

Raport

Pranie pieniędzy

Chmielniak Adwokaci we współpracy z Kroll Ontrack



Spis treści

Wstęp	3
Część pierwsza	
Definicja	4
Etapy i metody	6
Pranie pieniędzy w liczbach	8
Przestępstwa bazowe dla prania pieniędzy	12
Część druga	
Liczba nadużyć i koszty z nimi związane	14
Wiele firm nie jest przygotowanych na sytuację, w której coś pójdzie źle	15
Człowiek wewnątrz	17
Co zrobić w przypadku podejrzenia nadużycia?	17
Analiza dokumentów	18
Znaleźć igłę w stogu siana	19
Cyfrowe odciski palców	20
Dochodzenia w sprawach związanych z praniem pieniędzy	21
Studium przypadku obrazujące rolę dowodów elektronicznych	22
Studium przypadku dotyczące fałszowania korespondencji	23
Podsumowanie	24

Wstęp

Przekazujemy Państwu raport „Pranie pieniędzy”. To już drugi z serii raportów opracowanych z inicjatywy kancelarii Chmielniak Adwokaci. W tym roku materiał powstał przy współpracy kancelarii oraz firmy Kroll Ontrack, światowego lidera w zakresie odzyskiwania danych i informatyki śledczej. Specjaliści Kroll Ontrack podzielili się z nami ważnymi informacjami i danymi, które wzbogaciły warstwę merytoryczną raportu m.in. o zagadnienia związane z analizą cyfrowych dowodów nadużyć.

Tegoroczny raport dotyczy zjawiska prania pieniędzy. To niewątpliwie jedna z najniebezpieczniejszych oraz najbardziej skomplikowanych patologii w sferze przestępczości gospodarczej ostatnich lat zarówno w Polsce, jak i na świecie.

Chcemy przybliżyć specyfikę prania pieniędzy, pokazać dane odnoszące się do tego przestępstwa oraz wskazać na przestępstwa, z którymi pranie pieniędzy wiąże się najczęściej.

Zapraszamy do lektury, wyrażając nadzieję, że będzie ona dla Państwa ciekawa i wartościowa.



Część pierwsza 1

Definicja

Pranie pieniędzy jest zjawiskiem w polskich realiach prawnych stosunkowo młodym. Pierwsze jego symptomy były zauważalne dopiero pod koniec lat osiemdziesiątych XX stulecia¹.

Ten typ przestępstwa związany jest bowiem z powstaniem nowoczesnego rynku finansowego, rozwojem nowych technologii informatycznych, wykorzystywanych zarówno przez sektor bankowy, jak i służących zbieraniu informacji przez organy skarbowe oraz rozbudową systemów podatkowych i z jednoczesnym zjawiskiem istnienia szarej strefy w gospodarce.

Dla uniknięcia nieporozumień należy wyjaśnić, że termin „pranie pieniędzy” jest mylący, gdyż „praniu” mogą podlegać nie tylko pieniądze, ale także inne aktywa, na przykład instrumenty finansowe, czy papiery wartościowe.

Pomimo stosunkowo niedługiego okresu funkcjonowania tego zjawiska w Polsce, pranie pieniędzy stało się jednym z najbardziej skomplikowanych i niebezpiecznych zagrożeń występujących w obszarze tak zwanej przestępczości gospodarczej. Wpływa na to zarówno złożoność samego procesu prania pieniędzy, jego częsta zależność od wielu innych przestępstw (tak zwanych przestępstw bazowych) oraz, nierzadko, międzynarodowy charakter.

1 J. Długosz, w: System Prawa Karnego. Tom 9. Przestępstwa przeciwko mieniu i gospodarce, pod Redakcją R. Zawłockiego, s. 564.

Przedmiotem prania pieniędzy mogą być “środki płatnicze, instrumenty finansowe, papiery wartościowe, wartości dewizowe, prawa majątkowe lub inne mienie ruchome lub nieruchomości” pochodzące bezpośrednio lub pośrednio z popełnienia czynu zabronionego.

Uchwała SN z 18.12.2013
Sygn. I KZP 19/13

Pranie pieniędzy znalazło się wśród sześciu typów przestępstw (obok korupcji, naruszenia regulacji, sprzeniewierzenia funduszy, kradzieży własności intelektualnej i zmowy rynkowej), wymienianych jako zagrożenie w 2013 r. przez przedstawicieli większej liczby przedsiębiorstw z całego świata (także z Polski), niż liczba przedsiębiorstw, jakie zostały faktycznie dotknięte takimi przypadkami w 2012 roku.

Reakcją na kształtującą się patologię jest system regulacji prawnych, których zadaniem jest zarówno zapobieganie, czy też przeciwdziałanie praniu pieniędzy, jak i wprowadzanie sankcji karnych w związku z popełnieniem przestępstwa prania pieniędzy.

Próbując oddać charakterystykę zjawiska prania pieniędzy należy najogólniej wskazać, że polega ono na podejmowaniu szeregu czynności zmierzających do nadania cech legalności składnikom majątkowym, pochodzącym z przestępstwa, czyli wprowadzeniu nielegalnie uzyskanych wartości majątkowych do legalnego systemu finansowego i w ten sposób ich legalizowaniu².

Aż 62,6 procent badanych przez Kroll Ontrack w USA zatrudnionych jako tzw. compliance officer (odpowiedzialnych za monitorowanie przestrzegania przepisów i regulacji w przedsiębiorstwie) uważa pranie pieniędzy za istotne zagrożenie, związane z korupcją.

Źródło: 2014 Anti-Bribery and Corruption Benchmarking Report

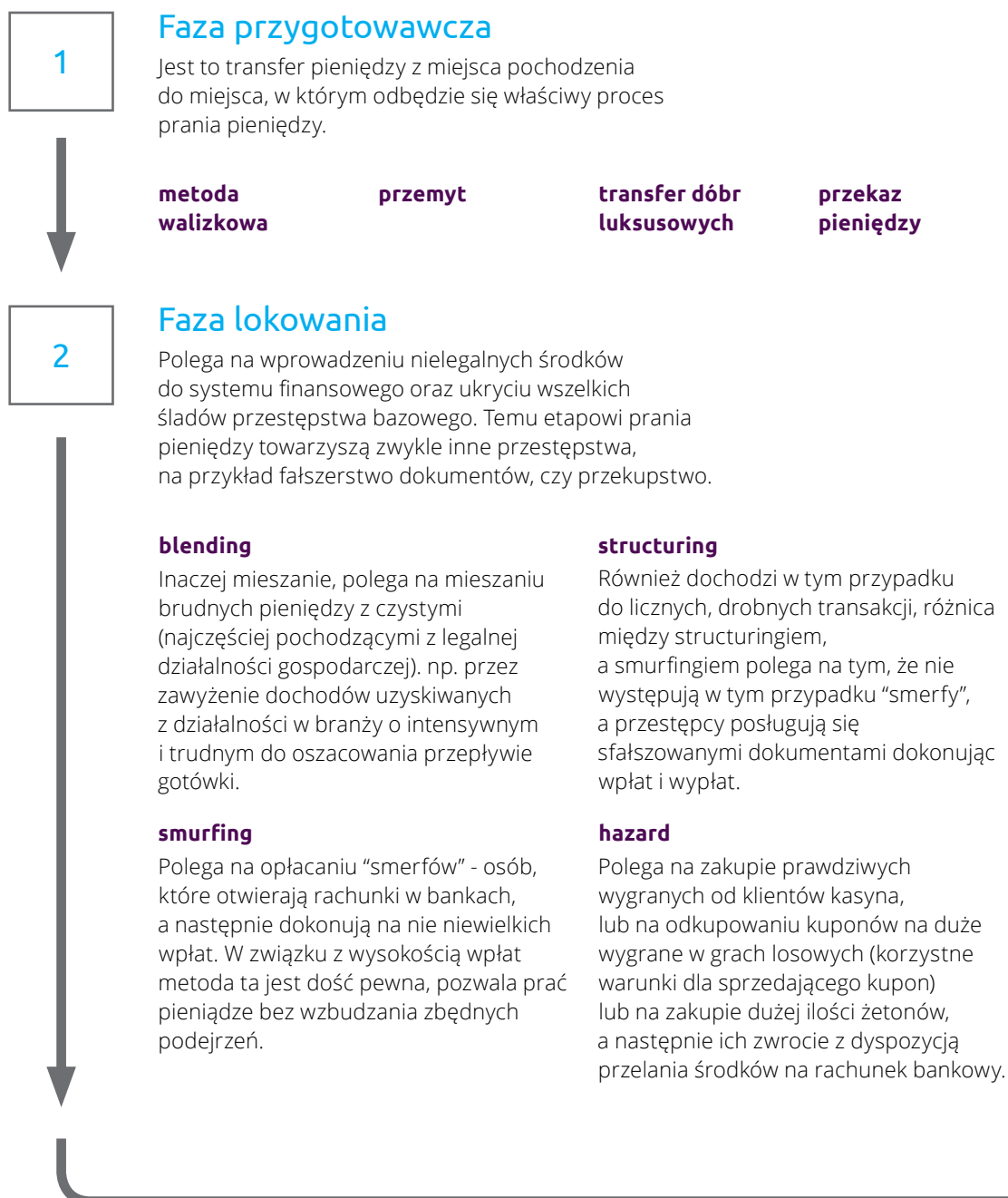
² J. Długosz, w: System Prawa Karnego. Tom 9. Przestępstwa przeciwko mieniu i gospodarcze, pod Redakcją R. Zawłockiego, s. 577.



Etapy i metody

Pranie pieniędzy jest procesem skomplikowanym i cechuje się wielofazowością oraz długotrwałością. Jego celem jest zerwanie więzi pomiędzy przestępstwem bazowym a pochodzącymi z niego brudnymi pieniędzmi, przy zachowaniu maksymalnej kontroli nad tymi pieniędzmi przez sprawcę.

Proces prania pieniędzy może zostać podzielony na 4 fazy.



3

Faza maskowania

Ma na celu ukrycie nielegalnego źródła pochodzenia środków wprowadzonych do systemu finansowego. Polega na przeprowadzaniu dużej liczby transakcji między różnymi kontami, najczęściej w różnych bankach.

skrzynka rozdzielcza

zasilanie rachunku kwotami niskimi - poniżej progu wymagającego rejestracji. Po osiągnięciu odpowiedniej sumy, środki przelewane są na inny rachunek

przelew na nieistniejące konto

najczęściej nieistniejącego nawet klienta

realizacja czeków podróżnych

w celu otrzymania gotówki

4

Faza integracji

Polega na tworzeniu pozorów legalnego pochodzenia pieniędzy. Metody stosowane w tej fazie służą umieszczaniu brudnych pieniędzy w legalnym obrocie gospodarczym. Po dokonaniu tej fazy odróżnienie środków legalnych od nielegalnych staje się praktycznie niemożliwe.

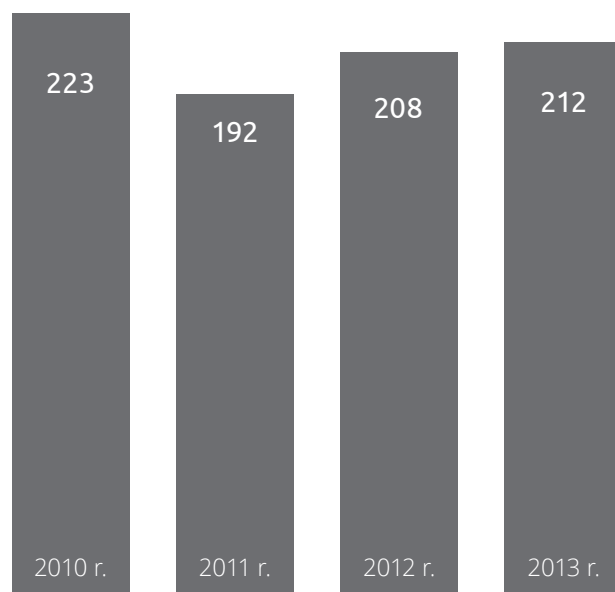


Sprawcą przestępstwa prania pieniędzy „może być również sprawca czynu zabronionego, z którego popełnieniem związana jest korzyść stanowiąca przedmiot czynności wykonawczej.”

Uchwała SN z 18.12.2013 Sygn. I KZP 19/13

Pranie pieniędzy w liczbach

W 2013 roku prawnicy kancelarii Chmielniak Adwokaci odnotowali wzrost liczby postępowań karnych wszczynanych w sprawach o przestępstwa prania pieniędzy w stosunku do roku 2011 i roku 2012.



Liczba wszczętych postępowań przygotowawczych dotyczących przestępstwa prania pieniędzy w okresie 2010-2013

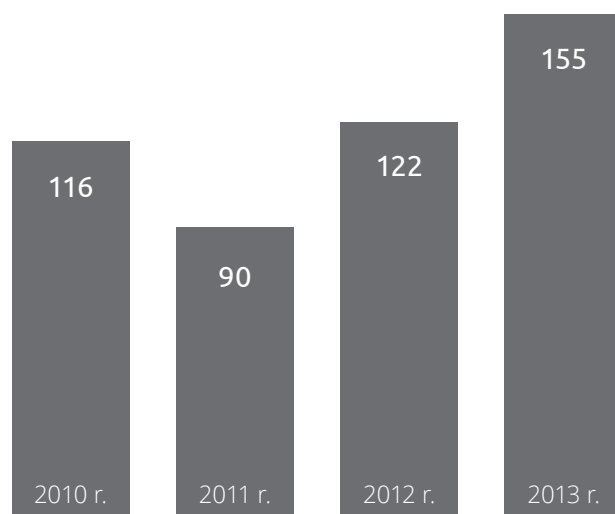
Źródło: GIIF na podstawie danych z Prokuratury Generalnej

Okolo
15 250 000 000,00 zł
- łączna kwota
wartości
majątkowych,
będących
przedmiotem
podejrzenia
przestępstwa prania
pieniędzy, objętych
zawiadomieniami
przekazanymi
w 2013 r. przez
GIIF do właściwych
prokuratur.

Źródło: GIIF

W 2013 roku w związku z podejrzeniem prania pieniędzy wszczęto 212 postępowań przygotowawczych, sporządzono 65 aktów oskarżenia wobec 198 osób oraz wydano 37 wyroków, skazując 129 osób.

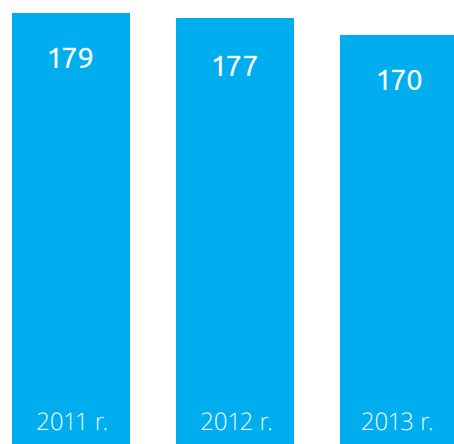
Źródło: GIIF na podstawie danych z Prokuratury Generalnej



Liczba postępowań w sprawach o pranie pieniędzy wszczętych przez Policję

Źródło: Policja

Spadła natomiast liczba wszczynanych postępowań sądowych o te przestępstwa. Zjawisko to potwierdzają zarówno statystyki, jak i praktyka. Może być ono podyktowane długotrwałością postępowań karnych prowadzonych przez organy ścigania.



Liczba wszczętych postępowań sądowych dotyczących przestępstwa prania pieniędzy w okresie 2011-2013

Źródło: GIIF na podstawie danych z Ministerstwa Sprawiedliwości

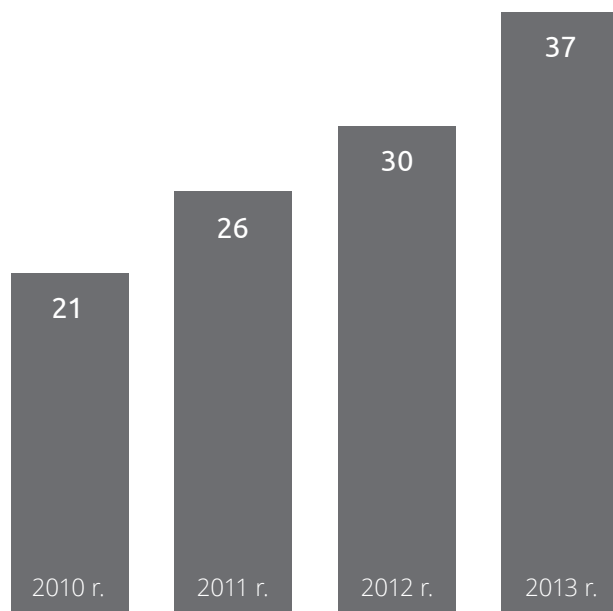
W 2013 r. Policja wszczęła aż o 27% więcej postępowań w sprawach o pranie pieniędzy niż w 2012 r.

Źródło: Policja

W 2013 r. wszczęto 170 spraw sądowych o pranie pieniędzy wobec 524 osób.

Źródło: GIIF na podstawie danych z Ministerstwa Sprawiedliwości

Z badań przeprowadzonych przez prawników Chmielniak Adwokaci wynika, że 2013 rok przyniósł także wzrost liczby wyroków skazujących w sprawach o pranie pieniędzy.



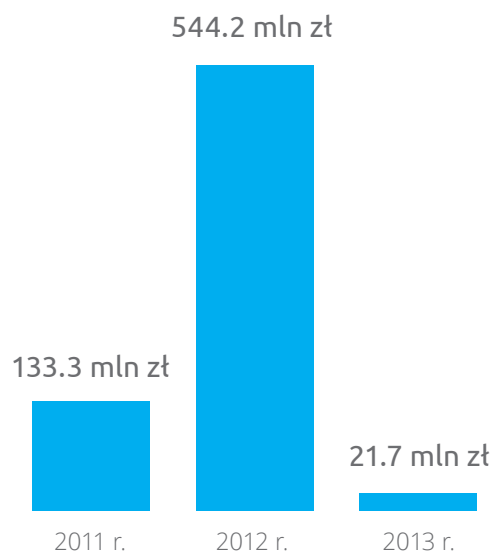
Liczba wyroków skazujących za pranie pieniędzy

Źródło: GIIF na podstawie danych z Prokuratury Generalnej

Wyniki kontroli NIK prowadzonych w pięciu urzędach kontroli skarbowej wykazały, że w 2011 r. dla Skarbu Państwa odzyskano 22,7% kwoty zaniżeń VAT, 8,8% w 2012 r. oraz 4,8% w I półroczu 2013 r.

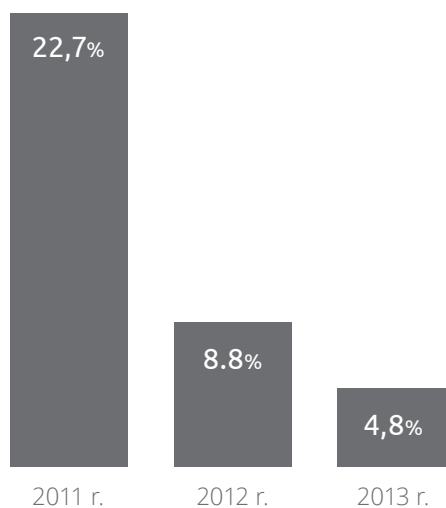
Źródło: GIIF

Wartym odnotowania zjawiskiem w 2013 roku jest natomiast spadek zarówno orzekanych przez sądy przepadków mienia, jak też kwot odzyskiwanych przez Skarb Państwa.



Wysokość orzeczonego przepadku mienia w sprawach o pranie pieniędzy w okresie 2011-2013

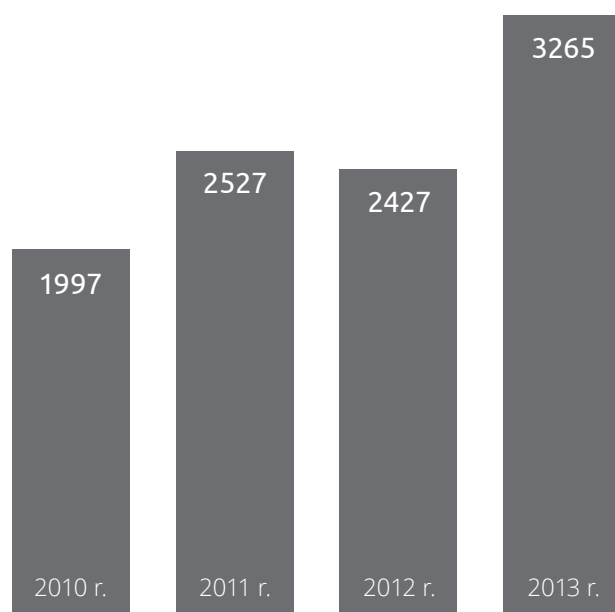
Źródło: GIIF na podstawie informacji z Ministerstwa Sprawiedliwości



Procent odzyskanych kwot zaniżeń VAT ustalonych przez urzędy kontroli skarbowej w okresie 2011-2013

Źródło: NIK

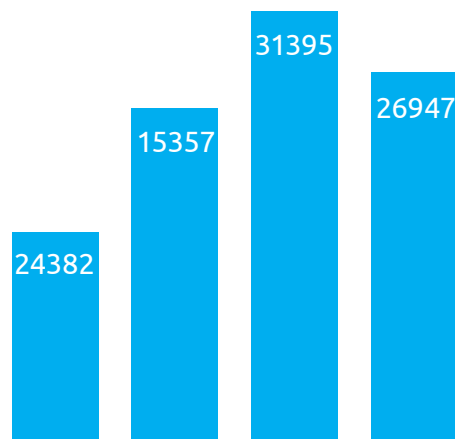
Oprócz działalności organów ścigania, znaczącą rolę w zwalczaniu przestępczości finansowej, w tym prania pieniędzy odgrywa Generalny Inspektor Informacji Finansowej. Prowadząc badania dotyczące 2013 roku, prawnicy kancelarii Chmielniak Adwokaci odnotowali znaczącą aktywność GIIF również w związku ze sferą prania pieniędzy. Świadczy o tym między innymi liczba zawiadomień o działalności i transakcjach podejrzanych tzw. SAR-ów (Suspicious Activity Reports) zarejestrowanych w systemie informatycznym GIIF, która w badanym okresie wyniosła 3 265 i w stosunku do roku 2012 wzrosła o ponad 30 procent, a w stosunku do roku 2010 o ponad 60 procent.



Dynamika zmiany liczby otrzymanych przez GIIF zawiadomień opisowych o działalności i transakcjach podejrzanych w okresie 2010 – 2013

Źródło: GIIF

W 2013 r. aż 26 925 transakcji zostało oznaczonych przez GIIF jako podejrzane o pranie pieniędzy (STR-ML), a 22 jako podejrzane o finansowanie terroryzmu (STR-TF).



Dynamika zmiany liczby otrzymanych przez GIIF informacji o pojedynczych transakcjach podejrzanych

Źródło: GIIF

Pranie pieniędzy to nie tylko polski problem. Odsetek przedsiębiorstw z całego świata, jakie zostały narażone na oszustwa związane z praniem pieniędzy wynosił w 2013 roku 3 procent i wzrósł o 2 procent w porównaniu do roku 2012.

Aż 11 procent firm na całym świecie w 2013 roku uważało, że zagrażają im oszustwa związane z praniem pieniędzy. W 2012 roku takie zagrożenie dostrzegało jedynie 4 procent ankietowanych.

Przestępstwa bazowe dla prania pieniędzy

Z doświadczenia prawników kancelarii Chmielniak Adwokaci wynika, że jednymi z najczęściej występujących przestępstw bazowych dla prania pieniędzy są przestępstwa karne skarbowe, a w szczególności te polegające na uszczupleniu podatku VAT.

Badania potwierdzają, że w kręgu największego zainteresowania służb skarbowych pozostaje proceder fikcyjnych transakcji, potwierdzanych fałszywymi fakturami.

Z danych Ministerstwa Finansów wynika, że w 2013 r. urzędy kontroli skarbowej przeprowadziły prawie 10,2 tys. postępowań kontrolnych. Dokonały one 3,7 tys. przeszukań i oględzin, a 7 tys. razy wystąpiły do instytucji finansowych o udzielenie informacji stanowiących tajemnicę bankową – wynika ze sprawozdania z działalności kontroli skarbowej za rok 2013.

Przestępstwa tego typu przybierają różne formy. Począwszy od najmniej skomplikowanych, polegających na zakupie przez przedsiębiorcę jednej lub kilku faktur celem zmniejszenia obciążeń podatkowych, a skończywszy na stworzeniu zorganizowanych struktur przestępczych, w celu wyłudzenia nienależnych zwrotów VAT.

W 2013 roku prawnicy kancelarii Chmielniak Adwokaci zaobserwowali zjawisko rosnącej przestępczości związanej z oszustwami w podatku VAT, zmierzające bądź do fikcyjnego obrotu towarami, bądź też do wielokrotnego obrotu tymi samymi towarami.

W 2013 r. wykryto 154,6 tys. fikcyjnych faktur wystawionych na łączną kwotę 19,7 mld zł.

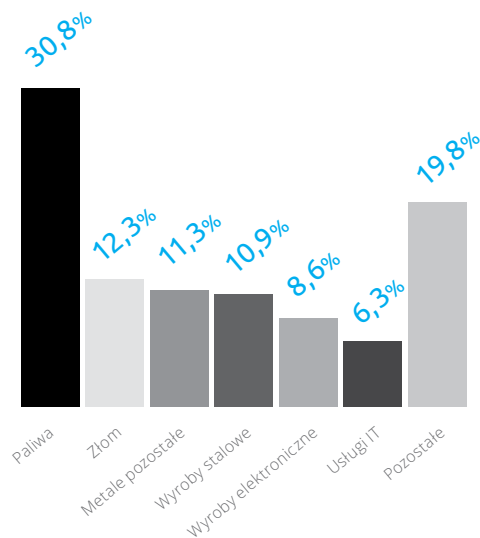
Źródło: Ministerstwo Finansów

Taka działalność potocznie jest nazywana karuzelą podatkową. Bierze w niej najczęściej udział grupa kilku lub kilkunastu firm z kilku państw Unii Europejskiej, które zawierają pozorne transakcje. Firmy te są zazwyczaj powiązane personalnie i kapitałowo, co umożliwia sterowanie pozorowanymi transakcjami. Pomysłodawca całej operacji bardzo często pozostaje anonimowy.

Z doświadczenia prawników kancelarii Chmielniak i Adwokaci wynika, że niejednokrotnie zdarza się, iż ogniwami karuzeli są uczciwi przedsiębiorcy nieświadomie wciągnięci w nielegalny proceder. Firma, która w nieuczciwy sposób zyskuje na takich transakcjach, najczęściej znika, zaś zarzuty stawia się przedstawicielom innego przedsiębiorcy z łańcucha, często nieświadomego procederu, w jaki został wciągnięty.

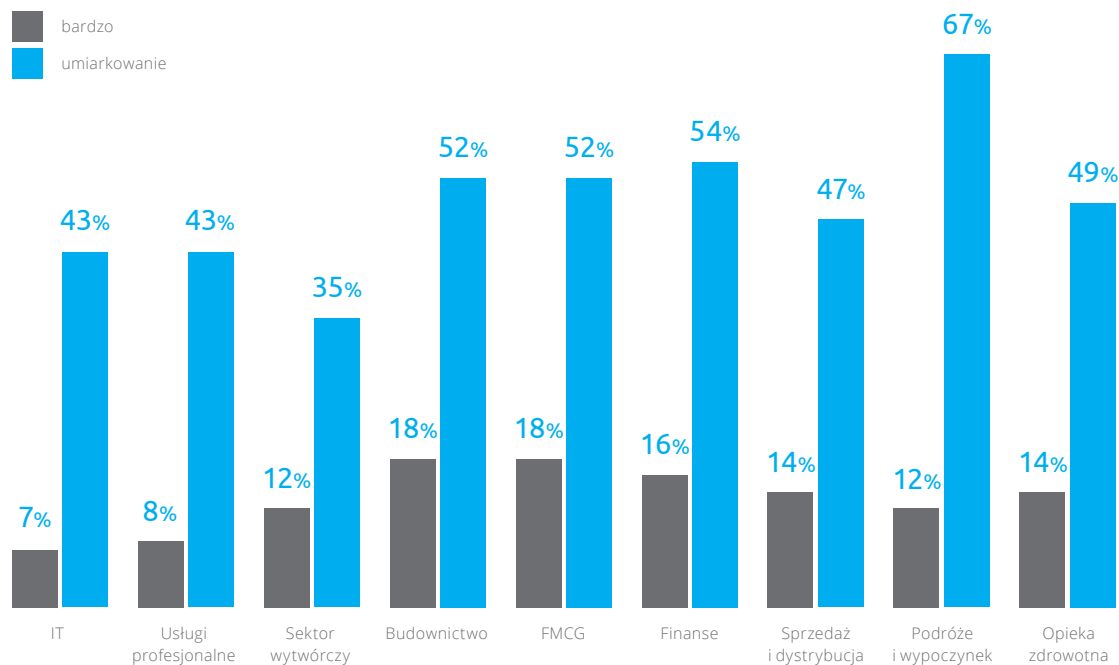
W 2013 roku obszarami szczególnie narażonymi na działalność przestępczą w ramach przestępstw podatkowych dotyczących wyłudzenia zwrotu podatku VAT były branże związane z obrotem paliwami, złomem, sprzętem elektronicznym, alkoholem i tytoniem, handlem narkotykami oraz z grammi losowymi i zakładami wzajemnymi.

W 2013 roku aż 73 procent firm w Europie padło ofiarą różnego typu nadużyć, w tym także związanych z praniem pieniędzy. Światowa średnia dla tego wskaźnika wynosi 70 procent. W przypadku aż 77 procent europejskich firm, zagrożenie oszustwami w minionym roku wzrosło. Najpowszechniejszym czynnikiem mającym wpływ na ten wzrost, była złożoność systemów IT, która leżała u genezy aż w 37 procentach przypadków.



Obszary ryzyka nieprawidłowości podatkowych w 2013 r.

Źródło: Ministerstwo Finansów
Departament Kontroli Skarbowej



Dane ukazujące procentowy udział poszczególnych branż z całego świata, jakie były bardzo oraz umiarkowanie narażone na nadużycia w 2013 roku

Źródło: 2013-2014 Global Fraud Report

Część druga **2**

Pranie pieniędzy, wraz z szeregiem innych przestępstw gospodarczych, stanowi problem, z jakim borykają się firmy na całym świecie. Kroll Ontrack bada to zjawisko już od siedmiu lat, obserwując stały wzrost w jego obszarze. W tej części raportu skupimy się na światowych i europejskich statystykach, związanych z problemem nadużyć, w tym także z praniem

pieniędzy oraz na cyfrowych dowodach tych przestępstw. Przybliżymy też działania z zakresu informatyki śledczej i electronic discovery (ediscovery), które bardzo często są niezbędne przy wykrywaniu oraz analizie wszelkich nadużyć.

Liczba nadużyć i koszty z nimi związane wzrosły znacząco w 2013 roku.

Jak wynika z badań przeprowadzonych przez Kroll Ontrack przedsiębiorstwa na całym świecie, w tym także w Polsce, zanotowały wzrost nadużyć praktycznie w każdym z obszarów tj.: kradzież informacji, korupcja, kradzież własności intelektualnej, naruszenie przepisów prawa, konflikt interesów, zмова rynkowa, sprzeniewierzenie funduszy firmy, pranie pieniędzy.

Aż 70 procent firm przyznaje, że w 2013 roku ucierpiało na skutek przynajmniej jednego nadużycia. Wśród głównych powodów takiego stanu rzeczy, badane przedsiębiorstwa wskazują na: złożoność infrastruktury IT, dużą rotację pracowników, a także wchodzenie na nowe rynki o podwyższonym stopniu ryzyka.

Odsetek firm określających się jako „podatne na nadużycia”, wzrósł w stosunku do roku 2012. Inwestycje jakie zostały poczynione by chronić przedsiębiorstwa przed tego typu zagrożeniami są nadal niewielkie, szczególnie jeżeli mowa o firmach europejskich.

Odsetek przedsiębiorstw dotkniętych wymienionym nadużyciem

	2013	2012
Kradzież aktywów fizycznych	28%	24%
Kradzież informacji	22%	21%
Konflikt interesów kadry zarządzającej	20%	14%
Oszustwo ze strony sprzedawcy, dostawcy lub na polu zamówień publicznych	19%	12%
Wewnętrzne przestępstwo finansowe	16%	12%
Naruszenie regulacji lub przepisów prawnych	16%	11%
Korupcja, łapówki	14%	11%
Kradzież własności intelektualnej	11%	8%
Zmowa rynkowa	8%	3%
Sprzeniewierzenie funduszy firmy	8%	
Pranie pieniędzy	3%	1%

Źródło: 2013-2014 Global Fraud Report

Z roku na rok współczynnik nadużyć rośnie, a aż 73 procent europejskich przedsiębiorstw, które brały udział w badaniu Kroll Ontrack przyznaje, że przynajmniej raz w przeciągu 2013 roku ucierpiało z tego tytułu (podczas gdy światowa średnia stanowi 70 procent). Na starym kontynencie częściej niż w innych częściach świata zdarza się m.in. kradzież informacji. Stanowi ona aż 25 procent odnotowanych przypadków nadużyć. W światowych statystykach kradzież informacji plasuje się na drugim miejscu w rankingu i dotyczy więcej niż jednej na pięć firm.

Odsetek firm uważających się za wysoce narażone na wymienione typy nadużyć

	2013	2012
Kradzież informacji	21%	7%
Korupcja, łapówki	20%	10%
Kradzież aktywów fizycznych	18%	6%
Kradzież własności intelektualnej	8%	7%
Oszustwo ze strony sprzedawcy, dostawcy lub na polu zamówień publicznych	18%	5%
Naruszenie regulacji lub przepisów prawnych	18%	5%
Konflikt interesów kadry zarządzającej	17%	4%
Zmowa rynkowa	14%	5%
Sprzeniewierzenie funduszy firmy	13%	
Pranie pieniędzy	11%	4%

Źródło: 2013-2014 Global Fraud Report

Wiele firm nie jest przygotowanych na sytuację, w której coś pójdzie źle

Na przestrzeni 2013 roku w Europie, podobnie jak na całym świecie, nadużycia stały się bardziej powszechne. W porównaniu do roku 2012, odnotowano wzrost w każdym z badanych obszarów. Kradzież fizycznych aktywów wzrosła z 23 procent do 28 procent, kradzież informacji z 18 do 25 procent, konflikt interesów wzrósł z 13 do 21 procent, a wewnętrzne oszustwa finansowe z 12 do 17 procent. Podobnie rzecz ma się ze stratami przedsiębiorstw z tytułu nadużyć. Wzrosły one z poziomu 0,8 do 1,2 procent przychodów rocznie. Firmy w 2013 roku czuły się zdecydowanie bardziej narażone na powyższe zagrożenia (77 procent), niż w roku ubiegłym (56 procent).



Pomimo ewidentnie narastającego problemu nadużyć, poziom przygotowania firm na to zagrożenie, jest daleki od zadowalającego. Spora część przedsiębiorstw nie planuje inwestycji w tym obszarze w najbliższym czasie. Europejczycy, w porównaniu z innymi regionami świata planowali zainwestować najmniej w obronę czy zapobieganie oszustwom

w 2014 roku. Wyjątek stanowią wydatki na kontrolę finansową oraz kontrolę zarządzania. Jeśli firmy europejskie chcą poważnie myśleć o swoim bezpieczeństwie, będą musiały poświęcić temu aspektowi zdecydowanie więcej uwagi.

	lata: 2012-2013	lata: 2011-2012
Powszechność: odsetek firm, które ucierpiały na skutek nadużycia	73%	63%
Obszary najczęstszej straty: odsetek firm, które odnotowały straty finansowe z powodu nadużycia	kradzież aktywów fizycznych lub akcji (28%), kradzież informacji (25%), konflikt interesów kadry zarządzającej (21%), wewnętrzne oszustwa finansowe (17%), oszustwa ze strony sprzedawcy, dostawcy, na polu zamówień publicznych (17%)	kradzież aktywów fizycznych lub akcji (23%), kradzież informacji (18%)
Wzrost zagrożenia: firmy, które odnotowały wzrost ryzyka wystąpienia nadużyć	77%	56%
Główne czynniki wzrostu zagrożenia: najczęstszy powód prowadzący do nadużyć i odsetek firm, które ucierpiały na skutek tego czynnika	złożoność infrastruktury IT (37%)	złożoność infrastruktury IT (27%)
Straty finansowe: średnia wartość przychodu utracona na skutek nadużycia	1,2%	0,8%

Źródło: 2013-2014 Global Fraud Report

Człowiek wewnątrz

Dane Kroll Ontrack pokazują, że osoby mające dostęp do istotnych dokumentów, planów, raportów, jak również osoby tworzące je, a zatem mające możliwość zmanipulowania ich, powinny być kontrolowane.

Aż 72 procent ankietowanych przyznało, że ich firma uciepiała na skutek nadużycia, w które zaangażowany był przynajmniej jeden pracownik firmy. Często jest to kilku pracowników, którzy współpracują ze sobą. Wśród przedsiębiorstw, w których sprawca był znany, w 32 procent przypadków był to ktoś z wyższego lub średniego szczebla zarządzania, w 42 procent przypadków sprawcą okazał się pracownik niższego szczebla.

Bardzo duża część nadużyć jest wykrywana wewnętrznie. Ponad połowa, bo aż 52 procent przypadków zostaje wykryta przez kadrę zarządzającą, 51 procent przez audyt wewnętrzny, a tylko 10 procent przez audyt zewnętrzny. Powiadomienia ze strony kadry zarządzającej i audyty wewnętrzne są niezbędne

do walki z nadużyciami, jednak w przypadku, gdy któryś z pracowników jest w nie zaangażowany, mechanizm ten może nie zadziałać. Audyt wewnętrzny z mniejszym prawdopodobieństwem wykaże wówczas, że w oszustwo zaangażowani są przedstawiciele kadry zarządzającej czy managerowie. Dla ujawnienia procederu niezbędni są wówczas informatorzy. Wśród przedsiębiorstw, które uciepiała na skutek nadużyć, 32 procent przyznało, że do wykrycia doszło właśnie dzięki informatorom. Ich wskazówki miały znaczenie aż w 42 procent przypadków, w których w sprawę zamieszany był zarząd wyższego lub średniego szczebla.

Co zrobić w przypadku podejrzenia nadużycia?

W przypadku podejrzeń odnośnie prania pieniędzy bądź innego nadużycia, należy ustalić odpowiedzi na kilka pytań:

- czy istnieją dowody na to, że doszło do nadużycia?
- ile osób może być zaangażowanych w proceder?
- od kiedy trwa proceder?
- czy takie działania miały miejsce wcześniej? Jeśli tak, to czy za każdym razem te same osoby są zamieszane?
- jak duża jest skala nadużycia – jak dotkliwe są konsekwencje dla firmy?

W przypadku niewystarczającej wiedzy i doświadczenia w przeprowadzaniu wewnętrznych dochodzeń, warto skorzystać z pomocy specjalistów. Wówczas wszystkie czynności przeprowadzane będą przez osobę niezależną, całkowicie spoza środowiska firmy. Minimalizuje to zagrożenie sytuacją, w której mogłoby dojść do ostrzeżenia osób zamieszanych w sprawę i niszczenia dowodów. Specjaliści są w stanie przeprowadzić wszelkie działania bez wiedzy pracowników firmy.

Przy przeprowadzaniu tego typu dochodzeń pomocne są usługi informatyków śledczych oraz electronic discovery.

Analiza dokumentów

Współczesne przedsiębiorstwa funkcjonują w dużej mierze w oparciu o elektroniczny obieg dokumentów. Codziennie pracownicy generują duże ilości emaili, dokumentów Word, arkuszy kalkulacyjnych, baz danych, prezentacji, wiadomości tekstowych, itp.

W większości dokumenty te nie są usuwane i archiwizuje się je, gdyż mogą się okazać przydatne w przyszłości. Bywają przechowywane na wszystkich urządzeniach, na jakie pozwala dzisiejsza technologia, czyli na komputerach stacjonarnych, laptopach, tabletach, pendrive-ach, smartfonach, a także w chmurze. Gdy zachodzi potrzeba odnalezienia konkretnej informacji czy pliku, pojawia się problem w postaci przejrzenia ogromnej ilości dokumentów, gdyż nie wiadomo gdzie dokładnie znajdują się ważne w danym przypadku dane. Angażowanie zespołu ludzi, którzy mieliby przeglądać i analizować dokumenty to proces kosztowny i mogący potrwać kilka tygodni czy nawet miesięcy. Z pomocą w takich sytuacjach przychodzą usługi ediscovery, czyli electronic discovery.

Bez względu na to, czy chodzi o wewnętrzne dochodzenie czy poszukiwanie dowodów, które mają następnie być przedstawione w procesie sądowym, technologia ediscovery pozwala na:

- zidentyfikowanie i zebranie dokumentów,
- wyłuskanie istotnych danych,
- przedstawienie dowodów.

W takich krajach, jak Stany Zjednoczone czy Wielka Brytania, ediscovery jest obowiązkowym elementem postępowań prawnych. Obejmuje ono zbieranie i dostarczanie dowodów przed rozprawą sądową bądź w ramach sporu prawnego. W pozostałych krajach firmy podejmujące aktywną postawę w zarządzaniu ryzykiem, wykorzystują technologie ediscovery w ramach wewnętrznych procesów kontroli, w celu zapewnienia zgodności z przepisami i wykrycia przestępstw, takich jak np.: korupcja, zachowania sprzeczne z zasadami konkurencji, czy pranie pieniędzy.

Ediscovery umożliwia przedsiębiorstwom rutynową weryfikację dokumentów. Podczas takich kontroli warto skupić się przede wszystkim na operacjach wysokiego ryzyka czy działaniach związanych z zawieraniem transakcji. Szybka reakcja na wykryte nieprawidłowości i działania sprzeczne z regulacjami oraz polityką firmy, może uchronić przedsiębiorstwo przed zagrożeniem. Usługa ediscovery pozwala także na przeprowadzenie wewnętrznego dochodzenia w momencie pojawienia się podejrzenia o możliwości popełnienia przestępstwa (np. dzięki informatorowi). Ta sama technologia wykorzystywana jest podczas fuzji firm, zarówno w kontekście dopełnienia należytej staranności, jak i po to, by mieć pewność, że działania są zgodne z przepisami. Usługi ediscovery wspierają postępowania w zakresie odpowiedzialności za produkt, naruszenia prawa ochrony konkurencji lub sporów dotyczących papierów wartościowych.

Znaleźć igłę w stogu siana

Doskonałe uzupełnienie ediscovery stanowi informatyka śledcza. Działania ekspertów z tej dziedziny są niezbędne, gdy dowody dokonania przestępstwa znajdują się na urządzeniu elektronicznym i należy odtworzyć proces korzystania z danego sprzętu lub przeprowadzić analizę szczątkowych czy też usuniętych danych. Informatyka śledcza to dostarczanie elektronicznych środków dowodowych, czyli zespół działań i czynności, polegających na zabezpieczeniu, przeszukiwaniu i wykrywaniu dowodów nadużyć i przestępstw dokonanych z użyciem komputera lub innych urządzeń elektronicznych.

Dzięki informatyce śledczej można odtworzyć kolejność działań na urządzeniu elektronicznym użytkownika w czasie, odpowiadając na pytania: „kto?”, „co?”, „gdzie?”, „kiedy?”, „jak?” na podstawie informacji normalnie niejawnych dla użytkowników i administratorów systemu. Można ustalić zatem cały łańcuch zdarzeń związany z danym urządzeniem i znaleźć „igłę w stogu siana”. Ekspert z zakresu informatyki śledczej pomoże ustalić, kiedy dokument był modyfikowany, przez kogo był edytowany lub też usunięty. W niektórych przypadkach analiza może wymagać wykorzystania specjalistycznych narzędzi do łamania haseł lub do uzyskania dostępu do zaszyfrowanych danych. Z usług informatyki śledczej bardzo często korzysta się przy sprawach dotyczących przywłaszczenia tajemnicy handlowej, nadużyć korporacyjnych, bezprawnego rozwiązania stosunku pracy, molestowania seksualnego, pornografii dziecięcej lub orzeczeń rozwodowych.



Cyfrowe odciski palców

Postawieni przed zadaniem znalezienia istotnych dowodów nadużyć, prawnicy i śledczy powinni wziąć pod uwagę kilka kluczowych obszarów, w których dowody elektroniczne mogą się znajdować. Cenne źródła dowodowe mogą obejmować maile i załączniki, dokumenty związane z codzienną działalnością gospodarczą, dokumenty operacyjne, dowody kopiowania dokumentów, dane z historii przeglądarek internetowych, znaczniki daty i czasu, dane z kosza, a także wiadomości z czatów elektronicznych.

Firma Kroll Ontrack wielokrotnie zajmowała się zdobywaniem cyfrowych dowodów w sprawach takich jak:

- kradzież własności intelektualnej,
- oszustwo,
- obrona w sprawach karnych,
- włamania wewnętrzne i zewnętrzne,
- pochodzenie dokumentów,
- i wiele innych.

Zgromadzenie dowodów najczęściej polega m.in. na zabezpieczeniu nośników danych i stworzeniu dwóch kopii binarnych dla każdego nośnika. Jeden z wykonanych obrazów nośnika używany jest do analizy danych pod kątem poszukiwania określonych z góry kryteriów, drugi obraz nośnika zostaje zabezpieczony. W przypadku wystąpienia poszukiwanych danych, stanowi on materiał dowodowy.

Cykl czynności związanych z informatyką śledczą:

- zabezpieczenie danych z dostępnych nośników,
- przygotowanie kopii, na której pracują specjaliści,
- odfiltrowanie nieistotnych danych (plików należących do systemu operacyjnego oraz typowych programów czy powtarzających się plików),
- analiza zebranych dowodów pod kątem prowadzonej sprawy,
- przedstawienie raportu,
- udostępnianie i prezentacja danych oraz opiniowanie w sprawie sądowej.

We wszystkich dochodzeniach i sprawach, które są przedstawiane przed sądem, pochodzenie dowodów ma zasadnicze znaczenie, zwłaszcza jeśli chodzi o dowody pozyskane ze sprzętów elektronicznych. Istotne jest, aby przy zbieraniu takich danych, stosowane były odpowiednie procedury, gdyż zwykłe kopiowanie pliku lub wiadomości e-mail może prowadzić do zarzutów o manipulację. Cały proces zbierania dowodów powinien być przeprowadzony zgodnie z autoryzowanymi zasadami przeprowadzania dochodzeń. Według nich, dysk twardy powinien np. być zabezpieczony poprzez pobranie pełnego obrazu oraz zabezpieczenie go tzw. sumą kontrolną. Suma kontrolna jest unikatowa dla obrazu i może być w każdej chwili sprawdzona. Zmiana choćby jednego znaku w dokumencie spowoduje, że suma kontrolna ulegnie zmianie. W przypadkach, w których nie jest możliwe wykonanie obrazu nośnika, można zastosować technikę kopiowania plików i zabezpieczyć je sumą kontrolną.

Nigdy nie należy udostępniać nośnika, na którym mogą znajdować się dowody osobom, które nie wiedzą jak właściwie zabezpieczyć sprzęt. Rodzi to ryzyko manipulacji oraz zniszczenia dowodów, a tym samym trudniejszą pracę dla informatyka śledczego.

Dochodzenia w sprawach związanych z praniem pieniędzy

W takich przypadkach, pierwszym działaniem specjalistów będzie uzyskanie pełnego obrazu zasobów IT i używanych aplikacji. Rozważyć należy następujące kwestie:

- czy przelewy zostały wykonane za pomocą systemów SWIFT lub podobnych?
- jak obsługiwano konta?
- jeśli przelewów dokonano w formie elektronicznej, jakie zapisy kontrolne i rejestrowe są przechowywane?
- jakie procedury autoryzacyjne zastosowano dla przelewów?
- jakie podstawowe systemy bankowości i rachunkowości były używane podczas operacji?
- jakie systemy komunikacji były wówczas w użyciu (e-mail, telefony komórkowe i inne urządzenia, zdalny dostęp, Skype, Lync, nagrania głosowe)

Działania informatyków śledczych mogą być jawne lub ukryte, w zależności od okoliczności. W tego typu procedurach ważne jest, aby jak najwięcej danych zostało zabezpieczonych już na początku, w celu uniknięcia jakiegokolwiek formy ich zmiany bądź zniszczenia.

Zabezpieczone informacje mogą być badane globalnie oraz pod kątem śladów zostawionych przez konkretne osoby, na podstawie obecności danych transakcji lub za pomocą kryterium daty i godziny. W niektórych wypadkach, jak np. pranie pieniędzy na skalę międzynarodową, dochodzenie może wymagać wszczęcia dochodzeń pomocniczych oraz jednoczesnej pracy informatyków śledczych w innym kraju. Dochodzenie może być bardzo złożone i wymagać działania na wszystkich poziomach, aby osiągnąć zamierzony cel.



Studium przypadku obrazujące rolę dowodów elektronicznych

Eksperti dziedzin prawnych, komentując dochodzenia dotyczące podejrzeń prania pieniędzy w instytucjach finansowych, twierdzą, że jest bardzo trudno wykazać odpowiedzialność karną pracowników lub menadżerów banków. W sprawach o naruszenie przepisów dotyczących przeciwdziałaniu prania pieniędzy, problemem jest brak jasności w kwestii czy osoby te świadomie zignorowały prawo.

Dla zespołów prawnych poszukujących dowodów nadużyć, poczta elektroniczna jest cennym źródłem informacji. Wiadomość e-mail może stanowić dowód w postaci tzw. „dymiącego pistoletu” (ang. Smoking gun evidence) i okazuje się niezbędną podczas śledztw dotyczących „przestępstw białych kołnierzyków” jak np. oskarżeń dotyczących wykorzystania poufnych informacji, łapownictwa, korupcji urzędników,

defraudacji środków finansowych, oszustw i działań kartelowych.

Oczywiście poczta elektroniczna jest coraz częściej zastępowana przez mniej formalne techniki komunikacji, jak wiadomości tekstowe, komunikatory czy sieci społecznościowe, które także należy wziąć pod uwagę, poszukując dowodów nadużyć.

Do spektrum elektronicznych śladów, należy dodać jeszcze informacje związane z kopiowaniem danych, historie przeglądarek internetowych, znaczniki czasowe czy też ślady pozostałe w koszu systemowym.

Podejrzenie prania pieniędzy w instytucji finansowej w Wielkiej Brytanii

Na komputerach klienta pewnego banku przeprowadzono działania z zakresu informatyki śledczej. Klient ten, poinformowany przez bank o podejrzeniu prania pieniędzy przez swoich pracowników, zdecydował się udostępnić swoje zasoby IT w celu przeprowadzenia dochodzenia. Wstępna analiza jednego z wyselekcjonowanych komputerów wykazała, iż do komputera podłączono dysk USB

o dużej pojemności. Idąc tym śladem specjaliści informatyki śledczej zbadali dysk USB i wykazali, że osoba korzystająca z komputera brała udział w defraudacji środków finansowych, kradzieży i przenoszeniu środków na zagraniczne konta bankowe.

Studium przypadku dotyczące fałszowania korespondencji

Fałszowanie korespondencji, sprawa CCE vs Komputronik

Firma Clean & Carbon Energy stwierdziła w raporcie giełdowym, iż Komputronik wypełnił niezgodnie z umowami weksel o zapłatę 4 mln zł (to jeden z weksli byłej firmy Karen, którego spłaty domaga się poznański dystrybutor od CCE). Według Komputronika zarzut był nieprawdziwy. Sprawa trafiła w końcu do sądu.

Firma Clean & Carbon Energy ujawniła maile, które miały udowodnić, że Komputronik używa weksli Karenu niezgodnie z wcześniejszymi ustaleniami.

Komputronik od początku twierdził, że korespondencja została spreparowana. Na jego zlecenie ekspertyzy w tej sprawie dokonał Kroll Ontrack. Z przeprowadzonego przez Kroll Ontrack raportu wynikało, że w opublikowanych przez CCE mailach zmieniano treść i temat, pojawiły się także wiadomości, które nie zostały napisane przez ich rzekomych autorów. Kroll Ontrack udowodnił, iż doszło do sfalszowania maili wysyłanych przez wiceprezesa Komputronika oraz pracownika byłej firmy Karen, a cała sprawa miała swój dalszy ciąg w prokuraturze.

Podsumowanie

W przygotowanym przez nas Raporcie staraliśmy się Państwu naświetlić proceder prania pieniędzy i pokazać, że pranie pieniędzy jest problemem globalnym. Nie dotyczy on jedynie obszaru jednego kraju, czy nawet obszaru Europy, lecz rozciąga się na cały świat.

Jak pokazuje niniejszy Raport, globalny charakter prania pieniędzy cechuje różnorodność. Dotyczy on bowiem wielu gałęzi przemysłu, handlu czy też sektora usług. Przez to staje się jeszcze bardziej niebezpieczny i coraz trudniejszy do wykrycia.

Rozprzestrzenianiu się tego procederu sprzyjają zaawansowane mechanizmy ekonomiczno-prawne, rozwój technologii, czy też coraz to nowe formy komunikowania się na odległość.

To wszystko powoduje, że wzrost przestępczości w tym zakresie jest faktem. W 2013 r. odnotowaliśmy w Polsce wzrost zarówno popełnianych przestępstw związanych z praniem pieniędzy, jak również wydawanych wyroków w takich sprawach. Rzeczywista skala tego zjawiska pozostaje jednak niezbadana.

Dla firm i instytucji dbających o swoją reputację, dobre imię oraz wiarygodność, umiejętność wykrywania nadużyć, a także wczesnego reagowania na nie jest kluczowa. Zaniechania na tym polu mogą być dla firmy bardzo kosztowne. Dotyczy to nie tylko kwestii finansowych ale także wizerunkowych. Jak wynika z raportu, problem staje się coraz poważniejszy, dlatego firmy powinny uzupełnić swoje procedury bezpieczeństwa o plan działania w przypadku podejrzenia prania pieniędzy czy też innego nadużycia.

Raport powstał przy współpracy kancelarii Chmielniak Adwokaci oraz firmy Kroll Ontrack. Publikacja została opracowana wyłącznie w celach informacyjnych, nie stanowi ona opinii czy też informacji prawnej.

CHMIELNIAK A D W O K A C I

Specjalistyczna kancelaria prawna wspierająca Klientów w sprawach karnych gospodarczych oraz karnych skarbowych. Kancelaria reprezentuje Klientów w postępowaniach sądowych, świadczy usługi doradcze związane z badaniem bezpieczeństwa transakcji gospodarczych, a także prowadzi szkolenia z tematyki prawa karnego, gospodarczego oraz skarbowego.

Kroll Ontrack.

Światowy lider w dziedzinie odzyskiwania danych oraz informatyki śledczej. Firma dysponuje największym i najbardziej zaawansowanym technologicznie w Europie Środkowej i Wschodniej laboratorium odzyskiwania danych i dostarczania elektronicznych środków dowodowych. Kroll Ontrack od wielu lat współpracuje ze służbami bezpieczeństwa, organami ścigania, kancelariami prawnymi i instytucjami chroniącymi prawo w Polsce i na świecie. Pomaga firmom chronić dane i tworzyć właściwie polityki bezpieczeństwa danych.

Chmielniak Adwokaci

40-079 Katowice, ul. Gliwicka 6/2

tel: 032/ 720 12 50

www.chmielniak.com.pl

Kroll Ontrack

40-082 Katowice, ul. Sobieskiego 11

tel: 032/779 99 99

www.krollontrack.pl