnych, a następnie zgłębić posiadaną wiedzę. Dobrze zbudowany system wymaga więc monitorowania klientów przez dłuższy okres czasu.

3.1. Wykorzystanie analizy połączeń i asocjacji w przeciwdziałaniu praniu pieniędzy

Jednym ze sposobów wykrywania pieniędzy są analizy połączeń i asocjacji. Metoda ta jest o tyle przydatna, iż proceder prania pieniędzy na ogół składa się z licznych operacji finansowych, które na pierwszy rzut oka nie charakteryzują się żadnymi zależnościami. Analiza połączeń pozwala na znalezienie krytycznych punktów oraz powiazań i relacji pomiędzy osobami a transakcjami, które potencjalne niosą ryzyko AML. Metoda ta pozwala na odnalezienie wspominanych połączeń, w taki sposób by móc scharakteryzować poszczególne grupy osób mogących brać udział w procederze prania pieniędzy [Kuijlen i Migut 2004: 71–80].

Jednakże, aby analiza powiazań mogłaby być użyta w praktyce, najpierw dane zgromadzone w bazach powinny zostać ujednolicone i powinien zostać wybrany poziom szczegółowości danych. Jest to proces czasochłonny, a czasami wręcz niemożliwy, np. gdy mamy do czynienia z transakcjami pomiędzy kontami tego samego klienta w różnych bankach. Może wtedy wystąpić niekompletność danych w momencie, kiedy jeden bank posiada podstawowe dane klienta, a drugi posiada zarówno pierwsze imię, nazwisko, jak i środkowe imiona klienta. Takie niekompletne rekordy mogą powodować pozorne korelacje między dwoma podmiotami, gdzie w rzeczywistości występuje tylko jeden podmiot transakcji. Także źle pobrany poziom szczegółowości, może dawać wyniki błędne i spowalniać cały proces odkrywania zależności.

Następnym krokiem jest stworzenie algorytmu mającego na celu wykrywanie anomalii, które mogą oznaczać nadużycie lub oszustwo. Warto na tym etapie tworzyć reguły mające na celu wykrywanie transferów o wartości znacznie przekraczającej przeciętną wartość operacji dla danej klasy klientów. Jest to możliwe dzięki łączeniu rekordów, tak aby wykryć nietypowe wzorce zachowań.

Transakcje powinno monitorować się w podziale na podgrupy w celu lepszej identyfikacji podejrzanych operacji finansowych. Takimi operacjami są transakcje pomiędzy [Kuijlen i Migut 2004: 71–80]:

– firmami (B2B – Business-to-Business),
– osobami fizycznymi a firmami (B2C – Business-to-Consumer),
– osobami fizycznymi (C2C – Consumer-to-Consumer).

3.2. Wykorzystanie SVM w AML

Metoda wzorów nośnych – SVM (*Support Vector Machine*) [Vapnik 1995: 267–290] jest metodą statystyczną powszechnie wykorzystywaną przy binarnej klasyfikacji i tworzeniu regresji. Zadaniem AML jest wykrywanie zachowań

Wrzesień/September 2015 • vol. II, no. 3 ISSN 2353-5601

nietypowych w różnych wymiarach np. transakcjach, kontach, rodzajach produktów itd. Oznacza to, że wykrywanie podejrzanych transakcji sprowadza się do wyboru pomiędzy dwoma kryteriami: zestawem normalnym oraz wzorcem nietypowym. Zwykle przy metodach opartych na klasyfikacji musimy dysponować dość dużą startową (treningową) bazą danych do określenia reguł klasyfikacyjnych, gdyż poprawne działanie mechanizmu klasyfikującego silnie zależy od baz treningowych. Tymczasem określenie powszechnego wzorca prania pieniędzy, w danym zbiorze danych jest stosunkowo trudne, szczególnie dla grup produktów czy klientów charakteryzujących się dużą ilością transakcji, dla których podejrzane transakcje zdarzają się jedynie kilka razy w miesiącu. W takich przypadkach sprawdza się właśnie metoda wzorców nośnych, gdyż opiera się ona na niedużych bazach treningowych, klasyfikujących transakcje jako prawidłowe lub podejrzane. Ponadto SVM nie jest wrażliwa na zaburzenia wymiarowości, które są charakterystyczne dla zbiorów danych finansowych [Kingdon 2004:87–89].

Tradycyjny model SVM polega na znalezieniu takiej płaszczyzny, która jest optymalna, poprawnie klasyfikuje dane oraz daje margines separacji jak największy. Marginesem separacji będziemy nazywać odległość od płaszczyzny klasyfikacji do najbliżej leżącego od niej punktu danych.

Załóżmy, że dane w bazie określone są na płaszczyźnie przez y_1, y_2, y_3, …y_i należące do Y, tak że dane w Y charakteryzują się określoną cechą, a niewielka liczba elementów to outlier'y, czyli transakcje odbiegające od normy. Jeśli model poprawnie klasyfikuje dane to wszystkie transakcje normalne, będą klasyfikowane jako $y_i = 1$, zaś transakcje odstające, czyli podejrzane, będą klasyfikowane jako $y_i = –1$ [Scholkopf 2000: 77–84].

Inną dość popularną metodą wykorzystywaną w dziedzinie walki z ryzykiem AML, jest również analiza regresji, gdzie na podstawie demograficznych i behawioralnych cech przewiduje się prawdopodobieństwo wykorzystywania konta jako kanału prania pieniędzy.

Wyżej wspominane sposoby wykorzystania narzędzi statystycznych w walce z ryzykiem AML są jedynie przykładami z literatury. Obecnie stosuje się coraz to nowsze narzędzia i metody, gdyż jest to obszar, który w ostatnich latach coraz szybciej rozwija się.

PODSUMOWANIE

Podnosząca się świadomość o zagrożeniach płynących z ryzyka, jakim jest pranie pieniędzy czy finansowanie terroryzmu skutkuje rozwojem metod, regulacji i standardów związanych z tym zjawiskiem w skali międzynarodowej. Grzywny regulacyjne opiewające na miliony, a czasem nawet na miliardy dolarów, groźba pozbawienia licencji bankowej oraz postępowania karnego wobec banków i osób prywatnych sprawiły, że banki zaczęły przykładać większa uwa-

Wrzesień/September 2015 • vol. II, no. 3 ISSN 2353-5601

gę do ryzyka operacyjnego w zakresie AML oraz rozwoju narzędzi mający na celu przeciwdziałaniu zjawisku prania pieniędzy.

Aby przeciwdziałać temu zjawisku nie wystarczą jedynie rozwiązania lokalne, ale potrzebna jest także skoordynowana współpraca i standardy międzynarodowe. Dzięki temu część analizy może zostać zautomatyzowana poprzez wykorzystanie metod statystycznych. Niezwykle pozytywnym zjawiskiem jest to, że same banki zaczęły doceniać wagę, jaka wiąże się z ryzykiem prania pieniędzy i finansowania terroryzmu. Ryzyko AML naraża bowiem bank nie tylko na wysokie kary pieniężne nakładane przez organy nadzorcze, ale również na problemy refutacyjne. Ryzyko to może prowadzić do utraty zaufania wśród społeczeństwa, co skutkuje zmniejszeniem się liczby jego klientów, a to może doprowadzić do redukcji zysków i zakończenia działalności przez bank.

Rozwój procedur i narzędzi zapobiegającym ryzyku AML jest też wynikiem tego, że są one wykorzystywane nie tylko do wykrywania oszustw finansowych (w tym podatkowych), ale także wykorzystywane do przeciwdziała finansowaniu terroryzmu, który w ostatnich latach stanowi coraz większe zagrożenie. Dlatego też kluczowe jest coraz szersze wykorzystywanie metod statystycznych w tej dziedzinie, aby lepiej identyfikować transakcje potencjalnie niosące ze sobą ryzyko i móc prewencyjnie reagować odcinając organizacjom terrorystycznym możliwość dostępu i transmisji środków pieniężnych.

BIBLIOGRAFIA

Lawrence M. Salinger, 2005, *Encyclopedia of white-collar & corporate crime: A – I*, Volume 1, SAGE Publications.

Kuijlen T., Migut G., 2004, *Wykrywanie nadużyć i pranie brudnych pieniędzy*, StatSoft Polska, Warszawa.

Kingdon J., 2004, *AI Fights Money Laundering*, IEEE Transactions on Intelligent Systems, Washington.

National Money Laundering Threat Assessment, December 2005. Retrieved 3 March 2011.

Scholkopf B., 2000, *A short tutorial on kernels*, Microsoft Research, Rech Rep: MSR-TR-200-6t.

Savla S., 2001, *Money Laundering and Financial Intermediaries*, Kluwer Law International, Boston.

UKNF, *Międzynarodowe Standardy Przeciwdziałania Praniu Pieniędzy i Finansowaniu Terroryzmu oraz Proliferacji – Rekomendacje FATF*, www.knf.gov.pl/Images/Rekomendacje_FATF_tcm75-40223.pdf.

Vapnik V., 1995, *The Nature of Statistical Learning Theory*, Springer Verlag, NewYork.

AML RISK AND ITS MEANING IN BANKING

Article covers the theoretical problem of money laundering and terrorist financing, as well as concisely presents selected statistical methods that allow the detection of unusual transactions, which may potentially pose a risk to use the bank for money laundering or terrorist financing. This topic has been chosen because global financial institutions pay more and more attention to

Wrzesień/September 2015 • vol. II, no. 3 ISSN 2353-5601

the risk of AML (Anti-Money-Laundering), that is the risks associated with the use of financial institutions in the process of money laundering and fraud. Banks are obliged to monitor transactions through various acts in Asia, the United States (*FACTA – Foreign Account Tax Compliance Act oraz US Patriot Act 2001*) and soon the four European directives (4MLD).

Key words: AML, operational risk, money laundering, fraud.