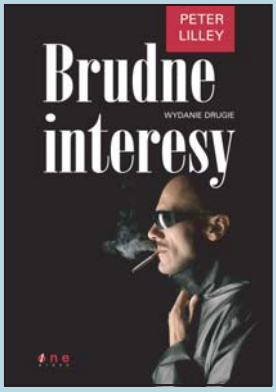
Brudne interesy. Wydanie drugie



Autor: John Paul Mueller
Tłumaczenie: Adam Balcerzak, Marcin Jędrysiak, Tomasz Wasilewski
ISBN: 83-7197-641-0
Tytuł oryginału: Dirty Dealing: The Untold Truth About Global Money Laundering, International Crime and Terrorism
Format: A5, stron: 376

Zbrodnia, terroryzm, narkotyki, handel żywym towarem. To tylko niektóre nielegalne źródła przychodów. Olbrzymie fortuny są pozyskiwane nieludzkimi sposobami. Wystarczy wspomnieć wywożenie młodych kobiet do domów publicznych w Berlinie, uprawy kokainy w Kolumbii, wymuszanie haraczy, porwania dla okupu... Za pośrednictwem systemu bankowego brudne pieniądze zamieniają się w gotówkę, którą widzisz w świetle dnia, trzymasz w kieszeni i na co dzień wydajesz.

Książka jest oparta na faktach, które autor zbierał przez 20 lat współpracy z instytucjami rządowymi zwalczającymi proceder prania brudnych pieniędzy. To ostrzegawczy obraz świata. Poznaj sekrety przerażającego podziemia. Dowiedz się, w jaki sposób rozwinięte i zorganizowane grupy przestępcze podkopują gospodarki państw i ich systemy finansowe.

- Metody prania pieniędzy online: www.zachowajanonimowość.com
- Znane sztuczki: bank-przykrywka, fundusze typu offshore, firmy fasadowe
- Przegląd państw narkotykowych: szokujące fakty i liczby
- Złota maska zbrodni: luksusowe życie narkotykowych baronów
- Przepisy utrudniające pranie brudnych pieniędzy
- Jak rosyjskie podziemie przenika do elit światowego biznesu

Kiedy przeczytasz tę książkę, dostrzeżesz, że świat oplata sieć kryminalnych struktur. I nie chodzi tu wyłącznie o Trzeci świat – zbrodnia panoszy się tuż pod linią Twojego wzroku.

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl

SPIS TREŚCI

Wstęp: Moja śliczna pralnia 7

1. Na początku … **13**

2. N-ty co do wielkości sektor gospodarki światowej ...**51**

3. Prawie jak alchemia **79**

4. Stracone w praniu: pranie brudnych pieniędzy **105**

5. Pełna anonimowość **141**

6. Wyprane w przestrzeni: cyberpranie w XXI wieku ...**171**

7. Terror w praniu **195**

8. Bielsze niż biel — oficjalna odpowiedź **219**

9. Czyste wyjście — strategie przeciwdziałania dla przedsiębiorstw **251**

10. Ostatnie spojrzenie **269**

A Indeks państw **275**

B Katalog sieciowy **349**

C Słowniczek **355**

Bibliografia 363

Skorowidz 367

ROZDZIAŁ SZÓSTY

WYPRANE W PRZESTRZENI: CYBERPRANIE W XXI WIEKU

Istotne problemy życiowe nigdy nie zostają rozwiązane. Jeśli takimi się wydają, to pewny znak, że coś zostało przeoczone. Znaczenie i powód istnienia problemu wydaje się leżeć nie w jego rozwiązaniu, lecz w naszej ciągłej pracy nad nim.

(CARL JUNG)

Kosmos, ostateczna granica… No, w każdym razie do chwili, w której nie pojawi się granica jeszcze bardziej ostateczna. Ocenia się, że do końca 2004 roku na świecie będzie około 945 milionów użytkowników Internetu. Nie można było nic poradzić na to, że w obecnej chwili przestępczość zorganizowana posługuje się najnowszymi osiągnięciami techniki, w tym cyberprzestrzenią. Na początku XXI wieku żyjemy w cyfrowym, globalnym świecie, gdzie wiadomość pisana i przesyłana jest za pomocą poczty elektronicznej i faksu, przelewów pieniężnych dokonuje się na ekranie monitora, coraz większa część handlu prowadzona jest zaś w Internecie. Każdy i w każdym miejscu może wejść do tej globalnej wioski. Wystarczy włączyć komputer, podłączyć się do sieci telekomunikacyjnej i *voilà*! Ściślej mówiąc, nie jest nawet potrzebny zwykły komputer, gdyż można do tego celu użyć palmtopa, a nawet telefonu z usługą WAP.

Szybkość tego ewolucyjnego rozwoju zwiększa się z każdą chwilą. Zorganizowane grupy przestępcze i ludzie piorący brudne pieniądze znajdują się w czołówce tego wyścigu, wykorzystując owe technologie na wiele różnych sposobów. Od opłaconych z góry telefonów komórkowych do anonimowej komunikacji (pamiętaj, że w samych Stanach Zjednoczonych jest ponad 80 milionów abonentów telefonii komórkowej) do transakcji zawieranych przez Internet — wszystkie narzędzia i technologie dostępne dla światowego biznesu trafiają również w ręce światowych przestępców.

Nowa gospodarka stanowi dynamiczny rynek, którego przestępcza brać nie ignoruje, lecz przyjmuje z otwartymi ramionami, przekuwając nowe możliwości w fakty. Skala tego nieregulowanego rynku ułatwia ukrywanie podejrzanych transakcji, procedur i działań. W każdej sekundzie siedmiu nowych użytkowników podłącza się do Internetu. W roku 1998 łączna wielkość sprzedaży internetowej wynosiła 7,8 miliarda dolarów, podczas gdy zaledwie trzy lata wcześniej wynosiła jedynie 0,5 miliarda. W kwietniu 2000 roku 6,6 miliona mieszkańców Rosji miało dostęp do sieci. Departament Handlu USA w wydanej w czerwcu 1999 *The Emerging Digital Economy II* przedstawił opinię, że „do 2006 roku połowa pracowników w Stanach Zjednoczonych zatrudniona będzie w sektorze IT bądź w przedsiębiorstwach wykorzystujących na szeroką skalę technologie, produkty i usługi informatyczne". W kwietniu 2000 roku amerykański sekretarz skarbu, Lawrence Summers, w rozmowie o atakach komputerowych ostrzegł dość optymistycznie, że w ciągu 10 lat bezpieczeństwo informatyczne będzie miało „absolutnie najwyższy priorytet w obliczu wielu zagrożeń biznesu". Opinia ta jest zbyt optymistyczna, gdyż zgromadzone dowody wskazują, że opanowanie najnowszych technik pozwalających na cyberataki i manipulowanie techniczną infrastrukturą zajmie wrogim krajom i zorganizowanym przestępcom znacznie mniej niż dziesięć lat.

Rozwój bankowości elektronicznej oraz systemów płatności elektronicznych tworzy cenne możliwości dla ludzi piorących brudne pieniądze. Główną kwestią, gorąco omawianą przez dostarczycieli

usług z zakresu bankowości internetowej, jest sposób wdrożenia polityki „Znaj Swojego Klienta", kiedy ów klient może być dowolną osobą siedzącą przed monitorem swojego komputera. Bezpieczeństwo i poufność, oferowane przez wszystkie banki sieciowe, są tym, czego właśnie ludzie piorący brudne pieniądze żądają od banków w świecie materialnym. Sercem handlu internetowego jest bowiem pozbawione granic, międzynarodowe środowisko zapewniające:

- efektywność kosztów wykorzystania nowego medium;
- szeroki zasięg Internetu;
- trudność z identyfikacją tożsamości, co dotyczy zarówno dostawcy, jak i klienta;
- anonimowość;
- nowość.

Mieliśmy już okazję zobaczyć, jak przepisy dotyczące prania pieniędzy potrafią się różnić w poszczególnych państwach, więc jeśli masz wielowalutowe konto w internetowym banku w Finlandii, ale mieszkasz w Hiszpanii, trzymając pieniądze przede wszystkim w bankach angielskich, portugalskich i szwajcarskich, to pod prawo której z tych jurysdykcji podpadasz? Oczywiście po raz kolejny jesteśmy świadkami efektywnego wykorzystania międzynarodowych kanałów przerzutowych przez przestępców zorganizowanych, co powinno wywołać odpowiedź w postaci rozwoju i zacieśnienia współpracy pomiędzy poszczególnymi krajami w tym zakresie. Czy jest to jednak możliwe, zważywszy na zróżnicowanie standardów, polityki czy opinii w poszczególnych krajach?

Wśród możliwości, na których przestępcy skupili uwagę, znajdują się:

- wykorzystanie najnowszej technologii w celu unikania i utrudniania oficjalnego śledztwa, zwłaszcza poprzez tworzenie anonimowych i bezpiecznych metod komunikacji;
- osiąganie zysków w wyniku przeprowadzania cyberataków;

- wykorzystywanie usług oferowanych za pośrednictwem Internetu przez „prawdziwych" dostawców, ułatwiające pranie pieniędzy;
- reklamowanie w sieci własnych usług (poprzez firmy fasadowe);
- wykorzystywanie przewagi, jaką dają zaawansowane technologie i systemy międzynarodowej bankowości i handlu, w celu przekazywania pieniędzy i towarów na całym świecie.

Kwestią dyskusyjną jest to, czy w świecie przestępstw informatycznych, w których komputer, sieć czy system stają się bezpośrednim narzędziem zbrodni, ludzie mający odpowiednią wiedzę (hakerzy) nie sprzymierzyli się już z przestępcami lub też nie zostali przez nich zatrudnieni. Podstawowym argumentem przeczącym powyższej tezie jest fakt, że większość ataków ze strony hakerów nie miała charakteru kryminalnego i dokonywana była w celu:

- zrobienia złośliwego żartu;
- udowodnienia, że coś takiego może zostać zrobione;
- przedstawienia swojego stanowiska.

Niestety, pojawia się coraz więcej dowodów na to, że nie zawsze tak to wygląda. Choć nigdy tego nie udowodniono, powszechnie podejrzewa się, że rosyjskie zorganizowane grupy przestępcze stały za osławionym (i skutecznym) atakiem Władymira Lewina na Citibank. Przed skazaniem go 24 lutego 1998 roku w południowej dzielnicy Nowego Jorku Lewin przyznał się do kradzieży 3,7 miliona dolarów z Citibanku, lecz w akcie oskarżenia znajdujemy zarzut kradzieży 400 000 funtów brytyjskich i nielegalnego transferu 11,6 miliona dolarów.

Nielegalne transfery oznaczały pieniądze skradzione przez Lewina za pomocą komputera, lecz później odzyskane przez Citibank. Jeżeli założymy, że w sprawę nie była zamieszana przestępczość

„zorganizowana", wówczas działaniom Lewina nie można przypisać motywu innego niż chęć kradzieży dużej ilości pieniędzy. Kluczowym pytaniem nie jest jednak to, czy było to przestępstwo, lecz to, czy Lewin działał sam, czy może był wykonawcą planu zorganizowanej grupy przestępczej. Jego ataki przeprowadzone zostały w 1994 roku i można się spierać, czy brak informacji o podobnych sprawach był spowodowany tym, że takowe nie istniały, czy raczej tym (Boże uchowaj), że albo nigdy nie odnaleziono sprawcy, albo też zaatakowane firmy nie chciały nagłaśniać swoich problemów. Działania Lewina miały miejsce w XX wieku, co czyni ogłoszone sześć lat później ostrzeżenia Lawrence'a Summersa, w którym mówi on o tym, że w przeciągu dziesięciu lat pojawi się zagrożenie cyberatakami, jeszcze bardziej optymistycznymi.

Jeśli przestępczość zorganizowana działa w tej branży, to istnieje też wiele innych metod i sposobów ataku, które mogą przynieść jej istotne korzyści:

- Istnieje wiele udokumentowanych przypadków kradzieży informacji o klientach, zwłaszcza związanych z kartami kredytowymi. W maju 1997 roku Carlos Felipe Salgado został aresztowany w San Francisco po próbie sprzedaży tajnym agentom FBI 100 000 pakietów danych dotyczących kart kredytowych za sumę 200 000 dolarów. Zatem każdy z pakietów informacji dotyczących jednego klienta był wyceniony na 2 dolary!
- Innym istotnym celem ataku przestępców są systemy należące do rządów i wymiaru sprawiedliwości. Innymi słowy, przestępcy próbują zdobyć informacje o działaniach podjętych przez władze w celu zwalczania przestępczości oraz prania pieniędzy. W ciągu ostatnich kilku lat dokonano milionów ataków na wiele agencji rządowych, w szczególności agencje w Departamencie Obrony Narodowej Stanów Zjednoczonych.

Co więcej, w obu wymienionych sieciach, jak również w tych należących do firm związanych z obronnością, można znaleźć tajne informacje dotyczące operacji i sprzętu wojskowego, które mogą sprzedane temu, kto zaproponuje najwyższa cenę, zwykle zagranicznej organizacji lub obcemu państwu.

- Sieci komputerowe krajowych i zagranicznych korporacji mogą być źródłem istotnych informacji o klientach, produktach i systemach ochrony przed działaniami przestępców.

Możliwości przestępczego wykorzystywania technologii w celu popełniania przestępstw wydają się być nieograniczone. W styczniu 1998 roku niemiecki Verbraucherbank wyznaczył nagrodę w wysokości 10 000 marek niemieckich za informację, która doprowadziłaby do aresztowania szantażującego bank hakera. Haker domagał się okupu w wysokości miliona marek, grożąc, że jeśli nie otrzyma pieniędzy, opublikuje w sieci poufne dane klientów, które wydobył z systemu bankowego. Opowieści o podobnych szantażach, zwłaszcza w odniesieniu do dużych banków, są na porządku dziennym.

Wykorzystanie stron internetowych w charakterze środka umożliwiającego i ułatwiającego pranie pieniędzy zostało wspomniane w niniejszej książce już wielokrotnie, od zawartego w pierwszym rozdziale podsumowania, jakie środki uzyskania anonimowości są dostępne w Internecie, do licznych usług oferowanych przez dostarczycieli usług zagranicznych usług bankowych na ich stronach internetowych. Z całą pewnością Internet stał się istotnym czynnikiem mającym wpływ na wzrost mniej lub bardziej tajemniczych zagranicznych centrów finansowych.

Gdy austriackie banki oferowały konta Sparbuch, w celu ich otwarcia należało udać się do tego kraju lub zapolować na firmę oferującą taką usługę. W jednym i drugim przypadku oznaczało to przedzieranie się przez poufne ogłoszenia i wykonywanie licznych telefonów. Jednakże pod koniec lat 90. XX wieku wszystko uległo

zmianie. Od tego momentu przyszły użytkownik musiał jedynie kliknąć znajdujący się na stosownej stronie przycisk opatrzony napisem „Zamów konto Sparbuch już teraz". To konkretne konto anonimowe należy już do przeszłości, niemniej istnieje wiele alternatywnych rozwiązań, oferowanych w sieci przez tysiące usługodawców, którzy utrzymują, że udostępniają „prawdziwie anonimowe usługi bankowe".

Nawet po wydarzeniach 11 września i ich wpływie na przepisy dotyczące przeciwdziałania praniu pieniędzy ta sama zasada działania odnosi się do banków zagranicznych. Wystarczy kliknąć myszą, by otrzymać pełną ofertę, porównać zakres działania norm prawnych i zamówić coś w sieci.

Co ważniejsze, ze względu na to, że żyjemy po części w wirtualnym, cyfrowym świecie, bardzo wiele miejsc, które są tak tajemnicze, że trudno znaleźć je w atlasie, w jednej chwili stało się bardziej realnymi i znacznie bliższymi dla wszystkich — mają one swoje strony internetowe bądź też zostały przedstawione i opisane na setkach innych. W wielu książkach dotyczących rajów podatkowych znajdują się szczegóły opisujące, jak się tam dostać, w którym hotelu się zatrzymać i gdzie się stołować. Tak pomocne poradniki nie poruszają jednak kluczowej kwestii, jaką jest fakt, że aby otworzyć zagraniczny bank lub firmę, przyszły posiadacz nie musi ruszać się sprzed ekranu komputera.

Jeszcze bardziej zadziwiające jest to, że przestępczość zorganizowana używa Internetu jako środka komunikacji oraz miejsca do reklamowania swojej działalności. Chociaż nie znalazłem nigdy strony, która zawierałaby przycisk opatrzony komentarzem *Kliknij tu, by wstąpić do Jakuzy* (czy dowolnej innej organizacji przestępczej), istnieje kilka stron niebezpiecznie się do tego zbliżających. Kiedyś (do momentu zamknięcia jej przez autora) istniała strona *www.gotti.com* broniąca Johna Gottiego, głowy nowojorskiej rodziny Gambino. Istnieje też strona *www.yakuza.com*, która jest najprawdopodobniej żartem.

W Stanach Zjednoczonych rozmaite gangi wykorzystują sieć, aby promować swoje działania i jednocześnie pogrążać inne gangi. Daje się jednak zauważyć, że zorganizowane grupy przestępcze wykorzystują Internet do celów związanych z ich działalnością. Wiadomo, że tradycyjne mafie stoją za wieloma stronami przyjmującymi w sieci zakłady sportowe. Jeszcze bardziej zuchwałym przypadkiem jest ujawniona w czerwcu 1998 roku sprawa włoskiej mafii z Nowego Jorku, która stworzyła firmę doradczą oferującą innym przedsiębiorstwom pomoc w uporaniu się z „pluskwą milenijną" (ang. *Y2K*). Firma ta, chwaląca się własną stroną i bezpłatną infolinią, opracowała interesujące rozwiązanie wspomnianego problemu. Jej programiści udawali się do firm klientów i tam przerabiali programy fiskalne tak, by kierowały fundusze na zagraniczne konta będące własnością mafii.

Szeroki zakres dostępnych dla wszystkich produktów, usług czy całej infrastruktury informatycznej otwiera przed przestępcami wspaniałe możliwości, przysparzając jednocześnie nowych kłopotów prawodawcom i organom śledczym. W Internecie można znaleźć ogromny wybór:

- darmowych programów pocztowych pozwalających na dostęp do własnej poczty z dowolnego komputera na świecie;
- licznych darmowych programów przekierowujących pocztę z jednego adresu na inne;
- najwyższej jakości oprogramowania szyfrującego;
- programów „anonimizujących".

Dołącz teraz do tych ułatwień inne dostępne usługi:

- Jeśli używasz darmowego konta pocztowego, możesz korzystać z niego w dowolnym miejscu na świecie, na przykład: w publicznej bibliotece, kafejce internetowej czy na komputerze przyjaciela. Można więc założyć takie konto i łączyć się z nim wyłącznie z publicznych terminali, co oznacza, że wytropienie osób komunikujących się w ten sposób jest w zasadzie niemożliwe.

- Duża dostępność telefonów komórkowych z opłaconym z góry abonamentem, które pozwalają na zdobycie środka komunikacji prosto z półki bez ujawniania tożsamości oraz na doładowanie rachunku za pomocą karty kredytowej lub, co rozsądniejsze, gotówki, stanowi zaproszenie do anonimowej komunikacji. Jako że telefon taki jest tani i może być używany na całym świecie, przestępca może kupić go, dzwonić z niego przez dzień lub tydzień, a następnie go wyrzucić.

- Ze względu na częste korzystanie przez policję z podsłuchów przestępcy regularnie skanują swoje domy, biura i pojazdy w poszukiwaniu elektronicznych urządzeń podsłuchowych.

- Wykorzystanie przez przestępców zorganizowanych bezpiecznego szyfrowania elektronicznego w telefonach komórkowych od zawsze utrudniało próby tropienia i analizowania działalności przestępczej przez wymiar sprawiedliwości. Szyfrowanie jest kluczowym narzędziem dla wszystkich zajmujących się technologią komunikacyjną. Legalni usługodawcy korzystają z niego w celu zapewnienia autentyczności, spójności, prywatności i bezpieczeństwa. Z kolei przestępcy mogą swobodnie porozumiewać się między sobą, jeśli komunikacja jest bezpiecznie zaszyfrowana.

  Drugą stronę medalu stanowi fakt, że próby przeciwdziałania, wykrywania, dochodzenia i, ostatecznie, karania przestępców są poważnie ograniczone, jeśli stróżom prawa nie uda się złamać szyfru stosowanego do przekazywania wiadomości.

Jak na ironię, liczne opinie, że nowa, cyfrowa era całkowicie pozbawia ludzi prywatności, zostały wywrócone na lewą stronę przez przestępców oraz ludzi piorących pieniądze, ostrożnie badających dostępne środki i koncentrujących się na ułatwieniach, które raczej ukrywają, niż ogłaszają.

Jeśli uważasz to za sianie paniki, przyjrzyj się uważnie raportowi, który w grudniu 1999 roku pojawił się we włoskiej gazecie *Milano Finanza*. Według niego prokuratura i policja w Palermo odkryły oszustwo na sumę 330 milionów funtów, które stanowiło część zaprojektowanej przez włoską mafię światowej operacji prania pieniędzy. Pieniądze przekazywano między kontami firmy amerykańskiej, która była w rzeczywistości zarejestrowana w Nowej Zelandii i na Kajmanach oraz posiadała konta w Izraelu i Hiszpanii. Po zakończeniu tych transferów pieniądze były składane w Szwajcarii i fizycznie przewożone do banków w Rumunii, Chorwacji, Rosji, Chinach i Liberii. Na jednym z etapów tej podróży pieniądze rozpłynęły się w cyberprzestrzeni i pojawiły się jako zakupione w sieci akcje. Prokurator z Palermo stwierdził, że „dochodzenie pozwoliło odkryć nieuregulowany i pozbawiony granic rynek finansowy, otwarty dla każdego posiadającego możliwość wymiany pieniędzy i akcji w dowolnym celu".

Nie należy jednak pomniejszać potencjału, jaki Internet ma dla kogoś, kto chce wykorzystać go do ułatwienia prania pieniędzy czy też generowania zysków ze zbrodni, które następnie trzeba będzie wyprać. Co więcej, jak zobaczyliśmy na przykładzie tradycyjnych metod prania pieniędzy, prawie zawsze istnieją pewne mechanizmy łączące oba wspomniane problemy. Wśród dostępnych w Internecie stron komercyjnych są też takie, które dają przestępcom istotne możliwości działania. Dla przykładu:

- hazard internetowy;
- pornografia;
- internetowe usługi seksualne;
- seksualne wykorzystywanie nieletnich;
- inne strony komercyjne oferujące nielegalne usługi bądź produkty (takie jak narkotyki bądź organy do przeszczepów).

Analiza czarnej listy FATF (a właściwie, żeby użyć jej prawdziwej nazwy, „listy niewspółpracujących krajów i terytoriów") ujawnia, że nie ma na niej miejsca, które idealnie sprzyja rozwojowi zagrożeń ze strony prania pieniędzy w XXI wieku. W miejsce to może trafić każdy, nie obowiązują w nim żadne wymagania wstępne, podróż do niego jest zaś niezwykle tania. Internet nie ma granic geograficznych i, co ważniejsze, nie obowiązują tam żadne przepisy. Ta nowa cyfrowa gospodarka nie została zignorowana przez brać przestępczą, wręcz przeciwnie: oszuści oraz ludzie piorący brudne pieniądze z radością powitali oferowane przez nią możliwości. W cyberprzestrzeni dostępnych jest wiele okazji, z których jedną stanowią zakłady internetowe.

Kiedy w marcu 2000 roku podejmowałem wstępne badania nad elektronicznym praniem pieniędzy, przeszukiwanie sieci z zapytaniem „*virtual casino*" („wirtualne kasyno") dało 36 000 trafień. Dziś identyczne wyszukiwanie pozwoliłoby na uzyskanie 45 000 trafień[1]. Po wybraniu jednej konkretnej gry (blackjacka) pojawiło się ponad 350 wirtualnych kasyn, wliczając jedno, które skutecznie połączyło grę w blackjacka z kwintesencją rozrywek dla dorosłych. Całkowita liczba wirtualnych kasyn musi być liczona w setkach, jeśli nie w tysiącach. Strony te próbują naśladować wygląd gry w prawdziwych kasynach i podobnie jak te ostatnie pragną wyciągnąć od Ciebie jak najwięcej pieniędzy. Ocenia się, że w 2002 roku internetowi szulerzy stracili 3 miliardy dolarów, ale taka przegrana oznacza, że łączny przepływ pieniędzy musiał być dużo wyższy i, faktycznie, ocenia się go na około 6 miliardów dolarów. W rzeczywistości nikt jednak nie wie, ile tego typu stron istnieje w sieci, jak wielu graczy je odwiedza ani jak wysoki jest poziom zawieranych transakcji. Izba Reprezentantów USA w wielu różnych dokumentach opisała hazard internetowy jako raj dla prania

[1] Wpisanie hasła „hazard online" daje 44 800 wyników, a dla hasła „wirtualne kasyno" wyników jest 1330. Dla porównania wpisanie angielskiego hasła „*gambling on-line*" („hazard online") daje 738 000 wyników — *przyp. red.*

pieniędzy, władze tego kraju próbowały też zakazać takiego hazardu, początkowo powołując się na ustawę o przelewach federalnych z 1960 roku. Mimo to próby wprowadzenia takiego ograniczenia przypominają do złudzenia wysiłki króla Kanuta chcącego zawrócić morskie fale.

Próby zakazania hazardu internetowego w Stanach Zjednoczonych zmusiły legalne firmy hazardowe do udania się za granicę. W ten sposób legalni usługodawcy zostali uwikłani w działania znacznie bardziej podejrzanych firm w tajemniczych i egzotycznych miejscach. Spora część tych kasyn internetowych (ocenia się, że nawet 75%) znajduje się podobno w „rejonie Karaibów". Muszę przy tym nadmienić, że kilka odwiedzanych przeze mnie stron nie miało podanego adresu albo były praktycznie niemożliwe do zlokalizowania. Jak w przypadku wszystkiego, co mieści się w odległych miejscach za granicą, posiadanie przez firmę adresu wcale nie musi oznaczać, że jest on prawdziwy. Rządy takich krajów czerpią duże zyski z rejestrowania tego typu działań: około 75 000 dolarów za strony przyjmujące zakłady sportowe i co najmniej 100 000 za wirtualne kasyna. W roku 1999 wiarygodne źródła podały, że udzielające takich licencji kraje zgarniają z tytułu rocznych opłat ponad 1,5 miliona dolarów miesięcznie.

Oczywiście z wirtualnych kasyn korzystać może każdy człowiek na świecie, nie mając pojęcia, jakie przepisy (jeśli w ogóle jakieś) odnoszą się do takiej działalności. Istnieją przy tym dodatkowe zagrożenia, takie jak bezprawne wykorzystanie danych z kart kredytowych przez administratorów tego typu stron. Podobnie jak w przypadku „prawdziwych" kasyn, dają one wspaniałe możliwości prania pieniędzy. FBI w przynajmniej jednym śledztwie namierzyło zagraniczne strony internetowe oraz ich powiązania z oszustwami na przelewach i praniem pieniędzy. Wśród zamieszanych w to jurysdykcji znajdowały się: Curacao, Holandia, Antyle, Antigua i Dominikana. Dodatkowo FBI prowadzi też dochodzenia w sprawie związków między hazardem internetowym a przestępczością zorganizowaną (co podkreśla stwierdzenie, że cyberprzestrzeń pod niejednym względem przypomina prawdziwe życie).

„Podwójny cios" zadawany przez kasyna, które są rozproszone za granicą, w połączeniu ze słabymi (lub nieistniejącymi) procedurami sprawdzania historii klienta w tych obszarach prawnych sprawiają, że uregulowanie rynku hazardu internetowego jest w zasadzie niemożliwe.

Co więcej, wcześniej zakładaliśmy, że kasyna internetowe naprawdę prowadzą interes, czyli przyjmują zakłady od rzeczywistych klientów. Wydaje mi się (i na pewno nie jest to oryginalna myśl), że jedną z bezbłędnych metod skutecznego prania pieniędzy jest utrzymywanie przez robiącą to osobę, że prowadzi ona hazardową stronę w sieci (choć w rzeczywistości nie zajmuje się tym) i założenie w tym celu konta bankowego. Daje to doskonały pretekst do pojawiania się na tym koncie pieniędzy napływających z różnych stron świata, jak również dokonywania podobnych wypłat. Jeszcze jedną korzystną dla piorących pieniądze ludzi komplikacją jest możliwość wykorzystania przez kasyno małych zagranicznych banków, które prowadzą współpracę korespondencyjną z dużymi instytucjami finansowymi w Stanach Zjednoczonych (co stwarza powszechnie znane ryzyko prania pieniędzy, nierozerwalnie związane z bankowością korespondencyjną).

Nie wiadomo zatem, czy należy się śmiać, czy płakać, kiedy w internetowym kasynie natrafi się na coś takiego (jest to parafraza właściwej zawartości strony):

> *Jesteśmy jednym z cieszących się największym zaufaniem kasyn w Internecie (…) nasza licencja została wydana przez (nazwa zagranicznej jurysdykcji) (…) Aby grać o pieniądze, musisz wpierw zarejestrować kredyt w naszym kasynie. Stawki i wypłaty rozliczane są w dolarach amerykańskich. Możesz płacić za pomocą:*
>
> 1. *Ważnej karty kredytowej.*
> 2. *Przelewu bankowego lub pocztowego.*
> 3. *Przekazów pieniężnych Western Union.*
> 4. *Przekazów bankowych, czeków bankowych lub czeków potwierdzonych przez bank.*
> 5. *Czeków osobistych.*

6. *Możesz przysłać gotówkę. Nie zalecamy tej formy płatności, gdyż jest ona niemile widziana przez lokalne władze. Prowadzimy legalną działalność i nie zamierzamy brać udziału w żadnym praniu pieniędzy. Płatność gotówką powinna być zatem realizowana wyłącznie w ostateczności. Nie przyjmujemy jednorazowo (podkreślenie własne) stawek większych niż 5000 dolarów.*

Wygrane i niewykorzystana część kredytu będą wysyłane tą samą metodą, jaka została użyta do otwarcia kredytu (…) będą one przelane na użytą kartę kredytową lub wysłane przelewem bądź za pośrednictwem czeku firmowego.

Sugeruję zatem wysyłać za każdym razem sumy odrobinę mniejsze niż 5000 dolarów, rozegrać kilka gier (do wyboru jest ich około 20) i zażądać, by pozostałe pieniądze zostały przelane z powrotem za pomocą czeku.

Jest kwestią dyskusyjną, jakie przepisy „Znaj Swojego Klienta" realizowane są przez strony oferujące hazard internetowy. Teoretycznie każda z takich stron powinna postępować zgodnie z regułami ZSK obowiązującymi w jurysdykcji, w której została zarejestrowana. W tym schemacie (z braku lepszego słowa) istnieją dość poważne luki, dla przykładu:

- Większość kasyn internetowych (jeśli nie wszystkie) zarejestrowana jest w jurysdykcjach, w których przepisy o przeciwdziałaniu praniu pieniędzy są relatywnie słabe. Pamiętaj, że na liście krajów i terytoriów niewspółpracujących z FATF znajdują się m.in.: Nauru, Niue, St Kitts i Nevis oraz St Vincent i Grenadyny.
- Nawet jeśli przepisy dotyczące prania pieniędzy są w danym miejscu dobrze rozwiązane, jest mało prawdopodobne, że istnieją tam regulacje odnoszące się do kasyn internetowych, zwłaszcza w zakresie należytego starania o klienta.

- Do powyższych czynników dodać należy brak przejrzystości, która jest kluczowym elementem tego typu zagranicznych rajów finansowych.

Tak więc w praktyce, opierając się na próbce odwiedzonych przez nas kasyn (rzecz jasna, wyłącznie dla celów badawczych), ogólne zasady ZSK sprowadzają się do tego, że obsługa kasyna przyjmuje za prawdę wszystko, co mówi klient, i robi bardzo niewiele lub zgoła nic, by potwierdzić te informacje.

Jako potencjalnych przestępców piorących brudne pieniądze szczególnie zainteresowała nas hazardowa strona działająca za pośrednictwem skrytki pocztowej (ang. *PO box*) w Antigui. Sama strona przyjmuje płatności czekami i przekazami bankowymi, przekazami American Express lub w gotówce. Płatność gotówką jest akceptowana, jeśli tylko realizowana jest za pośrednictwem przesyłek poleconych. Następnie firma zwraca pozostałe na koncie środki przez „prywatnego kuriera w dowolne miejsce na świecie, gratis" lub wysyła „dowolną sumę przesyłką poleconą, całkowicie gratis".

Z anonimowością tą łączy się atrakcyjność odległych miejsc, w których można obstawiać zakłady, jak również wykorzystanie zaszyfrowanych danych. Tak więc podczas gdy prawodawcy, stróże prawa i wymiar sprawiedliwości wciąż koncentrują się na wyeliminowaniu umożliwiających pranie pieniędzy luk w „rzeczywistym" świecie, ich przeciwnicy wykorzystują w optymalny sposób wszystko to, co jest dostępne w cyberprzestrzeni. Ktoś ma ochotę wytypować zwycięzcę tego wyścigu?

Wysyp stron o tematyce seksualnej w każdej możliwej do opisania odmianie (i wielu takich, które nie nadają się do opisania) stanowi dla przestępczości zorganizowanej wspaniałą okazję do uzyskania wpływów dzięki kontroli roztoczonej nad sektorem usług seksualnych. Ustalono, że każdego roku ilość dostępnej w sieci pornografii wzrasta o 400%. Podczas gdy zwykła pornografia w Internecie stanowi bardzo dochodowy interes, o tyle pornografia z udziałem dzieci jest najczęściej rozprowadzana bezpłatnie.

Jak na razie nie ma dowodów na to, że w działalność taką zamieszana jest przestępczość zorganizowana, lecz jest jedynie kwestią czasu, zanim to się stanie, co przy okazji zwiększy zagrożenie szantażem i wymuszeniami, których właściciele takich stron będą dopuszczać się względem subskrybentów.

Ludzie piorący brudne pieniądze zyskują najwięcej na wzroście popularności bankowości internetowej i systemów płatności elektronicznej. Po pierwsze, należy jednak odróżnić banki, które mają reklamowe strony w Internecie, od takich, które oferują tam usługi. Gwałtowny rozwój serwisów komercyjnych sprawił, że sektor bankowy szybko wkracza na strony oferujące usługi przekazywania pieniędzy. Dość często strony takie są podwykonawcami noszącymi nazwy sprzyjające działaniu w sieci, a świat bankowy postrzega bankowość internetową jako logiczne rozwinięcie bankowości telefonicznej. Ostatnie badania wykazały, że podobnie jak wielkie centra połączeniowe (ang. *call center*) były tańsze niż sieć oddziałów, tak personel obsługujący bank internetowy jest tańszy niż ten obsługujący centrum połączeniowe. Na stronach WWW pojawiają się więc nowe, legalne banki oferujące otwieranie i zamykanie kont, przekazy bezpośrednie, transfery elektroniczne, wydawanie czeków czy zakup papierów wartościowych.

Dodatkowo klienci już istniejących „tradycyjnych" banków są zachęcani, a może raczej nakłaniani, do korzystania z banków przez Internet. Rzadko się zdarza, by przynajmniej raz na miesiąc mój bank nie przysłał mi pisma lub programu komputerowego mającego mnie zachęcić do takiego działania. Ostatnie pismo (któremu towarzyszyła pięknie zapakowana płyta CD) informowało mnie, że ten bezpieczny system umożliwia mi:

- sprawdzenie szczegółów rachunku, w tym aktualnego stanu konta i debetu;
- sprawdzanie ostatniego i przedostatniego wyciągu;
- wydrukowanie informacji o koncie bądź zapisanie ich na dysku mojego komputera;

- płacenie rachunków;
- przemieszczanie pieniędzy między kontami;
- sprawdzanie, poprawianie i anulowanie stałych operacji;
- sprawdzania stałych zleceń.

Czegóż jeszcze mógłbym chcieć? Nie muszę już w ogóle chodzić do oddziału mojego banku. Ale tu pojawia się problem… Jak wszystko w wirtualnym świecie, tak i to eliminuje konieczność bezpośredniego kontaktu. Bank nie może mieć pewności, że osoba po drugiej stronie linii telefonicznej jest ich klientem. Wygląda to raczej tak, jak w przypadku kont Sparbuch, gdzie wystarczyło pojawić się w banku z książeczką i hasłem, by zabrać pieniądze. Z bankowością internetową jest identycznie — dopóki masz hasło dostępu, pieniądze są Twoje.

Podobnie jak w przypadku poczty elektronicznej, klient ma dostęp do swojego konta z dowolnego miejsca na świecie za pośrednictwem rozmaitych usług internetowych, z których żadna nie pozwala usługodawcy sprawdzić, kim jest osoba korzystająca z rachunku. Podsumowując, w przypadku internetowych banków reguła „Znaj Swojego Klienta" zostaje dosłownie wyrzucona przez okno, choć usługodawcy starają się z tego mętnie tłumaczyć. W Japonii zdalne operacje można przeprowadzać wyłącznie na kontach otwartych w tradycyjny sposób, twarzą w twarz. W Belgii nie ma formalnego rozróżnienia pomiędzy sposobami dostępu do konta, więc przepisy o przeciwdziałaniu praniu pieniędzy stosuje się do wszystkich jednakowo. W Stanach Zjednoczonych konta mogą być otwierane przez Internet, jednakże klient musi podać oficjalne numery identyfikacyjne, które są później weryfikowane przez bank. Wszystko to jednak dość mocno mija się z celem. W sieci znalazłem wiele banków, które oferują natychmiastową możliwość prowadzenia operacji przez Internet i istniejących wyłącznie w Internecie. Co więcej, nawet jeśli procedury ZSK są przestrzegane, to w przypadku konta obsługiwanego wyłącznie przez Internet i tak nie dochodzi do bezpośredniego kontaktu z klientem.

Wyobraźmy sobie, że człowiek piorący brudne pieniądze może przedstawić lub też ma dostęp do prawdziwych danych i dokumentów danej osoby, ewentualnie dysponuje podrobionymi papierami. W tym przypadku może on otworzyć tyle kont, ile tylko zapragnie, i wyprać wszystko, co tylko zapragnie. Po raz kolejny pojawia się tu pytanie o kontrolę ze strony władz. Które bowiem państwo jest odpowiedzialne za nadzorowanie internetowych usługodawców? Oficjalna odpowiedź brzmi (jak mniemam), że jednostki oferujące sieciowe usługi finansowe są w danej jurysdykcji podległe tym samych przepisom, co zwykłe banki. Brzmi to rozsądnie do momentu, w którym nie porównamy tego z rzeczywistością, przez co pomysł taki traci sens. Weźmy European Union Bank w Antigui (a właściwie tam zarejestrowany). Bank of England informował potencjalnych klientów o ryzyku inwestowania w EUB, ale w zasadzie nie mógł zrobić nic więcej. Cała idea Internetu polega na tym, że niezależnie od tego, gdzie się znajdujesz, możesz robić interesy z kimkolwiek i gdziekolwiek.

Logicznym rozwinięciem prowadzenia działalności w Internecie jest powstanie powszechnie akceptowanej i przekazywanej cyberwaluty. Przez ostatnie 15 lat środowisko fiskalne doprowadziło nas do sytuacji, w której przeważająca większość pieniędzy ma formę wirtualną. Twoja wypłata przelewana jest na konto i widzisz ją w formie cyfr wydrukowanych na wyciągu czy też wyświetlanych na ekranie bankomatu. Za większość towarów płacisz kartą kredytową lub debetową, kiedy przychodzi rachunek kredytowy, wystawiasz czek, gdy korzystasz z Internetu, płacisz za kupione rzeczy powszechnie akceptowanym kawałkiem plastiku. Następnym oczywistym krokiem jest ustanowienie mechanizmu pozwalającego na transfer pieniędzy bez udziału gotówki. Nosi on wiele różnych nazw: płatność bezgotówkowa, waluta elektroniczna, e-pieniądz, e-gotówka, lecz w rzeczywistości jest to jedno i to samo. Terminem płatności elektronicznych określa się wiele różnych technik i systemów. Za FinCEN:

> *Wspólnym elementem tych systemów jest to, że zostały one stworzone, aby zapewnić użytkownikom natychmiastowy, pewny, bezpieczny i potencjalnie anonimowy sposób transferu środków pieniężnych. Po całkowitym jej wprowadzeniu technologia ta wpłynie na użytkowników na całym świecie, zapewniając oczywiste zyski legalnym przedsiębiorstwom. Jednakże istnieje też możliwość, że ułatwi ona międzynarodowe przemieszczanie nielegalnie pozyskanych funduszy.*
>
> (FINCEN, *MONEY IN CYBERSPACE*, NIEDATOWANY DOKUMENT INTERNETOWY)

Obecnie istnieje szereg firm próbujących sprzedać swój system jako ten, który w przyszłości wyznaczy obowiązujący standard. Jednocześnie promuje się też inne systemy. W tej chwili dostępnych jest około 100 form elektronicznej gotówki, które mogą być wykorzystywane w Internecie. Dla przykładu, jeżeli trafisz na stronę serwisu informacyjnego, możesz założyć za pomocą karty kredytowej elektroniczny portfel, a koszta wyszukiwania i pobierania artykułów będą pobierane z tej elektronicznej skrytki. Kwestie dotyczące wykorzystania takich systemów przez ludzi piorących brudne pieniądze odnoszą się m.in. do następujących problemów:

- Z prawnego punktu widzenia banki oraz instytucje finansowe pełniły coraz ważniejszą rolę w zgłaszaniu podejrzanych transakcji i kontrolowaniu prób prania pieniędzy. Jeśli banki zostaną wyłączone z obiegu pieniądza, wówczas zniesiona zostanie kluczowa instytucja takiej kontroli.
- Jako że dostępne są różne rodzaje systemów płatności elektronicznych, utworzenie jednolitych zasad zgłaszania może okazać się trudne.
- Zasada ZSK może całkowicie stracić znaczenie, gdyż transakcje praktycznie nigdy nie są zawierane twarzą w twarz.
- Kolejnym starym problemem są międzynarodowe kwestie prawne oraz konieczność zapewnienia ściślejszej współpracy pomiędzy poszczególnymi krajami. Jak pisze FinCEN, unikając jakiejkolwiek złośliwości:

> *Obserwowany błyskawiczny rozpad międzynarodowych granic finansowych, będący wynikiem transakcji opartych na płatnościach elektronicznych, daje asumpt do poszerzenia współpracy i zwiększenia wysiłków między instytucjami międzynarodowymi, aby zapewnić jednolitość reguł i standardów. Sytuacja, w której jeden kraj będzie posiadał szczegółowe przepisy, podczas gdy drugi nie będzie miał żadnych, nie odstraszy przestępców finansowych. Nielegalne pieniądze przepłyną po prostu do najsłabszego ogniwa.*
>
> (FINCEN, *MONEY IN CYBERSPACE*, NIEDATOWANY DOKUMENT INTERNETOWY)

Brytyjska NCIS wyraziła swoje oczywiste obawy w wydanym w 1999 dokumencie *Project Trawler: Crime on the International Highways Report*:

> *Można by przypuszczać, że poznanie i wykorzystanie nowych technologii zajmie organizacjom przestępczym nieco czasu. Jednakże rzeczywistość jest zupełnie inna. Po wprowadzeniu w Wielkiej Brytanii przepisów przeciwdziałających praniu pieniędzy w latach 1993 – 1995 gwałtownemu przyspieszeniu uległo przestępcze wykorzystanie słabiej uregulowanych sektorów (w których istniała mniejsza szansa na zdemaskowanie). Rozsądnie jest przypuszczać, że nowy system płatności zostanie wykorzystany w podobny sposób, jeśli pojawią się sprzyjające okoliczności.*

Jedną z kluczowych kwestii, która została zignorowana i podkreślona zarazem, jest to, że aby otrzymać fundusze w formie elektronicznej, przestępca musi przekształcić gotówkę na pieniądze wirtualne, aby zapłacić zaś gotówką, musi dokonać operacji odwrotnej na pieniądzu cyfrowym. W rzeczywistości jedynie pierwsza połowa tego twierdzenia jest prawdziwa. Nie sugerujemy, że wirtualne pieniądze zastąpią czy wyprą materialną walutę, lecz najprawdopodobniej będzie można wykorzystywać elektroniczne pieniądze do kupowania cennych ruchomości, takich jak samochody. W ten sposób możliwe będzie pranie funduszy uzyskanych z prze-

stępstw bez potrzeby przekształcania ich w rzeczywiste pieniądze. Ryzyko związane z wirtualnym pieniądzem polega na jego niezwykłej mobilności oraz anonimowości. Obecna sytuacja, w której nie ma dominującego systemu czy produktu, jest bardzo atrakcyjna dla ludzi piorących brudne pieniądze, gdyż zróżnicowanie systemów i podejścia do nich oznacza brak wspólnych sposobów kontroli czy standardów zapobiegania praniu pieniędzy. W tej chwili wiele form elektronicznej gotówki jest zależnych od środków przekazywanych za pośrednictwem banków lub kart kredytowych. Najlepszym sposobem na osiągnięcie maksymalnego stopnia anonimowości i uniknięcie bezpośredniego kontaktu przy przekazywaniu elektronicznych pieniędzy jest nawiązanie współpracy z internetowym bankiem przez Internet. Dla przykładu, klient odwiedza wirtualny bankomat i uzupełnia swój elektroniczny portfel za pomocą prawdziwych pieniędzy ze swojego konta lub karty kredytowej. Z tego powodu można twierdzić, że elektroniczne pieniądze mogą zostać wykorzystane jako narzędzie na etapie maskowania, lecz nie umożliwiają prania pieniędzy jako takiego.

Prawdopodobny scenariusz może wyglądać tak: fundusze uzyskane z przestępstw są umieszczane w zagranicznym banku lub nawet lokalnej instytucji finansowej w jurysdykcji, w której przepisy dotyczące prania pieniędzy są mało efektywne. Od tego momentu wszystkie operacje dokonywane są za pomocą komputera, gdy bank, w którym złożono pieniądze, dysponuje internetowym systemem bankowym, pozwalającym na przesyłanie elektronicznych pieniędzy. E-gotówka może też zostać zakupiona za pomocą wydanej na to konto karty kredytowej. Przestępca jest następnie w stanie przemieszczać elektroniczne pieniądze szybko i praktycznie anonimowo. Fundusze mogą zostać później użyte do zakupienia portfela papierów wartościowych na całym świecie. Jedyny bezpośredni kontakt następuje w chwili otwierania pierwszego konta, a i to da się ominąć, otwierając je w banku internetowym. Jako że istnienie elektronicznych środków płatności ułatwia to wszystko, nic nie stoi na przeszkodzie, by przestępca zrobił to teraz. I to skutecznie.

Inną formą elektronicznej gotówki są karty chipowe. Były one próbnie wprowadzane w wielu rejonach świata, najczęściej przez firmę Mondex (obecnie stanowiącą część Mastercard International), która, jak mi wiadomo, prowadziła eksperymenty w Wielkiej Brytanii, Australii i Nowej Zelandii. W chwili, gdy piszę te słowa, wielu światowych właścicieli koncesji czeka na wdrożenie tej technologii. Karty te podobne są do elektronicznych portfeli pod tym względem, że po przelaniu na nie funduszy można wykorzystywać je tak, jak karty kredytowe lub debetowe, dokonując zakupów za zawarte na nich pieniądze. Podczas prób w angielskim Swindon ogólne wrażenie nie było szczególnie korzystne, gdyż karty Mondex nie miały przewagi nad standardowymi kartami, a nawet sprawiały więcej problemów, gdyż trzeba było upewniać się, że są one zasilone gotówką.

Jednakże w Australii i Nowej Zelandii możliwe było posiadanie kart nieprzypisanych, które można zasilać za pomocą transferów z innych kart, lecz nie z kredytowych i debetowych kont bankowych. Transfery takie mogły być dokonywane za pośrednictwem telefonu, sieci bądź specjalnego portfela przemieszczającego fundusze z jednej karty do drugiej. Stanley Morris, dyrektor FinCEN, w przemówieniu wygłoszonym w 1995 roku przed Podkomisją Kongresu ds. Bankowości podczas posiedzenia poświęconego przyszłości pieniądza zauważył, że takie karty niosą ze sobą poważne ryzyko prania pieniędzy:

> *Załóżmy, że użytkownik Internetu jest też handlarzem narkotyków lub członkiem gangu przestępców prowadzących inną złożoną działalność. Pomyślcie, jakie zamówienia mógłby taki handlarz przyjmować, jakie towary zamawiać i jakich transakcji dokonywać, gdyby, dla przykładu, mógł on pobrać nieograniczoną ilość gotówki z karty chipowej na komputer, a następnie przekazać te fundusze w dowolne miejsce na świecie, czyniąc to wszystko anonimowo, nie zostawiając za sobą śladu po transakcjach i bez potrzeby korzystania z tradycyjnych instytucji finansowych.*

Lub, jak sam Mondex pisał w zamieszonym na swojej stronie internetowej w 2000 roku materiale reklamowym:

Elektroniczne pieniądze Mondex różnią się od innych kart chipowych tym, że są na tyle bezpieczne i złożone, by pozwolić na przekazywanie elektronicznej gotówki „z ręki do ręki", dokładnie w taki sam sposób, jak przy wręczaniu gotówki członkowi rodziny czy przyjacielowi. Inne karty chipowe działają na zasadzie kart kredytowych czy debetowych i muszą kontaktować się z centralnym systemem komputerowym, przez co umożliwiają jedynie przepływ gotówki od klienta przez sprzedawcę do banku.

Karty Mondex pozwalają również na przechowywanie wielu walut jednocześnie. Oczywiście, jak każdy mechanizm wykorzystywany przez ludzi piorących pieniądze, Mondex i podobne systemy oferują legalnym przedsiębiorcom wspaniałe możliwości oraz usprawnienia. Niestety, nowe osiągnięcia tego typu mogą być również bardzo szybko wykorzystane do celów przestępczych.

Internet i postęp w zakresie systemów płatności elektronicznej nie tylko całkowicie zmieniają sposób prowadzenia interesów na całym świecie, ale również mogą zapewnić (o ile już tego nie zrobiły) istotną możliwość prania pieniędzy w cyberprzestrzeni bez pomocy świadomych wspólników. We współczesnym systemie finansowym w każdym kraju istnieje ścisła kontrola ze strony banku centralnego. W świecie pieniędzy elektronicznych cała idea odrębnego państwa, a co za tym idzie, także systemy regulacyjne, zostają zniesione. Nowy świat handlu elektronicznego nie ma jeszcze mechanizmów pozwalających na monitorowanie czy kontrolowanie prania pieniędzy. Co więcej, banki nie są już potrzebne do przelewania pieniędzy, gdyż każdy może to zrobić za pomocą komputera osobistego przy wykorzystaniu elektronicznej gotówki i przelewów bezpośrednio pomiędzy użytkownikami, bez konieczności włączania w to tradycyjnej instytucji finansowej.

Elektroniczne pieniądze dostępne są teoretycznie w dowolnym miejscu na świecie i mogą być wysłane w dowolne inne miejsce na świata. Na początku XXI wieku przestępcy prawdopodobnie wynaleźli nowy technologiczny wybielacz pozwalający im prać pieniądze jeszcze lepiej.

Jest coś niezwykle smutnego w tym, że zwykłe pranie pieniędzy wciąż panoszy się w najlepsze, jednym z powodów takiego stanu rzeczy jest zaś niemożność ustanowienia międzynarodowych środków zapobiegawczych. Stosowne władze koncentrują się na zagranicznych centrach finansowych, traktując je jako siedliska zarazy w cywilizowanym świecie. Jednakże ludzie piorący pieniądze znajdują się o krok naprzód w stosunku do tego, przemieszczając i piorąc pieniądze w cyberprzestrzeni. Jeśli to pole pozostanie nieuregulowane, przestępcy nie będą musieli korzystać z zagranicznych centrów finansowych. Po co się tak wysilać, jeśli najlepszym narzędziem do prania pieniędzy jest osobisty komputer?

Wszystko, czego potrzebuje osoba piorąca pieniądze, dostępne jest dziś w sieci. Można tam otworzyć konto bankowe, regulować przedsiębiorstwo międzynarodowe, zapisać się do jednego z wielu programów handlu akcjami, kontaktować się za pomocą anonimowych kont pocztowych, handlować przy użyciu dostępnych systemów płatności elektronicznych, przelewać pieniądze przez internetowe kasyna i kolektury sportowe, kupować nieruchomości, przelewać pieniądze przez aukcje, otwierać swoje zagraniczne lub sieciowe banki. Możesz robić tam, co tylko zapragniesz. I cokolwiekby nie mówiły władze, nie istnieją tam granice państwowe, nie wymaga się bezpośrednich spotkań, nie ma doradców zadających dziwne pytania, w sumie jest tam bardzo niewiele przeszkód uniemożliwiających lub utrudniających pranie pieniędzy w przestrzeni.