



# Cyber Laundering: An Analysis of Typology and Techniques

Wojciech Filipkowski<sup>1</sup>

University of Białystok, Poland

## Abstract

*The Internet is a great tool for exchanging information. However there are people who want to take advantage of it in order to commit crimes. The main goal of this paper is to answer following question: How the Internet could be and is abused by “launders” – criminals who want to legitimize their illicit profits? And the whole phenomenon is called cyber laundering. The main goal of this paper is to present a typology of criminal activities – both potential as well as actual – which can be described as cyber laundering. It consists of four parts. The first and the second one briefly present the characteristics of the Internet and the financial services available on-line, correspondingly. The third part is a presentation of different techniques applied by criminals to launder money via the Internet. It bases on the information available from articles, papers, government reports and other sources. The last part presents some examples and symptoms of cyber laundering.*

Key Words: money laundering; Internet; cyber laundering; typology; techniques

## Introduction

The abuse of the Internet by money launderers is potentially a significant threat (Solicitor General Canada, 1998; Veng Mei Leong, 2007). Why we cannot say “it is a significant threat”? To date, there are only few criminal cases concerning so called cyberlaundering. But there are some symptoms observed by international organizations, law enforcement agencies, financial intelligence units and financial institutions. How we can explain that fact? Maybe it is not such a “great tool” after all as many people think or criminals does not trust new technologies or we are looking in the wrong direction? However criminals have been constantly seeking new ways to clean their illicit gains in order to stay ahead of law enforcement. Similar situation was in case of wire transfers in the 80's and 90's.

<sup>1</sup> Lecturer and Researcher, The Faculty of Law, University of Białystok, Poland Email: fwojtek@uwb.edu.pl

### **Characteristics of Internet – What attracts launderers?**

There are few features of the Internet which attract criminals (including launderers) (Skalski, 2004; GIFI, 2008).

#### *Anonymity*

The Internet seems to be a “place” where you can hide yourself among millions of other users; where you can pretend to be someone else since no one can truly identify you. But it seems that is no longer true, since there are some legal obligations put on Internet Service Providers to record and keep log files for a long period of time. They show which computer and when was connected to Internet. This measure is being used to fight computer crimes. It makes law enforcement’s work to trace somebody’s activity in cyberspace easier. Of course there are some means to circumvent them and to keep the anonymity. They include Internet Protocol (IP) spoofing, use of modem connections (every time user connects he gets different IP address), Wireless Fidelity technology which allows to abuse publicly open so called “hot spots” or unprotected routers to connect to the Internet (Ashwell, 2008), use of pre-paid phones as modem in order to connect to the Internet (it hides the identity of a user). Also the use of encryption technology (widely available on the Internet) and many proxy servers hinders the efforts of law enforcement to catch cybercriminals.

#### *No Face-To-Face contacts*

This is called the depersonalization of financial operations. When we are using one of the financial services available on the Internet, we actually use our computer (and software) which connects to the bank’s server. The whole process of placing orders (making requests) and executing them is fully (or partially) automatic without the presence of a human factor. So in fact we can very easily pretend to be some one else each time we “visit” bank in the cyberspace. The financial institution’s server checks only two things the login (e.g. unique ID number) and the password – not the true identity of a customer. If the information is correct (meaning the same as the one stored in server’s memory), the access is granted. As a result, it would be harder to detect and hold up transactions related to money laundering activities. It also cuts out another potential source of reporting suspicious transactions – financial institution employees (Cyber Laundering, 2002).

#### *Speed of the transactions*

Money laundering process would be less expensive and faster as the one using ‘normal’ or old-fashion transactions. New payment technologies permit to move funds more rapidly on long distances and make law enforcement work even more complicated (Williams, 1998). Some of them are instantaneous e.g. within one financial institution. It allows launderers to move funds very quickly within one country or even world wide. In essence it makes hiding the illicit source of money easier and difficult to trace. It makes also the whole procedure cheaper (Cyber Laundering, 2002).

#### *Globalization process: free movement of goods, services, people and new payment technologies*

The globalization of economy includes the necessity for people (entrepreneurs and customers) to move, invest and spend money wherever they want to. In order to achieve that with the help of developing information technology, there have emerged new payment technologies. They allow freeing ourselves from carrying large quantities of cash,

as well as to do businesses at a long distance. Another word is “investments' mobility”. Access to the Internet and to on-line services is easy and common. This channel of the distribution of financial or investment products has become very important factor. These services will become even more significant for financial institutions in the near future. There is also a trend to reduce any obstacles (including legal ones) in trade between countries or moving funds around the world to find more efficient way of investing them.

*Cross border activity: involves several jurisdictions, mutual legal assistance treaties issues*

The on-line service provider's abode usually differs from the place where the servers are located in reality, from where these servers are administrated, or from where the client accesses the Internet (“Cyber Laundering”, 2002)<sup>2</sup>. The new payment technologies let us conducting business between different countries, various legal systems (Chepesiuk, 2000). It means there are several jurisdictions involved in the case of an offence. And the cooperation between law enforcement, revenue services and judiciary is one of the most difficult tasks as far as the transnational criminality is concerned. Even though there are plenty of mutual legal assistance treaties and international conventions. So in fact it is easier to get away from the government agencies with money derived from illicit activities.

What is worth to write is that we cannot stop the development of new payment technologies in order to fight crime (including money laundering), since some of these features are important for lawful commercial activities, too. They encompass speed of transactions, access to customers or counterparts and capacity to extend beyond national border (Cyber Laundering, 2002). As a result we need to find another way to prevent and fight money laundering in the cyberspace. It has to be stressed that the launderers and other criminals sponge on the development of new payment technologies. On the other hand they also stimulate that development by exploiting it. In other words we need to learn the causes and the phenomenology of cyberlaundering in order to fight it efficiently or just to control it.

### **Financial services available through the Internet**

First of all, there is no unanimity on the meaning of the term cyber payments. In general they can be described as payments which facilitate the transfer of financial value in the Internet (Molander, Mussington, & Wilson, 1997). And this is a wide approach. Some call it digital currency or e-cash, but those terms cover only a part of the phenomenon. That technology has a strong impact on the way we do business, transfer money (and other values) and the cash-oriented society. The common element is that these systems provide counterparts with immediate, convenient, secure and sometimes anonymous means by which they can transfer financial value (Molander et. al, 1997). Although these systems will provide promptly evident benefits to legitimate commerce, it may also have the potential to facilitate the international movement of illicit funds. At the same time it prevents law enforcement from obtaining necessary information to detect illegal activity.

---

<sup>2</sup> Many reasons for reporting a transaction as suspicious is to do with the geographical origin of the funds. If the origin of the transaction can be kept anonymous, one of the indicators of potential money laundering could be removed.

There are also different typologies of what is being encompassed by term cyber payments (Corrigan, 1999). It may include:

- Internet payment services (e.g. mobile payments, micro-payments or digital precious metals).
- Stored value cards – smart cards.
- On-line banking.

#### *Internet Payment Systems*

Companies provide so called electronic cash or e-cash services to their customers. It is a sort of replacement for physical cash. Usually, software which stores value on the computers of their clients (merchants and consumers) is provided to them. This stored value can than be transmitted *via* the Internet between personal computers in order to buy and sell goods or services.

#### *Stored Value Cards*

Also known as “smart cards” or e-purse; those cards are pieces of plastic, typically the size of a credit card. They contain a microchip (a memory chip) to which value can be encoded. These cards can be loaded (or added value) *via* automatic teller machine, properly equipped telephones, personal computers and from other stored value cards using a device which can transfer value directly. But the range of possibilities depends on the system. Theoretically they can be programmed to store billions of dollars. However, most current stored value card programs place a limit on the amount of value that can be loaded onto any individual card (FATF, 2006).

Smart cards may make it easier for the launderer to transfer illicit funds without detection by law enforcement and financial institutions (Molander et. al, 1997). Because the cash value is stored on the card, there is no need for the merchant to dial up a bank or credit card company to get approval for the transaction. What is more interesting and useful for launderers, funds can be moved from one country to another without alarming financial institution. A card issued in one country can be used to withdraw money in another one. And users may hold numerous cards. They can allow criminals to move billions of dollars without using banks at all. Digicash was developing a computer-based payment system that involved so called “one way privacy” method. It means that payers can check who received money from them, but does not allow the recipients to find out where it came from (Chepesiuk, 2000).

#### *On Line Banking*

Many financial institutions provide their customers with software to conduct most, if not all, of their banking business *via* personal computer.<sup>3</sup> This software allows customers to check account balances, transfer funds between accounts and direct payments to creditors. But these days you don't need special software. A typical web browser (most popular MS Internet Explorer or Mozilla family) is enough since it uses encrypted connection protocols (e.g. SSL, TLS). You can access also virtual casinos, universities, libraries, bookstores, auction houses, etc (Corrigan, 1999; FATF, 2006).

---

<sup>3</sup> Any financial institution that offer on-line banking should have procedures, whether it be driven by software, humans or a mix of the two, that verify the identity of the customer who seek to do business with the institution. This can be difficult for on-line banks that often rely on customers to confirm who they are through passwords (“Cyberlaundering threats”, 2001).

### **How on-line financial services can be abused?**

Although it is difficult to provide an all encompassing definition of a cyber payment, it is possible to make some generalizations (Corrigan, 1999). It means all of the systems which intend to allow their users to move funds electronically (in the Internet). They may serve as a cause (a legal title) to perform transaction (transfer of funds) or tool to perform transaction (transfer of funds) (Filipkowski, 2004). The latter needs a few words of explanation. Banks allow their account holders to send funds from one account to another one. However it is possible to establish a bank account with false ID or hire someone to do it for us for a commission. Therefore one person can have an access to different bank accounts and enter them as a different person simultaneously via the Internet. If the accounts are located in one bank there is one more vital advantage. There transfer is almost instantaneous which allows for fast moving funds and multiple withdrawing them in cash at the end using ATM (e.g. abroad).

New payment technologies depend on applications of high-speed communication and information analysis that is part and parcel of the use of computer based information processing. The system bases on fast ways of communications and computing data using networks (Corrigan, 1999). Cyber laundering was believed to be the latest (and most advanced) technique in money laundering typology (Levi & Reuter, 2006). So far, the process has been depending on a physical transportation of cash to conceal the existence of illegal source or blending licit company's incomes with illicit ones. As the physical moment of cash has become more risky and the electronic means of communication (wire transfer) have emerged, the launderers have changed their modus operandi. The wire transfer system have been allowing organized crime, as well as legitimate businesses and individual banking customers to enjoy a swift passage for moving money between jurisdictions.

Although there are no or just few criminal cases connected purely with Internet (it depends on jurisdiction), it does not mean that there is no cyber laundering activity going on and all of this is just a hype provided by law enforcement agencies in order to get more power (e.g. Jasiski, 2001; FATF, 2001; Wójcik, 2002; FTAF, 2006). Maybe we look not thoroughly enough or our instruments aren't good enough to detect this phenomenon? However, using Internet based financial services is possible on all stages of money laundering process (Bumeter, 2001).

#### *The Placement Stage*

The first step in money laundering is the physical disposal of cash (Solicitor General Canada, 1998). Traditionally, placement might be accomplished by:

- depositing the proceeds derived from criminal activity in domestic banks or other types of financial institutions,
- smuggling the cash across borders and depositing in foreign accounts,
- buying high-value goods, such as artwork, airplanes, or precious metals and gems; it can then be resold with payment by cheque or bank transfer.

With cyber laundering, cash might be:

- deposited through an unregulated financial institution (a sort of financial

- intermediary<sup>4</sup>) which issues smart cards, or
- deposited by Smurfs<sup>5</sup> using ATM with deposit feature.

However in case of cybercrimes, there is no need to go through this stage, since the money (or other values) already has an electronic form and “exists” in cyberspace. Internet frauds, identity thefts, false investments opportunities may serve as examples.

#### *The Layering Stage*

The second stage of money laundering process benefits the most from the on-line services. The layering involves creating complex layers of financial transactions to distance the ill-gotten gains from their source and break the audit trail (Solicitor General Canada, 1998). There are plenty of traditional techniques, such as the wire transfer (e.g. SWIFT), the conversion of deposited cash into other financial instruments or goods, and investment in legitimate businesses, using shell companies (e.g. registered in off-shore financial centers).

The most important issues for launderers are: the speed, the distance and the anonymity. All of them can be provided by on-line financial services (Cyber Laundering, 2002). It includes:

- opening many Internet accounts (it is hard to verify client's true identity), it is not necessary to have steady incomes (which is important while using students or unemployed as Smurfs), You can open an account in a foreign bank (if law allows that).
- collecting bank accounts and controlling them through personal computer; it is being done by building up an extensive audit trail in a short space of time with instantaneous transactions – including several jurisdictions which makes difficult for law enforcement to follow the audit trail.

#### *The Integration Stage*

The last stage has an aim to make the wealth derived from criminal activities appear legitimate (Solicitor General Canada, 1998). There are also many traditional techniques such as: using front companies, “lending” money back to the owner (using funds deposited in foreign financial institutions as security for domestic loans), transfer pricing, false invoicing, winning ticket, etc.

The most effective way is probably to establish an on-line service company. Offering services (true or fake) provide incomes which appear legitimate (Cyber Laundering, 2002). Funds end up on safe corporate account after the second stage somewhere in off-shore jurisdiction. It could deal with gambling, betting, etc.. However the service would never be delivered – there would be no (net) winnings paid back to the account. The payment would appear as profit in the books of the Internet service company. Thus the wealth of

---

<sup>4</sup> The Bank for International Settlements (BIS) notes: “With technology facilitating the breakdown of traditional banking services into multiple components and the addition of analytical tools and other capabilities into traditional banking services, more unlicensed non-bank entities are likely to provide bank-like services via the Internet, including those that are extended cross-border. Differences in definitions as to what constitute a ‘bank’ among jurisdictions would likely be magnified and will increasingly challenge how bank supervisors deal with financial entities with no home supervision” (Basel Committee on Banking Supervision, 2000).

<sup>5</sup> This is the name for a group of people who help launderer deposit dirty cash on bank accounts. They do it for a commission.

the owner would appear to be legitimate – a profit of her/his own Internet Company (FATF, 2001). Payment for services may come from different parts of the world; there are no geographical restrictions. Since there are just a few criminal cases we could describe as cyber laundering, presented below specific techniques can be describe as potential money laundering *modus operandi* (see also e.g. FATF, 2001; FATF, 2006).<sup>6</sup>

#### *On-Line Services*

On-line banks are a prime target for money launderers (Cyber Laundering, 2002). Banks in general provide the widest range of financial services. This is the reason why they are always targeted by launderers. What is more important, the regulations concerning opening an Internet bank account are different from one jurisdictions to another. It leads to asymmetric regulations between jurisdictions. The less information is required, the better for the launderer because it conceals her/his identity from law enforcement.

One can come up with simple *modus operandi*:

1. opening an Internet account and making deposits from other account or using ATM using ill-gotten gains; not one account is being create but few tens;
2. members or supporters of a criminal group establish company providing Internet-based services (e.g. in off-shore jurisdiction or just other country);
3. accessing on-line service using personal computer – in order to do that customer has to buy a limited in time access e.g. monthly/6-months/annual subscription; service provider gives him/her a bank account number;
4. he/she makes a direct payment using his/her Internet bank account – stating that this is payment for internet-based services;
5. bank transfer funds to another bank account; and this is a legitimate company's income.

The service might be a fake (meaning it does not take place). On the other hand, if service is being provided also for “normal” customers, it gives the opportunity to use the blending technique (which means mixing licit and illicit incomes) which makes things even more difficult for law enforcement or financial institution to mark transactions as suspicious.

Additionally launderer can abuse financial intermediary such as PayPal (e.g. FATF, 2006; “PayPal”, 2003). It acts as non-bank, Internet-based agent – payments intermediary for individuals and organizations that want to trade or transfer funds *via* the Internet. A person sets up a pre-paid account in his name with this agent. It can be funded from a credit or debit card or a bank account. Using those pre-paid funds, person can buy goods or transfer funds to other agent's account holders. The payment or transfer of funds occurs as a book-entry transaction between the agent's accounts. When an account holder wishes to access the funds located in his account, he order agent to credit his credit or debit card or bank account *via* a credit transfer or a paper check (GAO, 2002).

#### *Credit cards*

There is a very similar situation with the use of credit cards (charge type) or e-cards. They are widely use by customers who wish to pay for services available on the Internet. None of other companies involved in the process (meaning the credit card company, the

---

<sup>6</sup> Those descriptions base on information which has derived from articles, books, reports, news, Author's personal contacts as well as knowledge regarding money laundering phenomenon and financial market.

Internet service provider, and even the bank) would think that there was anything suspicious about the transactions.

#### *Pre-paid cards*

It seems – according to FATF report – that the most popular method of cyber laundering is the use of pre-paid cards.<sup>7</sup> There are two types of cards: open and close system. First one is a typical debit card with which everyone can pay for services, goods or withdraw money from ATM. Second concerns systems like pre-paid telephone cards which can be bought and then resold. They can be exploiting in all three stages of money laundering (NDIC, 2006). The pre-paid cards are especially good to transfer funds across borders.

#### *On-line Gambling*

Internet gambling has been identified – by experts in the field of money laundering and tax evasion – as a potentially ideal web-based service to legitimize ill-gotten gains (Cyber Laundering, 2002). In the real world casinos are used to launder dirty money. The same thing can be done by on-line gambling sites. There are two possibilities: launderer exploits legitimate web-based service or launderer sets up an on-line gambling company in order to clean money (Bumeter, 2001).

It is an excellent method because transactions are conducted primarily through credit cards as mentioned earlier (Cyberlaundering threats, 2001). Additional obstacle is the place where on-line gambling companies operate. Usually, they are based in off-shore financial centers which lack regulatory or prudential measures. This method can affect a normal bank since such companies have their accounts in offshore banks that, in turn, use a reputable United States correspondent bank. The tracing of the source and ownership of the illegal money that moves through these accounts is difficult or impossible for enforcement and regulatory agencies in the United States and elsewhere (e.g. FATF, 2001; Malcolm, 2003; Wollert, 2004).

#### *On-line Auctions*

Another business that can be useful for launderers is the auction sale. It is a booming industry in the Internet. It allows its registered users to put items on a sale or to buy such items. There are auction sites which offer some basic financial services, too. They do it for security reasons for persons buying and selling things. The buyer sends money to company's bank account and the seller sends the item to the buyer. If everything is “all right” and the item is exactly as it was promised by the seller, the company sends money to him/her. It also gives the whole process the appearance of licit business activities since it involves reputable auction company and its bank account. Since this is auction price has no limits and the Smurf can bid higher and higher. Actually the higher the price is, the more dirty money receive legitimate appearance.

---

<sup>7</sup> In 2001, a suspicious activity report (SAR) filed in the United States detailed the acquisition of more than 300 prepaid cards by a single individual who used them to transfer almost \$2 million to Columbia. Other countries where money is being withdrawn include Venezuela, Mexico, Argentina and Brazil. Such method can be observed also in Europe (FATF, 2006).



### *Mobile-payments*

Mobile payments can be described as payments done through the use of services *via* mobile phone or any other communication device (FATF, 2001). Payments are initiated using voice access, text messaging protocols, or wireless application protocols (WAP) that allow the device to access the Internet.

However new mobile payments services are not based on an underlying bank or credit card account. The telecommunication operator acts as a financial intermediary to authorize, clear, and settle the payment between its client and the mobile service provider. The GSM (or UMTS) operator engaged in these activities usually are not overseen by a country's central bank or other banking regulators but may be subject to anti-money laundering measures.

There are two possibilities. The operator may either:

1. allow customer to charge transactions to the phone bill (post-paid) or
2. may permit the phone owner to fund an account held by the telecom operator (or other service provider) for the purposes of making payments (pre-paid).

Pre-paid phone gives also a sense of anonymity since usually it is not required to register the identity of a SIMM card buyer. Prepaid mobile payments accounts operate in the same manner as a prepaid card or an electronic purse (FATF, 2001).

### *Digital Precious Metals (DPM)*

The ground for using Digital Precious Metals services is to facilitate on-line transactions without regard for underlying currencies or access to foreign exchange (FATF, 2006). Those transactions have immediate finality since they are conducted as a book-entry transaction between the dealer's accounts. It involves the exchange of options or the right to purchase an amount of precious metals at a specific price. These derivatives can be exchanged, like any other traditional commodity or securities derivatives, between account holders. Consumers purchase a quantity of virtual precious metal holdings based on the current price of the metal on the world commodity exchanges. Once a purchaser has acquired a quantity of the virtual precious metal, those holdings or a portion of them can be transferred either to another individual or a merchant in exchange for goods and services.<sup>8</sup>

The dealer's internal regulations usually differentiate between themselves. There might be some restrictions or limits on value of DPM, method of funding or usage of account (FATF, 2006). Sometimes they allow anonymous accounts. The access to account only *via* the Internet hinders dealer's efforts to verify customers' true identity. It shifts the money laundering risk to a new level.

---

<sup>8</sup> In March 2004, an Oklahoma man admitted to a financial fraud scheme involving an on-line investment fund. Thousands of people lost almost \$9 million U.S. dollars. According to the FBI, the on-line investment scheme, E-Biz Ventures, laundered investor money through e-gold Ltd. The Oklahoma man who created this criminal enterprise may have been targeting tax evaders and other criminals because he 'allegedly highlighted his reliance on e-gold to appeal to his victims' fear of the federal government and their desire for anonymity' (Grow, 2006).

### *Virtual Money Laundering*

There is a relatively new method of laundering money and is called virtual money laundering (Rijck, 2007). Criminals can make use of the growing in popularity of the massive multiplayer on-line role playing games (MMORPG) or web based social services, e.g. Second Life, Entropia Universe. What is so interesting in it as far as money laundering is concerned? Some of them allow purchasing virtual currency using “old-fashion” real money at a fixed exchange rate. Then the player (user) can earn more in virtual world, exchange it with other users, buy and sell virtual items. It works in both directions – the virtual coins can be converted into real money and transferred to desired account before withdrawing it from ATMs worldwide. Sometimes players are given a re-loadable debit card with which they can withdraw money directly from ATM.

### **Examples of Cyber laundering**

#### *Financial Action Task Force's cases*

One of the Financial Action Task Force on Money Laundering special reports was devoted to new payment methods (FATF, 2006). It has based on a survey conducted in member countries around world. Apart from description of several methods of paying (which were used also in this paper), there were few actual cases shown in order to illustrate the problem. As it can be seen above, some methods can still be described as a potential treat to financial institutions. That group encompasses electronic purse, mobile payments, and Internet payment systems. It is connected with the fact that they are not as popular as the others. On the other hand, FATF presented few examples of the other methods used by criminals.

The report shows that there were only 3 cases connected with pre-paid cards (open system) and 2 cases – pre-paid cards (close system). According to that research there were also 3 cases connected to digital precious metal services. At the same time no cases involving electronic purse, mobile payments, nor Internet payment systems were reported by member countries. The question is how close to the reality those results are?

The research done by FATF has stressed three main risk factors:

- the Internet is used as a distribution channel for financial instruments, cards, etc.;
- there is no face-to-face contact with the customer who buys such an instrument, card, etc. and
- the payment method is an open network type and it can be accessed in a high number of jurisdictions (FATF, 2006).

Those factors pose hazard especially when accompanied by the fact that payment operator is located abroad in a country or territory which do not have enough regulations as far as fighting money laundering is concerned.

### **Conclusion**

The exploitation of the Internet for the purpose of money laundering was the subjects of analysis made by Financial Action Task Force on Money Laundering (FATF, 2000).<sup>9</sup> Also there are some theoretical works regarding cyber laundering (Molander, et. al, 1997;

---

<sup>9</sup> There was cited a case from the Denmark. The authorities gave an example in which an Internet website in another country was used to offer money laundering services. Some other jurisdiction gave examples of web sites have been being used in fraudulent activities. That was in 1999. In the next report there were three examples provided by the member states how the Internet gambling had been used to launder money (FATF, 2001).

Prengel, 2003). It is a matter of time when the criminals (or their professional advisers) will start to use this incredible tool in their schemes more often (Morris-Cotterill, 2001). However it depends on several socio-economic factors, among others the availability of on-line financial services, the telecommunication infrastructure and the society approach to the new payment technologies. The number of non-cash transactions is among other a very vital feature. And it has been growing rapidly (FRS, 2007). Up until then it has to be treated as “potential” threat for the anti-money laundering regimes (Skalski, 2004) and the situation has to be monitored (Joyce, 2001).

## References

- Ashwell, R. (2008). The wireless gateways to cybercrime. [Electronic version] The Guardian May 22, 2008. Retrieved July 4, 2008 from The Guardian Web site: <http://www.guardian.co.uk/technology/2008/may/22/wifi.internet>
- Basel Committee on Banking Supervision (2000, July). Management and Supervision of Cross-Border Electronic Banking Activities. Retrieved May 29, 2008 from the Bank For International Settlements Web site: <http://www.bis.org/publ/bcbs99.pdf>
- Bumeter, B. H. (2001, June 1). Cyberlaundering: Low Tech meets High Tech. Retrieved May 29, 2008, from the Maven Mapper's Information Web site: <http://www.softduit.com/mavenmappersinformation/2001/06/01/cyberlaundering-low-tech-meets-high-tech/>
- Chepesiuk, R. (2000). Cyberlaundering – The Internet's Ultimate Scam. Retrieved September 2, 2003 from the Moneywise International.com Web site: <http://www.moneywise-int.com/ezine/Cyberlaundering.html>
- Corrigan, S. D. (1999, June 11). Remedies. International experiences. Prospects for regulation and action to combat on-line money laundering. Retrieved September 2, 2003 from the TRANSCRIME, Research Centre on Transnational Crime, University of Trento (Italy) Web site: <http://www.transcrime.unitn.it>
- Cyber Laundering: The Risks to On-line Banking and E-Commerce Companies. Retrieved May 29, 2008 from Stop money laundering! International conference (London, February, 2002) Web site: <http://www.antimoneylaundering.ukf.net/papers/solicitor.htm>
- Cyberlaundering threats should put all bankers on alert, FATF warns (2001, April). Retrieved September 2, 2003 from the Anti-Money Laundering.Com on-line Data Base.
- Federal Reserve System (FRS, 2007). [Electronic version] The 2007 Federal Reserve Payments Study. Noncash Payment Trends in the United States: 2003 – 2006.
- Filipkowski, W. (2004). Przypadki prania pieni dzy w Polsce i na wiecie – diagnoza, metody i tendencje rozwojowe (The cases of money laundering in Poland and elsewhere – diagnosis, techniques and trends). In S. Lelental & D. Potakowski (Eds.), *Pozbawianie sprawców korzy ci uzyskanych w wyniku przest pstwa (The forfeiture of proceeds derived from crimes)* (pp. 87-102). Szczytno: Wydawnictwo Wy szej Szkoły Policji.
- Financial Action Task Force on Money Laundering (FATF, 2000). [Electronic version] Report on Money Laundering Typologies 1999-2000. Paris.
- Financial Action Task Force on Money Laundering (FATF, 2001). [Electronic version] Report on Money Laundering Typologies 2000-2001. Paris.

- Financial Action Task Force on Money Laundering (FATF, 2006). [Electronic version] Report on New Payment Methods. Paris.
- General Inspector for Financial Information (GIFI, 2008). [Electronic version] Informacja Generalnego Inspektora Informacji Finansowej o realizacji ustawy z dnia 16 listopada 2000 r. o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł oraz o przeciwdziałaniu finansowaniu terroryzmu w roku 2007 (Information of the General Inspector of Financial Information on the execution of the Act of 16 November 2000 on Counteracting Introduction into Financial Circulation of Property Values Derived from Illegal or Undisclosed Sources and on Counteracting the Financing of Terrorism in 2007), Warsaw.
- Grow, B. (2006). Gold Rush, [Electronic version] Business Week, January 9, 2006. Retrieved May 29, 2008 from the Business Week Web site: [http://www.businessweek.com/magazine/content/06\\_02/b3966094.htm](http://www.businessweek.com/magazine/content/06_02/b3966094.htm)
- Jasiński, W. (2001). Przeciw szarej strefie, Nowe zasady zapobiegania praniu pieniędzy (Against grey economy, New Standards of Fighting Money Laundering). Warsaw: Poltext.
- Joyce, B. P. (2001). E-diligence: Money Laundering Risks in the Electronic Arena. *Journal of Money Laundering Control*, 5(2), 146-149.
- Levi, M., & Reuter, P. (2006). Money Laundering. In M. Tonry (Ed.). *Crime and Justice: A Review of Research*. Vol. 34: (pp. 289-375), Chicago: Chicago University Press.
- Malcolm, J. G. (April 29, 2003), Statement before the Subcommittee on Crime, Terrorism, and Homeland Security. Committee on the Judiciary United States House of Representatives. Retrieved May 29, 2008 from <http://www.usdoj.gov/criminal/cybercrime/Malcolmtestimony42903.htm>
- Molander, R. C., Mussington, B. D., & Wilson, P. A. (1997). [Electronic version] Cyberpayments and Money Laundering. Problems and Promise., Washington: RAND Critical Technology Institute Report.
- Morris-Cotterill, N. (2001). Money Laundering. Retrieved May 29, 2008 from the Global Policy Forum Web site: <http://www.globalpolicy.org/nations/corrupt/2001/05morris.htm>
- National Drug Intelligence Center, U.S. Department of Justice (NDIC, 2006). [Electronic version] Prepaid Stored Value Cards: A Potential Alternative to Traditional Money Laundering Methods. Assessment. Product No. 2006-R0803-001.
- PayPal is given bleak choice by U.S. prosecutor for alleged violations of Patriot Act-fortified laundering law (2003, April). Retrieved December 31, 2006 from Anti-Money Laundering.Com on-line Data Base.
- Prengel, M. (2003). środki zwalczania przestępstwa prania pieniędzy w ujęciu prawnoporównawczym (The measures to fight the crime of money laundering in different legal systems). Toru : TNOiK Dom Organizatora.
- Rijock, K. (January 2, 2007). Virtual money laundering now available on the world wide web. Retrieved May 29, 2008 from the World Check Web site: <http://www.world-check.com/articles/2007/01/02/virtual-money-laundering-now-available-world-wide/>
- Skalski, D. (2004). Wykorzystanie sieci teleinformatycznych w procesie prania pieniędzy (The abuse of telecommunication networks in money laundering process). In S. Lelental & D. Potkowski (Eds.), *Pozbawianie sprawców korzyści uzyskanych w*

- wyniku przestępstwa (The forfeiture of proceeds derived from crimes) (pp. 103-114).  
Szczytno: Wydawnictwo Wyższej Szkoły Policji.
- Solicitor General Canada (1998, October). Electronic Money Laundering: An Environmental Scan. Retrieved May 29, 2008 from the Department of Justice (Canada) Web site: [http://www.justice.gc.ca/eng/pi/rs/rep-rap/1998/wd98\\_9-dt98\\_9/wd98\\_9.pdf](http://www.justice.gc.ca/eng/pi/rs/rep-rap/1998/wd98_9-dt98_9/wd98_9.pdf)
- U.S. General Accounting Office (GAO, 2002). Internet gambling: An overview of the Issues, Report to Congressional Requesters. GAO-03-89. Washington, DC: U.S. General Accounting Office.
- Veng Mei Leong, A. (2007). Chasing dirty money: domestic and international measures against money laundering. *Journal of Money Laundering Control*, 10(2), 140-156.
- Williams, P. (1998). Organizing Transnational Crime: Networks, Markets and Hierarchies. In P. Williams & D. Vlassis (Eds.), *Combating transnational crime: concepts, activities and responses*, *Transnational Organized Crime*, Special Issue, 4(3/4), pp. 68-69.
- Wollert, L. (2004), Can Online Betting Change Its Luck?. *Business Week*, December 20, 2004, 66-67.
- Wójcik, J. W. (2002), *Pranie pieniędzy, Kryminologiczna i kryminalistyczna ocena transakcji podejrzanych (Money Laundering, Cryminological and Forensic Analysis of Suspicious Transactions)*, Warsaw: Twigger.