NBP–Beograd, Vol. IX, No. 2, 99 -110, 2003.

343.53

САВРЕМЕНЕ ТЕНДЕНЦИЈЕ У ПРАЊУ НОВЦА

Горан Бошковић
Полицијска Академија, Београд

Резиме: На основу резултата спроведених истраживања, у раду се износе садржаји који се односе на савремене тенденције у области прања новца, односно специфичне начине прања новца извршене злоупотребом нових технолошких система. Анализирају се карактеристике појединих начина прања новца и могућности злоупотребе електронских система плаћања, у контексту дефинисања превентивних и репресивних мера за супротстављање прању новца у савременом окружењу.

Кључне речи: прање новца, електронски системи плаћања, картице за одлагање новца, Интернет банкарство, електронска готовина, коцкање преко Интернета.

УВОД

Коришћењем нових технолошких система традиционални финансијски инструменти се све више потискују и замењују новим електронским системима плаћања.[1] Нови системи нуде оно што су некада били најбољи атрибути

1 Према истраживањима 85% плаћања у малопродаји у Финској врши се on-line. Steven

MODERN TENDENCIES IN MONEY LAUNDERING

Goran Boskovic
Police Academy, Belgrade

Summary:, This document presents the contents, obtained on the basis of conducted research results, that are related with modern tendencies in the area of money laundering i.e. the specific ways of money laundering conducted by new technological systems. In order to define preventive and repressive measures against money laundering in modern environment, the characteristic of some specific ways of money laundering, and possibilities for misuse of electronic payment systems are analyzed.

Key words: money laundering, electronic payment systems, smart card, Internet banking, electronic cash, Internet gambling.

INTRODUCTION

With new technological systems, traditional financial documents are replaced more and more with new electronic payment systems.[1] New systems offer the best attributes of traditional payment – easy use, anonymity, safety, international transfers,

1 According to researches: 85% of sales in Finland are done on-line. Steven Philippsohn, The

традиционалног плаћања - лакоћу употребе, широку примену, анонимност, сигурност, међународне трансфере, брзину трансакционих услуга, дематеријализацију и неограничену величину трансакције. Примена нових електронских система плаћања носи са собом и одређене ризике, који се односе на могућност злоупотребе ових система у сврхе прања новца. Експерти Групе за финансијске акције идентификовали су следеће ризике[2]:

- немогућност идентификовања и потврђивања лица која користе нове технологије,
- ниво транспарентности трансакција,
- одсуство или неадекватност контроле у вођењу евиденције или извештавању о сумњивим трансакцијама од стране продавца технологије,
- коришћење шифровања на високом нивоу (чиме се блокира приступ судским органима) и
- трансакције које нису обухваћене тренутном легислативом или регулаторним дефиницијама.

Да би се смањили и предупредили ти ризици потребно је изградити систем превентивних и репресивних мера, које ће омогућити ефикасно супротстављање злоупотребама нових система плаћања у сврхе прања новца. Нови технолошки системи плаћања обухватају пружање банкарских услуга преко Интернета, електронску готовину, картице за одлагање новца, коцкање преко Интернета, WAP технологију и картице за електронски трансфер осигурања.[3] У даљем тексту размотрићемо карактеристике и могућности злоупотребе у сврхе прања новца наведених електронских система плаћања.

fast transaction services, dematerialization and unlimited transaction. The application of new electronic payment systems brings along certain risks related with possibilities of misuse these systems for money laundering. Experts of Financial Action Task Force have identificated the following risks:[2]

- Impossibility of identification and confirmation of persons who use new technologies,
- Level of transaction transparency
- Lack of control or inadequate control of evidence keeping or of reporting about suspicious transactions of technology seller
- The use of coding on high level (that blocks access for court organs) and
- Transactions not included by present legislation or regulatory definitions

In order to reduce and prevent these risks, it is necessary to establish a system of preventive and repressive measures that will allow an efficient supression of misuse of new payment systems for money laundering. New technological payment systems include the option of banking services via Internet, WAP technology and electronic transfer insurance cards.[3] In the following part of the paper, we will discuss the possibilities and features of misuse with the purpose of money laundering related to quoted payment systems.

Philippsohn,The dangers of new technology-laundering on the Internet, *Journal of Money Laundering Control*, London, Summer 2001, volume 5, pp. 87-95.

2 Financial Action Task Force, Report on Money Laundering Typologies for 1998-1999, Paris, p.7.

3 WAP технологија омогућава директан приступ Интернету посредством мобилних телефона.

dangers of new technology-laundering on the Internet, *Journal of Money Laundering Control*, London, Summer 2001, volume 5, pp. 87-95.

2 Financial Action Task Force, Report on Money Laundering Typologies for 1998-1999, Paris, p.7.

3 WAP technology allows direct access to Internet via mobile phones

ЗЛОУПОТРЕБЕ КАРТИЦА ЗА ОДЛАГАЊЕ НОВЦА У СВРХЕ ПРАЊА НОВЦА

Картице за одлагање новца (енгл. *smart card*) представљају форму електронског новца који је развијен као алтернатива традиционалним финансијским инструментима.[4] Сличне су кредитним картицама, изузев што располажу новцем у електронском формату који је претходно пребачен са корисниковог рачуна на микрочип. Микрочип на картици чува новчану вредност на картици која се може трошити као новац, јер је вредност на картици задужена од стране финансијске институције. У случају губитка картице, нема губитка за финансијску институцију, већ он постоји само за корисника картице.

Системи картица за одлагање новца су веома разноврсни, и разликују се по специфичним оперативним карактеристикама. Неки од система дизајнирани су тако да обезбеде анонимност у трансакцији, док други прикупљају податке који се могу користити за контролу тока средстава. У већини земаља оператери система картица за одлагање новца поставили су лимите на износ који се може унети на картице.

Ризик злоупотребе картица за одлагање новца у сврхе прања новца, повећава се са постојањем следећих фактора: подизањем њиховог горњег лимита или потпуним отклањањем, директним пребацивањем новца са једне картице на другу без посредства финансијске институције, чиме се онемогућава праћење тока средстава, коришћењем ван територије земље у којој је картица издата, и могућношћу трансфера на картице других оператера. Постојање неког од тих фактора чини картице за одлагање новца погодним оруђем за прање новца.

Да би се смањио ризик злоупотребе картица за одлагање новца потребно је дефинисати скуп мера на превентивном и репресивном плану за супротстављање прању новца. Један број држава (Аустралија, Белгија, Шведска) формирао је истраживачке групе за електронску трговину при влади, које би требало да дефинишу смернице у супротстављању злоупотреби електронских инструмената плаћања у сврхе прања новца. Експерти Групе за финансијске акције дефинисали су следеће мере за супротстављање злоупотреби картица за одлагање новца у сврхе прања новца[5]:

4 Smart card се могу користити и као здравствене картице (Немачка, Канада), на којима се чувају овере здравственог осигурања и медицинска историја.

MISUSE OF SMART CARDS FOR MONEY LAUNDERING

A smart card represents a form of electronic money that is developed as an alternative form to traditional financial instruments.[4] It is similar to a credit card, but it differs from it as it handles money in electronic form, which has previously transferred user's account to an electronic chip. Microchip on the card keeps money value on the card that can be spent as money, because financial institutions charge the card value. In case of losing the card, there are no loses for financial institutions, but they exist only for a user.

Smart card systems are various and they are different from each other in specific operative characteristics. Some of the systems are designed to provide anonymity of transactions and some other collect data for cash flow control. In most countries, smart card operators limit the value you can put on the card.

The risk of smart card misuse for money laundering grows with the existence of the following factors: raising their limit or its complete removal; direct transfer of money from one card to some other without the intervention of a financial institution, by which the tracking of money flow is disabled; if the card is used out of the country where it was issued; the possibility of transferring money on-to cards of other operators. Smart card has become a common means of money laundering because of the existence of some of these factors.

In order to reduce the risk of smart card misuse, it is necessary to define a set of preventive and repressive measures against money laundering. Some of the countries (Australia, Belgium, and Sweden) formed government research groups for electronic trade. These groups should define the measures against the misuse of electronic payment systems for money laundering. Experts of the Group for financial actions have defined the following measures against the misuse of smart card for money laundering:[5]

- Distribution of cards from issuers related to financial institutions and linking with banking accounts,
- Limiting payments to the area of national territory

4 Smart card can be used as health cards (Deutschland, Canada), which keep insurance health verification and medical history.

5 Financial Action Task Force, Report on Money Laundering Typologies for 1998-1999, Paris, p.9.

– дистрибуција картица од стране емитената повезаних са финансијским институцијама и повезивање са банковним рачуном,
– ограничење операција плаћања картицама на националну територију,
– ауторизација и надзор емитената нових технолошких производа јер су мере о спречавању прања новца боље усклађене када се примењују на регулисан и контролисан сектор,
– могуће прилагођавање постојећих мера о спречавању прања новца, посебно у вези са идентификацијом клијента и током контроле, тако да се омогући емитентима нових технолошких производа да помогну компетентним властима да открију кружење анонимних инструмената плаћања у нелегалне сврхе,
– ограничавање функција и капацитета картица за одлагање новца (укључујући максималну вредност и лимите промета као и број ових картица по клијенту),
– захтевање стандардних процедура вођења евиденције за те системе да би се омогућило проучавање, документовање и преузимање релевантних досијеа од стране истражних органа и
– доношење међународних стандарда за ове мере.

ИНТЕРНЕТ БАНКАРСТВО И ПРАЊЕ НОВЦА

Пружање банкарских услуга преко Интернета подразумева да власник има приступ рачуну преко Интернета за обављање одређених трансакција.[6] Трансакционе услуге обухватају широк дијапазон услуга које могу бити електронски трансфери средстава, директна плаћања, издавање чекова, узимање депозита, куповина хартија од вредности, отварање и затварање рачуна и слично. Само присуство банака на Интернету преко web-sajt-ова, без пружања трансакционих услуга не сматра се Интернет банкарством. Један део банака које нуде своје трансакционе услуге преко Интернета су традиционалне банкарске институције које се баве тим послом да би употпуниле своју понуду

5 Financial Action Task Force, Report on Money Laundering Typologies for 1998-1999, Paris, p.9.

6 *За разлику од Интернет банкарства,* on-line банкарство је шири појам који укључује индиректан приступ финансијским услугама, то јест телефоном, аутоматима и преко Интернета.

- Authorization and control of new technological products issuers, because the measures against money laundering are more coordinated if they are taken within a regulated and controlled sector,
- Possible adoption of the present measures against money laundering, especially in the field of client identification and during control. With those measures, issuers of new technological products could help legal authorities discover anonymous payment instruments that are used for illegal purpose.
- Limiting smart card functions and capacitating (including maximal value and turnover limit and the number of these cards per client).
- Requesting standard procedures relating to keeping evidence of these systems in order to study, document and take relevant files by investigating officers and
- Determining international standards for these measures.

INTERNET BANKING AND MONEY LAUNDERING

Offering banking services via Internet means that the owner, when wanting to do some transactions, accesses his account via Internet.[6] Transactions services include a wide area of services such as electronic money transfer; direct payment; check issuing; deposit raising; buying stocks and bonds; opening and closing accounts etc. The presence of banks on the Internet by web sites, without giving transaction services, is not considered Internet banking. A number of banks that offer their transaction services via Internet are traditional banking institutions. They engage in that kind of business in order to complete their offer to potential clients. The rest of the banks are "clean" banks (that offer their services exclusively via Internet).

The client-bank communication is provided by personal computers. The client contacts the Internet

6 On-line banking is broader term in regard to Internet banking and it includes indirect access to financial services by phone, automatic devices or via Internet.

потенцијалним клијентима, а други део су тзв. „чисте" Интернет банке (банке које нуде своје услуге само преко Интернета).

Сам ток комуникације на релацији клијент - банка одвија се преко персоналних рачунара, којима клијент користећи се софтвером за Интернет и приступом мрежи преко провајдера Интернет услуга ступа у контакт са Интернет сервером банке. Клијент уноси на Интернет серверу банке своју личну шифру за идентификацију, преко које се потврђује да је реч о одређеном клијенту. Након потврде да је шифра исправна клијенту се омогућава приступ рачуну. Оваква комуникација на релацији клијент - банка обезбеђује лакоћу приступа преко Интернета, деперсонализацију контакта између клијента и банке и велику брзину електронских трансакција. Иако можемо сматрати да ови фактори доприносе нивоу ефикасности и смањивању трошкова финансијских услуга, они намећу и потенцијалне ризике за злоупотребе Интернет банкарства у сврхе прања новца.

Потенцијални ризици злоупотребе Интернет банкарства у сврхе прања новца односе се пре свега на могућности идентификације клијената и регулаторну и истражну јурисдикцију. Наиме, банка може рутински да потврди да је одређеном рачуну приступљено у одређено време, суму која је укључена у трансакцију, а могуће и корисника (име и број рачуна). Банка може само да претпостави да је рачуну приступио номинални власник, али нема никакав начин да потврди идентитет лица које приступа рачуну и место са којег је обављена трансакција. То практично значи да један појединац може контролисати већи број рачуна истовремено и вршити трансакције са било које локације у свету, а да не привуче пажњу финансијске институције или институција у којима се воде ти рачуни. Регулаторна јурисдикција односи се на давање лиценци и надзор над финансијским услугама које се нуде преко Интернета. Веома је тешко осигурати да финансијске институције поштују адекватне процедуре против прања новца, нарочито када пружају услуге на територији државе у којој се не налази сервер банке, јер не можете забранити грађанима да користе услуге које се пружају преко Интернета. Из перспективе истраге, питање јурисдикције се јавља у односу на чињеницу где је обављена трансакција преко Интернета да би се знало ко је надлежан за поступање у случајевима злоупотреба Интернет банкарства у сврхе прања новца.[7]

7 У том погледу, заједнички извештај Банке Француске и Француске банкарске комисије

bank server accessing the network by Internet service provider and by using software for Internet. Client enters his personal identification code and the Internet bank server confirms that it is the right client. After confirmation the client's access to the account is possible. This client-bank communication allows easy access via Internet, depersonalization between the client and the bank and a high speed of electronic transaction. Although we can consider that these factors contribute to a higher level of efficiency and to reducing financial service costs, they also bring potential risks of Internet banking misuse for money laundering.

Potential risks of Internet banking misuse for money laundering are in most cases related to client identification, and regulatory and investigative jurisdiction. Namely, a bank can confirm that an account was accessed at some time, the sum included in the transaction, and possibly the user (the name and account number). The bank can only suppose that the nominal owner accessed the account, but there is no way to confirm either the identity of the person accessing the account or the place the transaction was done from. In practice, it means that one individual can simultaneously control a number of accounts and that he/she can do transactions from any location in the world, not attracting attention of financial institution or institutions where the accounts are registered. Regulatory jurisdiction is related to license issuing and financial services offered via Internet. It is very difficult to provide that financial institutions respect adequate procedures against money laundering, especially in the cases in which they offer services in a country where the bank server is not located. For investigation, the matter of jurisdiction is related to the place where the transaction via Internet is done in order to know who is responsible in cases of Internet banking misuse for money laundering.[7]

7 In this context, the common report of French bank and French banking Commission propose the using of the logic that Internet serve as mean for accessing to account (the way similar to accessing to account by phone). Thus, is necessary to consider that transaction was done in computer with all information related to provider's financial services and management system. If the server of the service provider isn't on the same location as his management system with accounts, the management system must be considered as relevant location - Bank of France and Banking Commission, Internet: The Prudential Consequences, 5. 7. 2000, p. 17.

Сви наведени ризици захтевају планирање адекватних мера на превентивном и репресивном плану за супротстављање прању новца у овој области. У том смеру крећу се и напори међународне заједнице за хармонизовање стандарда за поступање са различитим облицима нелегалних активности у области Интернет банкарства (рад Групе за електронско банкарство Базелског комитета и рад Савета Европе на изради нацрта Конвенције о syber криминалу). Експерти Групе за финансијске акције предложили су скуп мера за супротстављање злоупотребама Интернет банкарства у сврхе прања новца[8]:

– спровођење тренутних захтева за идентификацију клијената да би се обезбедило да не дође до отварања „анонимних рачуна",
– доношење нових процедура које ће олакшати способност финансијских институција да заиста упознају своје клијенте током трајања пословних односа,
– сарадња између јурисдикција на једнообразним стандардима,
– развој капацитета нове информационе технологије која би омогућила откривање сумњивих on-line трансакција и потврђивање идентитета клијената,
– ограничавање броја и врста дозвољених on-line услуга или износа таквих трансакција,
– ограничавање on-line трансакција само на оне рачуне који су отворени на традиционални начин (то јест у директном личном контакту између клијента и финансијске институције),
– забрањивање финансијским институцијама које немају лиценцу у одређеним јурисдикцијама да у тој јурисдикцији нуде on-line своје услуге,

All mentioned risks require taking adequate measures for designing a preventive and repressive plan against money laundering in this area. All European Community efforts in standard harmonization for treating various illegal activities in the area of Internet banking are also moving in this direction (the work of Basel Committee's Group for electronic banking and the work of the European Committee on the Convention plan of cyber criminal). Experts of Group for financial actions proposed a set of measures against Internet banking misuse for money laundering:[8]

– Putting into effect the present requirements for client identification in order to prevent the opening of anonymous accounts,
– Making new procedures that will allow financial institutions to really get to know their clients during business contacts,
– Cooperation between jurisdictions in order to make uniform standards
– Development of new information technologies that allow discovering of suspicious on-line transactions, and client identity confirmation,
– Limiting the numbers and types of allowed on-line services or amounts of such transactions,
– Limiting on-line transactions only to those accounts that were opened in the traditional way (e. g. in a direct contact between the client and the financial institution),
– Forbidding financial institutions to offer their on-line services in some jurisdiction if they have not licenses for these jurisdictions,
– Finally, control can be done by jurisdiction where the Internet bank was opened and by jurisdiction where Internet bank has its clients, and
– The expert group also underlined that it is necessary for jurisdiction and investigation organs to develop skills for discovering and investigating possibilities for money laundering in Internet environment.

предлаже коришћење логике да Интернет служи као средство за приступање рачуну (на сличан начин приступања банковном рачуну преко телефона). Стога, треба сматрати да је трансакција обављена у рачунару у којем се налазе информације о финансијским услугама пружаоца и менаџмент систему. Ако сервер web-sajt-а пружаоца услуге није на истој локацији као и његов менаџмент систем где се држе рачуни, то друго треба сматрати релевантном локацијом – Bank of France and Banking Commission, Internet: The Prudential Consequences, 5. јули 2000, p. 17.

8 Financial Action Task Force, Report on Money Laundering Typologies for 1999-2000, Paris, p.4.

8 Financial Action Task Force, Report on Money Laundering Typologies for 1999-2000, Paris, p.4.

– коначно, надзор се може обављати и од стране јурисдикција у којима је отворена Интернет банка и од стране оних јурисдикција где Интернет банке имају своје клијенте и
– група експерата такође је истакла да постоји потреба да се у оквиру судских и истражних органа додатно развија стручност у откривању и истраживању потенцијала за прање новца у Интернет окружењу.

Пример 1: Злоупотребе Интернет банкарства у сврхе прања новца [9]

Колумбијски препродавац дроге који води већи број огранака у области Њујорка, има недељно приближно милион долара зараде, коју треба да опере. Он унајмљује стручњака за банкарство и компјутере, да опере тај прљав новац. Овај започиње циклус прања прљавог новца пласирањем у финансијски систем помоћу опробаног начина прања новца структурирањем новчаних трансакција.[10] Када се новац нађе у банкарском систему организује се подизање новца путем бакарских чекова који се могу уновчити. Ти банкаовни чекови се депонују код различитих Интернет банака. Када се новац нађе у виртуелном свету, исплате и трансфере у принципу је веома тешко пратити и открити, препродавац дроге има приступ лелалном електронском новцу.

Овако депонованом новцу препродавац дроге може приступити преко било којег рачунара било где у свету, користећи при томе услуге Итернет провајдера да електронским путем ступи у контакт са Интернет банком. Када оствари контакт са Интернет банком може да пребаци новац у неку другу банку или продавцу било којег производа који прихвата електронски начин плаћања.

Example 1: Internet banking misuse for money laundering[9]

Columbian drug dealer who manages a number of branches in New York City has the profit of around a million US dollars a week that must be laundered. For that purpose, he hires an expert for banking and computing. This expert begins the cycle of money laundering by planting the money in the financial system, applying the well known scheme for money laundering by structuring money transactions.[10] After the money is in the banking system, the expert organizes taking the money out by way of bank checks you can cash. All these bank checks are deposited at various Internet banks. Once the money is in the virtual world, it is very difficult to track and discover all payments and transfers, e.g. the drug dealer has access to legal electronic money.

Drug dialer can access this deposited money by any computer in the world, using Internet provider services for contacting Internet bank in the electronic way. After the contact with Internet bank is made, he can transfer his money to some other bank or to any seller of products who accepts payment in electronic way.

9 J. R. Richards, *Transnational criminal organizations, cybercrime, and money laundering: a handbook for law enforcement officers, auditors, and financial investigators*, CRC Press, Boca Raton, FL, 1999, p.79.

10 Bank Secrecy Act (Банкарски дискрециони закон САД из 1970), одељак 103.11, дефинише структурирање „... особа структурира трансакцију ако та особа, сама или у садејству са другим особама или у име других особа, спроводи или покуша да спроведе једну или више новчаних трансакција, у било ком износу, при једној или више финансијских институција, у једном или више дана, на било који начин, у покушају да заобиђе прописе о пријави порекла новца ...''

9 J. R. Richards, Transnational criminal organizations, cyber crime, and money laundering: a handbook for law enforcement officers, auditors, and financial investigators, CRC Press, Boca Raton, FL, 1999, p.79.

10 Bank Secrecy Act (Банкарски дискрециони Bank Secrecy Act of 1970 in Section 103.11 defines *structuring* as following: „ ... a person structures a transaction if that person, acting alone, or in conjunction with, or on behalf, of other person, conducts or attempt to conduct one or more transactions in currency, in any amount, at one or more financial institutions, on one or more days, in any manner, for the purpose of evading the reporting requirements ...„

ЗЛОУПОТРЕБЕ ЕЛЕКТРОНСКЕ ГОТОВИНЕ У СВРХЕ ПРАЊА НОВЦА

Електронска готовина омогућава плаћање роба и услуга преко Интернета. Суштина концепта електронске готовине огледа се у могућности дематеријализације трансакција преко виртуелног плаћања. Коришћење електронске готовине почиње куповином одређене вредности код овлашћеног продавца, која се потом чува у персоналном рачунару корисника. У случајевима када корисник купује робу или услуге преко Интернета, које се могу платити електронском готовином, одређена вредност електронске готовине се преноси на електронски готовински рачун продавца. Продавац потом наплаћује своја потраживања од овлашћеног продавца електронске готовине (најчешће банке). Основна предност електронске готовине у односу на остале видове плаћања јесте могућност микро плаћања. Наиме, микро плаћање малих номиналних износа код осталих видова плаћања није економично, код електронске готовине таква плаћања су најчешћа (читање on-line новина, тражење одређених информација путем Интернета и сл.). Потенцијални ризици злоупотребе електронске готовине у сврхе прања новца односе се пре свега на отежану могућност праћења трансакција електронском готовином након иницијалне куповине код овлашћеног продавца и коначног преношења средстава на рачун малопродавца. Такође, посао са електронском готовином може се користити као параван за операције прања новца у случајевима када перачи новца поседују предузеће чије се услуге могу плаћати електронском готовином. Ако се претходно реченом дода висок степен шифровања трансакција са електронском готовином, онда то упућује на погодности електронске готовине као оруђа за прање новца.

ELECTRONIC CASH MISUSE FOR MONEY LAUNDERING

Electronic cash allows goods and services payment via Internet. The concept of electronic cash is important for possibility of transaction dematerialization through virtual payment. The use of electronic cash begins with buying some value from a legal seller and after that, the electronic cash is kept in the user's personal computer. If the user is buying goods or services that can be paid for by electronic cash via Internet, part of the electronic cash value is transferred to seller's electronic cash account. After that, the seller collects his assets from a licensed seller of electronic cash (in most cases it is a bank). The main advantage of electronic cash concerning other ways of payment is the possibility of micro payment. Namely, micro payment of small nominal amounts is not economical with other ways of payment. In the case of electronic cash, this way of payments is the most frequent (reading newspapers on-line, looking for information via Internet, etc)

Potential risks of electronic cash misuse for money laundering are mostly related with the difficulty of electronic cash transaction tracking after initial shopping at a legal seller and final transferring of the means to the seller's account. Moreover, electronic cash business can be used as a screen for money-laundering operations in the cases of persons who own firms whose services can be paid for by electronic cash. In addition, we emphasize a high level of electronic cash transaction coding, and all elements point to the convenience of using electronic cash as a means for money laundering.

КОЦКАЊЕ ПРЕКО ИНТЕРНЕТА И ПРАЊЕ НОВЦА

Коцкање преко Интернета је веома погодно оруђе за прање новца, и то коришћењем овог начина пословања као паравана за прикривање операција прања новца. Наиме, сам ток комуникације на Интернету одвија се преко низа сервера који чине глобалну мрежу. Праћење комуникације веома је отежано због чињенице да већина корисника Интернета има привремене IP адресе, које је могуће прикрити или користити се туђим IP адресама. Трансакције којима се плаћају услуге виртуелних казина обављају се посредством кредитних картица.Ситуација се

INTERNET GAMBLING AND MONEY LAUNDERING

Internet gambling is a very common means for money laundering and it is usually used as a screen for hiding money-laundering operations.

Namely, several servers that make a global network realize the communication on Internet. Communication tracking is very difficult because most Internet users have temporary IP addresses. Paying transactions for virtual casinos services are done by credit cards. The situation becomes more complicated with the fact that the locations of most web sites that provide Internet gambling

усложава ако се томе дода да се локација већине web-sajt-ова који нуде услуге коцкања преко Интернета налази у офшор финансијским центрима. Њихова локација усложава истра-гу јер се не могу прикупити релевантне информације о трансакцијама које се налазе у серверу лоцираном у офшор финансијском центру.

Потенцијална решења тих проблема налазе се у успостављању система мера за супротстављање прању новца у тој области. Те мере би требало да захтевају лиценце за овакав вид пословања и транспарентност евиденција о трансакцијама. По питању праћења тока комуникације на Интернету експерти Групе за финансијске акције предложили су следеће мере[11]:

– захтевати од провајдера Интернет услуга да воде поуздане регистре корисника заједно са одговарајућим информацијама о идентификацији,
– захтевати од провајдера Интернет услуга да воде „улазне"фајлове са подацима о саобраћају којима би се повезивао број Интернет протокола са корисником и са телефонским бројем коришћеним за успостављање везе,
– захтевати да се ове информације чувају одређени период (од шест месеци до једне године) и
- обезбедити да те информације буду правовремено расположиве на међународном нивоу, када се воде истраге.

Пример 2: Злоупотреба коцкања преко Интернета у сврхе прања новца[12]

Заједничка истрага кривичне и фискалне полиције државе Ц била је усмерена ка спортској кладионици која је пружала услуге коцкања на Интернету. Ова кладионица такође је функционисала и као провајдер Интернет услуга. Кладионица је прикупљала, сређивала и анализирала статистичке и друге информације везане за спортске догађаје и потом продавала те информације корисницима који су их узимали у обзир приликом својих одлука о клађењу. Ова кладионица/Интернет провајдер проширила је своје услуге и нудила две офшор операције коцкања смештене у карипском региону а улози за обе примане су преко Интернета или телефоном. Агенти су успешно успели да се инфилтрирају у ову операцију.

are in offshore financial centers. Their location complicates investigation, as you cannot collect relevant information about the transactions that are in a server located in offshore financial centers.

Potential solution for these problems is establishing the system of measures against money laundering in this area. Those measures would include licenses for this type of business and transparency of transaction evidence. Experts of the Group for Financial Actions proposed the following measures for Internet communication tracking:[11]

- It is necessary for Internet service providers to keep reliable registers of users, including appropriate identification information,
- It is necessary for Internet service providers to keep "enter" files that include traffic data that would be used for relating the Internet protocol number with the user and the phone number used for connection,
- It is necessary to keep these information for a period of time (between six months and one year) and,
- Provide that all information is available internationally for conducting investigation.

Example 2: Internet gambling misuse for money laundering[12]

A joint investigation of criminal and fiscal police in the country named C was oriented toward a sport-betting place that provided Internet gambling services. This betting place functioned also as an Internet services provider. Statistical and other types of information relating to sport events were collected, arranged and analyzed and after that sold to users who used that information during betting. This betting place/Internet provider expanded its services and began to offer two offshore operations that were located in Caribbean region, where stakes were accepted by Internet or by phone. Agents successfully infiltrated this operation.

In order to launder their illegal activities of Internet gambling earnings, they hired a lawyer. He established a pattern where betting place/Internet provider rented its services to these subjects for some sum. Earnings were also laundered by banking accounts in the Caribbean region and they were eventually returned to bank institutions of the country C. Investigation organs estimated that around 170 millions dollars had passed through

11 Financial Action Task Force, Report on Money Laundering Typologies for 2000-2001, Paris, p.8.

12 Ibidem, p.7.

11 Financial Action Task Force, Report on Money Laundering Typologies for 1999-2000, Paris, p.4..

12 Ibidem, p.7.

Да би опрали приходе од својих нелегалних активности коцкања преко Интернета субјекти ове истраге користили су услуге адвоката. Он им је смислио разрађену схему у којој би кладионица/провајдер изнајмљивала своје услуге овим субјектима за назначену суму. Приходи су такође прани преко низа банковних рачуна у карипском региону и евентуално враћани у банкарске институције у држави Ц. Истражни органи процењују да је кроз ову кладионицу/провајдера годишње пролазило око сто седамдесет милиона USD опклада.

Предвиђа се да ће субјекти у овој истрази бити оптужени за коцкање, прање новца, пореску евазију и друга кривична дела везана за организовани криминал.

ЗАКЉУЧАК

Коришћење нових технологија у финансијском пословању, посебно Интернета не познаје границе, и ту је међународна сарадња од есенцијалног значаја за супротстављање прању новца. Напори међународне заједнице за супротстављање прању новца и покушају стварања правних оквира за супротстављање прању новца још више се компликују злоупотребом нових технолошких достигнућа у сврхе прања новца, јер системи виртуелног плаћања делују глобално а традиционалне физичке границе држава се „поништавају" уз помоћ рачунара. Посебно је значајна међународна сарадња на оперативном нивоу између различитих државних агенција које се баве проблематиком супротстављања прању новца, јер је потребно разменити информације и предузети адекватне мере у истрази прања новца пре него се изгубе релевантне информације које се налазе у електронском облику и подложне су променама.

У истрази случајева прања новца постоје тешкоће које се огледају прво, у немогућност примене метода попут праћења и анализе документације јер криминалац применом нових технологија у пословању нема потребе за физичким контактом са одређеном финансијском институцијом, већ све пословне активности обавља виртуелним путем. У таквим случајевима примена мера у супротстављању прања новца као што је програм упознај своју странку има ограничено дејство.[13] Друго, критична тачка је сигурност рачунара, што

13 Види Г. Бошковић, *Начини прања новца и методи супротстављања*, магистарска теза, Полицијска академија, Београд, 2003, p.97.

this betting place / Internet services provider per year. There are some assessments indicating that these subjects of investigations will be convicted for gambling, money laundering, tax evasion and some other organized crime criminal acts.

CONCLUSION

Using new technologies, particularly the Internet, in financial business knows no boundaries. Therefore, the importance of international cooperation in suppressing money laundering is essential. The efforts of European Community to establish jurisdiction frame against money laundering are becoming more and more complicated since there are new technological accomplishments for money laundering, every day. The main reason for this is the fact that virtual payment systems work globally and boundaries "disappear" with computers. The international cooperation on the operational level between various government agencies that deal with money laundering is very important. It is necessary to exchange information and take measures in money-laundering investigation before electronic information relevant to the investigation that are subject to changes are lost.

Firstly, there are many difficulties in investigating the cases of money laundering. It is impossible to use methods of tracking and analyzing documentation because with new business technologies there is no need for criminals to physically contact any financial institution as they all do their business activities in virtual way. In such cases, the use of measures against money laundering, such is program *Meet your client,* is limited.[12]

Secondly, a critical point is computer safety and it includes computer system ability to execute coding of outgoing and decoding of incoming data. Today, preventing or discovering illegal transaction by authorized organs is impossible without accessing and using more and more complicated software for coding and decoding. The reasons for this way of business being interesting for "money launders" are high quality and technology necessary for safe and accessible managing the business technological systems.

The previously quoted facts are very important for making strategic decisions and changes relating to concepts against money laundering. Namely,

13 G. Boskovic, *The ways of money laundering,* M. A. dissertation, Police Academy, Belgrade, 2003, p.97.

подразумева способност рачунарског система да изврши кодирање одлазећих и декодирање долазећих података. Без могућности приступа и коришћења све сложенијег софтвера за кодирање и декодирање, надлежни органи би били онемогућени да спрече или уђу у траг нелегалним трансакцијама.

Управо квалитет и технологија која је потребна да би нови технолошки системи били сигурни и доступни за вођење посла, разлози су што је овакав начин пословања посебно интересантан за „перач новца".

Претходно наведене чињенице имају изузетан значај за стратешка опредељења и потребне измене у концепту супротстављања прању новца. Наиме, постоји потреба за усавршавањем постојећих и увођењем нових криминалистичких метода у супротстављању прању новца. То подразумева стално праћење нових технолошких и научних достигнућа и њихово инкорпорирање у постојеће методе. Све то мора бити праћено стручним усавршавањем, специјализацијом и адекватним прилагођавањем постојеће организације полиције и других надлежних органа, која може да одговори изазовима супротстављања прању новца у савременом окружењу.

there is a need for improving the existing methods and introducing new methods against money laundering. It includes the constant learning about new technological and scientific accomplishments and their incorporating in the existing methods. All that must be followed by professional training, specialization, and adequate transformation of the existing police and other state organ organization, in order to deal effectively with the challenges of money laundering in the modern society.

ЛИТЕРАТУРА / REFERENCES

Bortner, R. M.: (1996) *Cyberlaundering: Anonymous Digital Cash and Money Laundering.* University of Miami School of Law.

Бошковић, М.: (2001) *Актуелни проблеми сузбијања прања новца*, Безбедност, број 5, Београд.

Бошковић, Г.: (2003) *Начини прања новца и методи супротстављања, магистарска теза*, Полицијска академија, Београд.

Candler, L. J.: (1998) *„Commingled Funds: How to Seize Proceeds of Electronic Crime."* Journal of Money Laundering Control, Vol.1, No.4.

Clark, F. and K. Diliberto: (1996) *Investigating Computer Crime.* Boca Raton, CRC Press.

Financial Action Task Force Annual Reports, 1995-1996, 1996-1997, 1997-1998, 1998-1999, 1999-2000, 2000-2001

Financial Action Task Force: The Forty Recommendations of Financial Action Task Force on Maney Laundering, Paris, 1990.

Philippsohn, S. (2001) *The dangers of new technology-laundering on the Internet*, Journal of Money Laundering Control, London, volume 5, pp. 87-95.

Richards, J. R.: (1999) *Transnational criminal organizations, cybercrime, and money laundering: a handbook for law enforcement officers, auditors, and financial investigators.* CRC Press, Boca Raton, FL.

Myers J Larry, Myers B Laura: (2003) *Identifying the required knowledge elements for the effective detection, investigation, and prosecution of high technology crime*, Journal of Criminal Justice Education, Vol. 14, Iss. 2, p. 245.