2014

Typology Project

Cybercrime and Money Laundering

Eurasian Group on Combating Money Laundering and Financing of Terrorism

CONTENTS

Introduction

The modern IT community is featured by a routine use of computers, communication networks, mobile communication devices and other equipment. The government institutions as well as the banking, utilities, transportation and many other systems cannot properly function on an ongoing basis without reliable and flawless operation of computer and communication equipment. At present, information technologies are not just commonly used by people in their everyday work, but have become, in fact, the integral part of almost every aspect of a human life.

The spread of the computer and communication equipment-based information technologies as well as optimization and computerization of processes in each and all areas of life have blurred the boundaries and interconnected national economies and infrastructures.

Besides that, these trends have led to the emergence of the integrated global information environment where everyone can access any information in any place around the world, remotely manage personal and corporate assets, enter into contracts with foreign counterparties without face-to-face contact, etc.

At the same time, the information environment has become both the place and instrumentality of crime. Criminals no longer need to brainwash their "targets" and have personal contact with their potential victims. All they need is a computer and access to the information and communication system where they use computer viruses and other illegal devices for accessing databases, bank accounts and management information systems.

Theft of payment card (bank account) data or online banking access codes for stealing funds of banks' customers, theft of personal data or commercial information from personal computers or servers, intentional damage of information systems or communication equipment for inflicting losses on companies – this is, by no means, the exhaustive list of threats associated with the explosive development of modern information technologies. All this leads to emergence of a phenomenon known as cybercrime.

Cybercrime is becoming a global plague - new technologies provide anonymity to criminals and an increasing number of people lured by a chance of becoming rich in a quick and easy way are getting engaged in this type of criminal activity.

According to various estimates up to 40 percent of the world population (about 2.5 billion people) use the Internet and this number keeps on growing. It is forecasted that another 1.5 billion people will get access to the Internet over the next four years.

The Internet gains popularity for obvious reasons – a user is capable of accessing large volumes of information on the round-the-clock basis, can quickly share information with other users, carry out banking, trade and exchange transactions in any convenient place and time and do many other things.

The banking sector is one of the industries that heavily rely on modern technologies and the Internet. And given that these technologies are used for transferring funds, this business activity is becoming increasingly attractive to criminals.

The most widespread information and computer technology-related crimes include: unauthorized debiting (removal) of funds from bank accounts, payment card fraud, interference with online banking systems, distribution of computer viruses, DDoS attacks against websites and information network fraud. According to some experts, each year, the global losses inflicted by cybercrime exceed USD 100 billion.

Cybercrime acts can be prepared and committed right at the "workplace", i.e. this type of criminal offences are relatively easy to commit since computer equipment is continuously becoming cheaper. A cybercrime offence can be committed from any place around the world, while the target of a cybercriminal may be located thousand miles away.

Besides that, it is difficult for investigators to identify, record and seize forensically relevant information that can be used as physical evidence for prosecution.

The aforementioned specificities of this type of criminal offences along with high "profits" derived from them makes cybercrime more advantageous to criminals compared to other types of crime.

Therefore, the typology research of basic ways and methods used by perpetrators for laundering proceeds of cybercrime is currently of high importance and value.

Given that this problem is becoming ever more urgent, the 19th EAG Plenary held in November 2013 decided to undertake the Cybercrime and Money Laundering typology exercise in 2014. This typology project is led by the State Financial Monitoring Service of Ukraine (SFMS).

In course of the research, the questionnaire drafted by the SFMS was disseminated to all countries engaged in the typology exercise.

The research was informed by the responses to the questionnaire received from the following countries:

- Belarus (the EAG member country);
- Kazakhstan (the EAG member country);
- Tajikistan (the EAG member country);
- Uzbekistan (the EAG member country);
- Russia (the EAG member country);
- Armenia (the EAG observer country);
- Turkey (the EAG observer country);
- Ukraine (the EAG observer country);

- Vietnam;
- Macao;
- Slovakia;
- Slovenia;
- Sweden;
- Estonia.

The typology research focuses on the following issues:

• Identifying the essence of cybercrime and the most widespread methods used for committing cybercrime offences;

• Examining typical mechanisms, methods and tools used for laundering proceeds of cybercrime;

• Categorizing criteria and red flag indicators for timely identification of financial transactions potentially related to laundering of proceeds of cybercrime;

• Reviewing ways and methods used for combating cybercrime and for fighting against laundering proceeds of cybercrime.

1. CYBERCRIME: ESSENCE, TYPES, THREATS AND RISKS

1.1. International and National Aspects of Combating Cybercrime

The attention of both government authorities and international community has long been focused on finding the efficient ways of combating criminal offences committed with the application of information and communication systems.

In a situation where development of new technologies far outpaces adoption of the relevant regulations and amounts of funds illegally obtained by cybercriminals continue to grow, it is necessary to constantly seek efficient ways of addressing the new and emerging issues related to data protection, cross-border access of law enforcement authorities to stored data and public-private information exchange.

In the context of the adverse effects of this phenomenon, the international community continuously seeks measures that would minimize the impact of cybercrime on society. The recent years have seen significant developments in promulgation of international and regional instruments aimed at countering cybercrime. These include both binding and non-binding instruments.

The UNODC Comprehensive Study on Cybercrime and Responses of Global Community and Private Sector identifies five clusters of documents, consisting of instruments developed in the context of, or inspired by:

I) the Council of Europe or the European Union;

II) the Commonwealth of Independent States or the Shanghai Cooperation Organization;

III) intergovernmental African organizations;

IV) the League of Arab States;

V) the United Nations (hereinafter UN).

A significant amount of cross-fertilization exists between all these instruments, including, in particular, concepts and approaches developed in the Council of Europe Convention on Cybercrime adopted in Budapest, Hungary on November 23, 2001 (hereinafter the Budapest Convention). At present, the Budapest Convention serves as the foundation for the development of the national and global cybercrime legislation.

The Budapest Convention requires the states:

– To criminalize attacks against computer data and systems (that is, illegal access, illegal interception, data interference, system interference and the misuse of devices) as well as offences committed by means of computer systems (including computer-related forgery and fraud), content-related offences (child pornography) and infringements of copyright and related rights;

– To put in place procedural law measures to enable their competent authorities to investigate cybercrime and secure volatile electronic evidence in an efficient manner, including expedited preservation of stored computer data, expedited preservation and partial disclosure of traffic data, search and seizure of stored computer data, real-time collection of traffic data, interception of content data;

– To cooperate efficiently with other parties to the Convention through general (such as extradition, mutual legal assistance and others) and specific provisions (expedited preservation and disclosure of stored traffic data, trans-border access to stored computer data, establishing networks operation on the round-the-clock basis, etc.).

The Cybercrime Convention Committee (T-CY) has been established in order to allow the parties to the Convention to exchange information and consider possible amendments or protocols to the Convention.

Besides that, the Council of Europe, in 2006, launched the Global Project on Cybercrime aimed at:

- Assisting countries in strengthening their legislation;
- Training law enforcement prosecutors and judges;
- Strengthening public-private cooperation;
- Developing measures for the protection of personal data and protection of children against sexual exploitation and abuse.

The European Police Office (Europol) has developed its own cybercrime strategy. Currently, Europol provides the EU member state with investigative and analytical support on cybercrime through its online investigation system and cybercrime database.

The new European Cybercrime Center (EC3) attached to Europol was launched in January 2013. The EC3 priorities include investigations into online frauds, including those targeting e-banking and other online financial activities, online child abuse and other cybercrimes affecting critical infrastructure and information systems in the European Union.

In its first year, the European Cybercrime Center assisted in coordination of nineteen major cybercrime operations and investigations into criminal offences involving online frauds, hacking attacks and online distribution of child pornography.

At present, the EC3 supports nine large online child sexual exploitation police operations. It provides support to investigations into online distribution of child pornography and sextortion.

The European Cybercrime Center is currently providing operational and analytical support to sixteen investigations regarding payment fraud. In 2013, it supported investigations resulting in three different international networks of credit

card fraudsters being dismantled.

One operation led to the arrest of 29 suspects who had made a 9 million euro profit by compromising the payment credentials of 30,000 credit card holders.

The second network that was tackled resulted in 59 arrests, two illegal workshops for producing devices and software to manipulate point-of-sales terminals dismantled and cloned cards and cash seized. This organized crime group had affected approximately 36 thousand bank/credit card holders in 16 European countries.

The third operation targeted the Asian criminal network responsible for illegal transactions and purchase of airline tickets. Around 15, 000 compromised credit card numbers were found on the seized computers. The operation was coordinated by the EC3 in 38 airports in 16 European countries. The operation resulted in arrests of 117 individuals who were also found to be linked to other criminal activities, such as drug trafficking, human smuggling and counterfeit documents.

The important role in addressing the problems related to international cooperation on combating cybercrime is played by the UN which pays adequate attention to the spread of crimes involving information and computer systems and to counteracting such criminal offences. The UN has repeatedly emphasized the transnational nature of cybercrime and the need for coordination of global efforts aimed at prevention and investigation of such offences.

In May 2011, the United Nations Office on Drugs and Crime (UNODC) and the International Telecommunication Union (ITU) signed the Memorandum of Understanding for developing regulatory frameworks and legal mechanisms to counter the threats.

With the view of mitigating threats and reducing exposure of the information environment to such threats, the ITU, being the UN specialized agency, has developed: Global Cybersecurity Agenda; Guideline on Child Online Protection; Guidelines for Parents, Guardians and Educators on Child Online Protection; Guidelines for Industry on Child Online Protection; Guidelines for on Child Online Protection; Guideline for Policy Makers on Child Online Protection; Elements for Creating a Global Culture of Cybersecurity.

According to the UNODC experts forms of international cooperation include extradition, mutual legal assistance, mutual recognition of foreign judgments, and informal police-to-police cooperation. Besides that, due to volatile nature of electronic evidence, international cooperation in criminal matters in the area of cybercrime requires timely responses and the ability to request specialized investigative actions, such as preservation of computer data.

The important step in building the effective system for combating offences in the information society is the development of CIS Information Security Cooperation Agreement.

Listed below are the main areas of cooperation and coordination under this

Agreement:

- Harmonizing the information security-related laws and regulations of the Parties to the Agreement;
- Developing regulations for undertaking joint coordinated efforts in the information environment aimed at ensuring information security in the member states;
- Developing information security-related regulations and disseminating them to users;
- Promulgating laws and regulations covering production of hardware, software and information security products;
- Developing regional information security standards in line with other international standards in this area;
- Creating secure information systems for various applications;
- Arranging for trans-border transmission of information;
- Upgrading technologies for protecting information systems and resources against potential and real threats;
- Analyzing and assessing threats to information security of information systems;
- Enhancing the efforts undertaken for identification and neutralization of software and devices that pose threat to operation of information systems;
- Implementing coordinated measures for prevention of unauthorized access and leakage of information posted on the information systems;
- Protecting the restricted information and information technologies in interconnected systems with different degrees of protection;
- Upgrading interstate information systems and software owned by the member countries;
- Establishing mutually agreed procedure of certification and mutual recognition of certification of information security products;
- Developing advanced information security technologies;
- Conducting expert review of information security-related R&D and technology solutions;
- Retraining and professional development training of information security personnel;
- Summarizing, sharing and implementing best practices;
- Arranging for and holding workshops, symposia and meetings.

In September 2014, the handover ceremony of the building of the Interpol Global Complex for Innovation (IGCI) took place in Singapore. The IGCI mission

is to consolidate the law enforcement efforts of different countries aimed at combating cybercrime. The IGCI will become fully operational in 2015 after installation of modern equipment.

The IGCI will focus on four main areas: operational and investigative support, innovations, research and digital security, police staff training, international partnership and development.

At the national level, crime prevention comprises strategies and measures that seek to reduce the risk of crime occurring, and mitigate potential harmful effects on individuals and society. The good practices on cybercrime prevention include the promulgation of cybercrime prevention legislation and strategies, effective leadership, development of criminal justice and law enforcement capacity, education and awareness, the development of a strong knowledge base, and cooperation across government, communities and the private sector.

1.2. Essence and Types of Cybercrime

The legislation of the majority of countries participated in this typology exercises does not contain the notion or definition of cybercrime. The only exception is Kazakhstan, which legislation defines "information-related crime" (cybercrime) as a type of criminal offence involving criminally punishable actions committed with the use of information technologies.

In general, most responding countries define cybercrime in a similar manner as illegal (criminally punishable) actions committed in the area of information (computer) technologies or with the use of such technologies.

The UNODC experts note that definitions of cybercrime mostly depend upon the purpose of using the term.

A limited number of acts against confidentiality, integrity and availability of computer data or systems represent the core of cybercrime. Beyond this, however, computer-related acts for personal or financial gain or harm, including forms of identity-related crime, and computer content-related acts (all of which fall within a wider meaning of the term "cybercrime") do not lend themselves easily to efforts to arrive at legal definitions of the aggregate term.

Globally, cybercrime acts show a broad distribution across financial-driven acts, and computer-content related acts, as well as acts against the confidentiality, integrity and accessibility of computer systems.

The Budapest Convention, being the fundamental cybercrime instrument, provides for the following categorization of cybercrime:

1) Offences against the confidentiality, integrity and availability of computer data and systems, including:

- Illegal access, for example, be means of hacking, deception or otherwise;
- Illegal interception of computer data;

- Data interference, including intentional damaging, deletion, deterioration, alteration or suppression of computer data without right;
- System interference, including intentional serious hindering of the functioning of a computer system, for example, by means of distributed attacks against the key information infrastructure;
- Misuse of devices, i.e. production, sale, procurement of devices, computer programs, computer passwords or access codes for the purpose of committing cybercrime offences;

2) Computer-related offences, including forgery and fraud committed with the use of computers;

3) Content-related offences, including child pornography, racism and xenophobia;

4) Offences related to infringements of copyright and related rights, including illegal reproduction and use computer software, audios/videos and other digital products as well as databases and books.

At the same time, in terms of criminal motivation, cybercrime offences may be arbitrarily divided into the following categories:

- Cyber fraud for gaining illegal possession of funds;
- Cyber fraud for gaining illegal possession of information (for personal use or further sale);
- Interference with operation of information systems for accessing management information systems (for intentionally damaging them for fee/payment or for inflicting losses on competitors);
- Other offences.

The first category includes criminal offences committed for stealing (gaining illegal possession of) funds. Perpetrators use various ways and methods for achieving their malicious goals and sometimes put users in a situation where they unwittingly disclose confidential information.

The most widespread offences fall into the second and third categories. These offences involve database hacking and damaging government and corporate computer systems as well as theft of innovative solutions and technologies.

This report focuses on cybercrime offences committed for financial or other material gain in form of illegal proceeds. Primarily, it refers to misuse of information and communication systems and computer technologies for accessing assets owned by individuals and legal entities in order to illegally control or dispose of such assets. In particular, accessing funds of banking institutions' customers is currently the most "popular" type of cybercrime offences.

The most widespread offences that fall into this category are as follows:

1) Internet (online) fraud, including:

- Online Ponzi/pyramid schemes;

- Internet sales fraud and online auction fraud;
- Production of malware for stealing financial, commercial and personal information (setting up "dummy" websites, distribution of computer viruses and Trojans, traffic interception, etc.);

2) Remote (online/distant) banking fraud, including:

- Production of computer viruses and Trojans for establishing covert control over customer's computer with installed online banking software;
- Opening accounts, carrying out unauthorized transactions and withdrawing cash as a result of such unauthorized transactions in online banking systems;
- Receipt of payments via SWIFT from foreign originators as a result of interference with operation of computers and online banking systems of customers of foreign banking institutions.

3) Counterfeit payment card and ATM fraud:

- Use of lost/ stolen/ counterfeit payment cards;
- Theft of payment card details, *inter alia*, with the application of card cloning devices;
- Skimming – production, sale and installation of devices on ATMs for reading/ copying data off a payment card's magnetic stripe and stealing PIN-codes;
- Use of white plastic for cloning (counterfeiting) payment cards and withdrawing cash from ATMs;
- Transaction Reversal Fraud – interference with ATM operation where an error condition is created which makes it appear that cash will not be dispensed. This forces a re-credit of the amount withdrawn back to the account when in fact a perpetrator gets the cash;
- Cash Trapping – attaching a device to ATM so that when ATM tries to dispense cash the cash is trapped and legitimate card holder cannot receive it. A perpetrator then returns to the ATM and retrieves the trapped cash.

It should be noted that the explosion in information technologies continuously generates new services, including financial ones. This, in turn, forces criminals to improve their capabilities and invent new methods of obtaining illegal proceeds in the cyberspace.

1.3. Cybercrime-Related Threats and Risks

The MONEYVAL typology research entitled *Criminal Money Flows on the Internet: Methods, Trends and Multi-Stakeholder Counteraction* analyses the following cybercrime and money laundering-related risks:

- Technological risks;

- Operational risks;
- Regulatory risks;
- Geographical or jurisdictional risks.

Such categorization, however, is too general and requires further more detailed analysis with consideration for exposure of a society and countries to the cybercrime-related threats and vulnerabilities, consequences of their materialization and potential management and mitigation measures.

Based on the essence and categorization of cybercrime the following threats to a state and society are identified:

- Openness of state and society.

The existing computer network and IT-based infrastructure provides favorable environment that promotes international supply of goods, provision of services and transfer of funds between individuals and legal entities and allows for connecting computers to the Internet and online storage of information. On the other hand, it provides broad opportunities for committing cybercrime acts as well as for laundering proceeds of cybercrime and other offences with the use of computer technologies;

- Cybercrime is high-speed and low-cost offence.

The said infrastructure allows criminals to quickly access both any information, documents and private assets and cheap and practically anonymous online payment systems enabling them to hide traces of their crime and further move illegally obtained proceeds in a cost-effective manner;

- Cybercrime is high-tech offence.

Explosion in information technologies and complexity of this area along with lengthy and excessively bureaucratic process of promulgation of the relevant legislation and regulatory framework lead to a situation where the spread of cybercrime far outpaces measures taken to prevent and combat this type of offences;

- Complex nature of cybercrime offence.

Apart from obtaining financial gain or other material benefits from committing cybercrime offences, perpetrators also misuse computer technologies and information and communication networks driven by socio-psychological motivations. In particular, cybercrime acts are committed for discrediting governments and countries, setting up terrorist websites, damaging and destroying the key systems by entering false data into such systems or continuously rendering them inoperable (which is a supplement to a traditional terrorism);

- Anonymity of cybercrime offence.

Absence of a direct physical contact, relatively light punishment imposed in some countries and difficulties in identifying, recording and seizing forensically relevant information in the virtual space make cybercrime attractive to criminals;

- Transnational and widespread nature of cybercrime.

The specificity of cybercrime offence is that a cybercrime act can be prepared and committed from almost any place were a perpetrator can access the Internet. In a situation where computer equipment and online services are becoming available for an increasing number of people, cybercrime is also becoming increasingly “popular”.

Transnational nature of cybercrime provides attractive opportunities to criminals, i.e. they can operate from territories of jurisdictions with insufficient anti-cybercrime and AML/CFT systems and supervision regimes where they are unlikely become subject to investigations conducted by foreign law enforcement agencies.

Some countries are used as transit hubs as money flows are constantly directed to those countries, but at the same time, money flows are generated from those countries to other destinations;

- Cybercrime offences are committed by “mixed” organized groups.

At present, successful large-scale cybercrime acts can be committed only subject to adequate organization and preparation, which, in fact, makes cybercrime an organized crime. Cybercriminals mainly seek high profits, which leads to increase in computer-related offences in the financial sector, which, in turn, requires deep understanding and knowledge of financial relationships and banking activity. Besides that, cybercriminals actively use the services of “traditional” criminals who help them to convert the stolen funds into cash.

All threats listed above lead to emergence and development of vulnerabilities of the anti-cybercrime system, which are primarily related to:

- Untimely detection of cybercrime offences;

- Lengthy and complex nature of investigation into cybercrime acts and difficulties in use of evidences (including electronic ones) for criminal prosecution.

Certain features of electronic payment systems (which are easy to create and require low cost for upgrading) may be the factors indicating potential money laundering risks. High speed of transactions, including cross-border money transfers, facilitates various money laundering schemes. Low expenses associated with such transactions decrease the cost of money laundering services and encourage criminals to seek new sources of illegal proceeds. The fact that proceeds can be easily converted into real money or cash may potentially allow perpetrators to launder the ill-gotten gains of crime in many jurisdictions.

Increase in number of cybercrime offences committed in this area has resulted in general decline in public trust in financial system integrity, bank secrecy, personal data protection and financial transactions carried out with the application of new technologies. Such public distrust of financial service markets prevents free funds available to population from being invested into economic development.

Such consequences can be generally divided into the following categories:

- Financial consequences – financial losses incurred by banking institutions and their corporate and individual customers; profits lost by right holders; decline in backing sector growth rate;
- Reputational consequences – disclosure of confidential information, including bank secrets and personal data; customer distrust of banking system in general and remote (online/distant) banking services in particular which entails decline in volume of non-cash transactions;
- Legal consequences – customers' claims;
- Technological consequences – banking institutions, companies and organizations are forced to create (or purchase) complex, expensive and less convenient security tools and products to ensure reliable operation of their information, computer and telecommunication systems.

1.4. Remote (Online/Distant) Banking-Related Risks

At present, the banking systems of most countries provide broad enough opportunities for online (remote/distant) management of financial resources. "Customer-Bank", "Customer-Internet-Bank" and "Telephone Banking" are the most widespread online (remote/distant) banking services.

Before having access to e-banking, customers are typically required to open accounts with the bank face-to-face and subject to CDD measures. When face-to-face contact is impossible, these customers are subject to enhanced CDD measures to mitigate the relevant higher risk, like submission of information capable of independent verification, certification of documents presented and referral by an introducer who carries out the same CDD measures. But banks are discouraged to open e-banking accounts non-face-to-face.

Remote/distant identification allows wider use of dummy companies and front men who do not need to appear physically, but just hand over their IDs and passcodes, which impeded identification of cybercrime organizers and perpetrators.

The following methods and tools may be used for identification of a customer who carries out an online (remote/distant) transaction:

- Authentication by login ID, password, pass-phrase, security code, knowledge-based authentication (security questions in both shared secret or dynamic);

- Something the user has, such as security token, smart card, key fob and etc.;

- One time password delivered by SMS;

- Electronic/ digital signature.

Connection of a financial system to the Internet for providing remote (online/distant) services to customers enables cybercriminals to interfere with operation of banking and other payment systems.

The most serious threats posed by cybercriminals to the remote (online /distant) banking systems include:

- Theft or alteration (deletion) of banking information or personal data;

- Malware infection of banking systems;

- Disabling remote (online /distant) banking systems by sending bulk messages through botnets (networks of infected computers).

There are many cybercrime related vulnerabilities, which involve, *inter alia*, the use of malware for stealing customer information stored with credit institutions, intellectual property, technologies, etc.

To illegally obtain personal information perpetrators may send e-mail messages to credit institutions' customers inviting them, under various pretexts (like technical upgrading, database reconciliation or updating), to enter the provided codes manually via a computer keyboard into the screen forms in course of online sessions initiated by perpetrators (using, for example, a fake website). In this process, the customer's computer may be infected with malware in form of computer viruses or implants that run in the background and allow perpetrators to covertly obtain personal data of remote (online /distant) banking service users in an unauthorized manner.

Vulnerabilities of the financial system to cybercrime are, to a large extent, associated with insufficient protection of banking information.

Instead of attempting to attack a bank's system which is usually equipped with strong protection, cybercriminals often favor those e-commerce portals and payment system where a great number of personal information and credit card data are being stored and processed. Such stolen card data and personal information are further used for executing "non-genuine" transactions through the banking systems.

Vulnerabilities of the financial system to cybercrime are also, to a large extent, associated with low awareness of banking institutions' customers and non-compliance with the basis RBS rules and regulations.

In particular, banks' customers often use unlicensed software (anti-virus programs, in particular), inadequately use and store personal access passcodes and visit various websites using computers with installed RBS banking software. Such actions lead to malware infection of computers and facilitate access by cybercriminals to banking information and personal data.

It should be noted that, as shown by the recent events, the sphere of influence is not limited to internet banking but also includes credit card and bank account in relation to e-commerce, as well as mobile banking and portable devices.

Cybercriminals also target at loopholes of mobile devices, and the threats are growing faster than it does on personal computer. Not alike personal computer where anti-virus or security software is usually pre-installed by the manufacturer, smart phones and tablets are usually not equipped with any security protection software or tools. Besides that, mobile device holders tend to connect their devices to public free wireless network especially when travelling abroad. Such portable devices induce even greater risks of cybercrime nowadays.

Cybercriminals may also use SMS spoofing to lure mobile device users to browse a malicious URL. These attacks aim to capture bank account credentials when the customer logins to a fake website.

Besides that, remote/distant transactions may be done by third parties which identity is not known to the banks or payment companies. The real identity of the persons conducting the distant transactions is hidden and thus the system may be used for performing illegal or money laundering activities.

2. CYBERCRIME PROCEEDS

2.1. Financial Fraud with the Use of Computer Technologies and Information and Communication Systems

For the purpose of this report cyber fraud means fraud committed with the application of computers, computer networks, information and communication systems and the Internet.

It should be noted that the rapid expansion of the Internet has created the situation where a significant portion of the "traditional" businesses is shifting towards virtual environment. Primarily, it applies to online advertising of goods and services and online trade, which is widely enough spread across the globe and is regarded as a serious competitor to the traditional trade.

Fraudsters, in their turn, misuse the modern opportunities provided by the Internet for implementing their fraudulent schemes. The following types of fraud are widely enough spread:

- Internet sales fraud and online auction fraud (website spoofing – creating fake websites of popular online stores, sale of non-existing or counterfeit goods and services, etc.);
- Online Ponzi/pyramid schemes;
- Illegal online gambling;
- Posting fraudulent advertisements for illegal fundraising (illegal collection of charity donations), etc.

Case Study (Ukraine)

Individual P, who pretended to be a legitimate operator of the branch of K Investment Exchange, invited public to invest funds into the online trading operations.

The members of Investment Exchange K were promised to receive not just return on their investments but also extra profit for engaging other persons in this pyramid scheme.

To become the exchange traders the members had to pay the fee in amount of UAH 20,000 (USD 2.5 thousand).

More favorable trading conditions were offered to those traders who paid extra fee.

After signing the sham investment contracts with the members, funds were electronically credited to their accounts. However, it was done for the sheer sake of appearance, as the members were not able to cash out funds earned by them. When the traders demanded individual P to pay them the earned funds or to repay money invested by them, the latter avoided making any payments.

Neither Investment Exchange K nor its branches were registered in Ukraine.

Over 50 victims incurred losses amounting to over UAH 1 million (USD 125 thousand) as a result of this illegal activity.

Case Study (Ukraine)

The law enforcement agency identified a group of fraudsters who stole funds from individuals under the guise of selling goods at online auctions.

The perpetrators used other persons' data (names, ID codes, residential addresses, bank card details and other information) for registering on the website as the sellers.

The fraudsters obtained this information in advance from the penitentiary institutions.

Besides that, they rented residential apartments with connection to the Internet in various cities across Ukraine for registering each new account.

In order to hide their identities, the fraudsters presented false ID documents each time when they rented new apartment and used new computer equipment each time when they registered on online auction site. Besides that, they used the services of over 10 Internet service providers located in different regions of Ukraine.

It was established that 140 persons from all Ukrainian regions became the victims of these fraudsters.

Case Study (Ukraine)

In course of the Internet monitoring operation, the law enforcement agency obtained information on the criminal activities of a number of persons involved in the fundraising fraud.

A group of individuals developed, created and administered website A which they used under the guise of an investment agency for implementing the Ponzi scheme.

The criminal scheme was designed to lure individuals to invest their funds by promising them high profit in form of dividends and in-kind gifts, such as apartments, cars and various household appliances. As the number of investors grew, some "dividends" were paid to certain investors. However, when the amount of payable investment returns exceeded the amount of invested funds, the Ponzi scheme ceased its operation.

Around 150 individuals from various CIS countries took part in the investment project A and invested over UAH 0.5 million (USD 62.5 thousand).

Searches conducted in the office and homes of the Ponzi scheme organizers resulted in seizure of computer equipment containing the database of the Ponzi

scheme participants (total number of participants exceeded 8 thousand people) and the investment project financial documentation.

The criminal proceedings were instituted under Article 190 (3) (Fraud) of the Ukrainian Criminal Code.

Case Study (Ukraine)

The Ukrainian, Cypriot, Italian and Israeli nationals and unidentified individuals (which distributed the roles among themselves) organized the online gambling business where people could play poker, blackjack and roulette in real time.

The Italian national and other unidentified individuals funded this project. The Israeli national ensured operation and maintenance of the software systems. The Cypriot national monitored operation of the gambling venue, while the Ukrainian national maintained and managed operation of the gambling venue and hired young women as "bankers" and "stick women".

The perpetrators used the software systems that automatically read the cards and determine position of a ball on a roulette table. The bets were accepted from gamblers all around the world. The used software automatically determined the winning and losing bets, and the "bankers" and "stick women", staying in front of web cameras, dealt out cards and operated the roulette.

It was found out that the master server located in the UK was the basic platform for the websites that provided services to the owners of the online gambling websites and venues in both Kiev and abroad.

The criminal proceedings were instituted under Article 203-2 (Operation of Gambling Business) of the Ukrainian Criminal Code against the members of this organized group.

The search of the gambling venue conducted during the gambling session resulted in detention of the Cypriot national.

Twenty four "bankers" and "stick women" and three system administrators that ensured computer operation were also detained. Being seized were 19 gambling tables equipped with barcode readers, video cameras and displays (with displayed players' nicknames and bets), 22 personal computers, server equipment and documents that evidenced involvement of the said persons in this criminal offence.

2.2. Remote (Online/Distant) Banking Fraud

In modern world, the remote (online/distant) banking services and systems (such as "Customer-Bank", "Customer-Internet-Bank", "Online Banking", etc.) have become the integral part of the global financial system.

Remote (online/distant) banking (hereinafter RBS) is the general term for defining the technologies used for providing banking services against instructions issued by a customer remotely (i.e. without physically visiting a bank).

The RBS is the multipurpose software and hardware system that allows bank customers to draw up and send payment instruction and other documents for execution by a bank, monitor their accounts and received a wide range of updated financial information without physically visiting a bank.

RBS obviously provides certain advantages, the main of which are as follows:

- Efficiency and cost-effectiveness. RBS allows a customer to manage the financial flows of the company from its office and significantly reduces working time spent by personnel for visiting a bank;
- Simplicity and convenience. Automated process of preparation of payment and other documents as well as availability of software for completing the mandatory details in the documents greatly simplifies the use of subsystems and minimizes operational errors;
- Security and efficacy. The correctly and property used RBS can increase the security and confidentiality of workflow with a bank; allows for obtaining, at any time, an extract containing detailed information on all incoming and outgoing documents without having to visit a bank.

At the same time, RBS, being the tool that provides access to fund transfers, are more frequently targeted by cybercriminals.

Typically, interference with operation of RBS occurs as a result of malware infection of computer by means of spamming, or as a result of visiting infected websites or use of infected data storage devices.

Viruses are downloaded into a victim's computer without being observed. At the initial stage, virus just performs monitoring, collects information and sends it to fraudster's computer. Virus may steal RBS access passcodes, digital signature keys and read wire transfer payment details. Computers may also be infected by malware that intercepts secret information when a RBS access window is opened on computer display or copies information contained in i/o buffer when a computer is connected to e-payment system.

The goal of fraudsters is to distort information and generate and perform, through RBS, a payment transaction that will not stand out in a stream of victim's regular activities but will transfer funds to an account of a front man or a dummy company for a purpose typical for such customer. After that, fraudsters typically cash out the stolen funds using ATMs to avoid face-to-face contact with bank officers.

Case Study (Ukraine)

Funds in amount of USD 0.4 million (UAH 3.1 million) were transferred by a non-resident company registered in the United States and credited to the account of Ukrainian national G as payment for the work performed under the contract.

The recipient of these funds (individual G) appeared to be the 18 years old young man. He had no officially reported sources of income and was not engaged in any business activities.

According to the US law enforcement authorities the funds were transferred as a result of interference of an unidentified person with the non-resident company computer network with the use of Zeus Trojan malware.

Based on the information received from the US law enforcement authorities the Ukrainian FIU ordered to suspend transactions carried out through the account of individual G.

The criminal proceedings were instituted under Article 190 (1) (Fraud) of the Ukrainian Criminal Code. The investigation is still underway.

Case Study (Ukraine)

Individual M got acquainted with an unidentified person who invited him to conspire in order to steal money from company A.

Individual M, knowingly using the forged passport issued to other person, approached company B and requested it to assist him in registration of company K, introducing himself as the director and sole founder of company K.

In order to steal money from company A, individual M authorized personnel of company B to represent him in all institutions and organizations, irrespective of their ownership structure, on all matters related to government registration of company K.

Company K was registered and its corporate account was opened with bank F.

The perpetrators misused the "Customer-Bank" system for generating false payment documents for transferring UAH 3.7 million (USD 0.5 million) from company A account to the account of company K.

On the same day when the transaction was carried out, individual K, acting in the capacity of the director of company K, visited bank F and presented counterfeit cheques to withdraw UAH 3.7 million (USD 0.5 million) cash.

Individual M was convicted by court for committing the criminal offences punishable under Article 190 (1) (Fraud), Article 200 (2) (Illegal Actions in Respect of Remittance Documents, Payment Cards and Other Means Providing Access to Bank Accounts, E-Money and Equipment for their Production) and Article 205 (1) (Sham Business) of the Ukrainian Criminal Code and was sentenced to 8 years of imprisonment with confiscation of all assets.

Later on, the appeal court sentenced individual M under Article 190 (4) (Fraud) of the Ukrainian Criminal Code to 6 years of imprisonment with confiscation of all assets.

Case Study (Ukraine)

The law enforcement agency detected unauthorized tampering with the "Customer-Bank" system of government-owned company C and illegal transfer of UAH 2.0 million (USD 250 thousand) from the bank account of this government-owned company to the account of four companies opened with different banks.

The criminal investigation was launched under Article 361(2) (Unauthorized Interference with Operation of Computers, Computer-Aided Management Systems, Computer Networks or Telecommunication Networks) of the Ukrainian Criminal Code.

In course of the pre-trial investigation, it was discovered that the company C computer on which the "Customer-Bank" system was installed was infected with malware. The criminals used the stolen digital signature keys of the managers to remotely generate and send payment instructions on behalf of company C. The computer was seized for forensic examination.

The law enforcement officers promptly disseminated information to the Ukrainian FIU which issued the order to suspend all debit transactions carried out through bank accounts of the aforementioned business entities.

The investigation is still underway.

Case Study (Belarus)

Four Belarusian nationals set up, jointly with other unidentified persons, the organized criminal group. Since November through April 2010, they stayed in Minsk city (Belarus) and Kiev city (Ukraine) and under the pretext of selling anti-virus software illegally obtained personal data of the Internet users and details of their bank cards. After that, they used these data for entering false information on purchase of anti-virus software into computer systems of the US and other foreign banks and payment systems processing centers. As a result of this fraud they stole 5 billion 160 million rubles (by committing 189,227 thefts).

Case Study (Tajikistan)

Unidentified individuals hacked the security system of the remittance office of the branch of one of the banks located in city Y and stole USD 130,200 by transferring them to the accounts of a number of foreign nationals. The criminal investigation under Article 289 (1) (Unauthorized Access to Computer Data) and Article 244 (4) (Theft) of the Tajik Criminal Code is underway.

2.3. Counterfeit Payment Card and ATM Fraud

In modern world, payment cards are not just used for drawing wages, pensions and making payments but also serve as the effective and convenient tool for receiving the entire range of banking services.

The use of payment cards helps to:

- Reduce the quantity of cash in circulation;
- Additionally secure funds (if a card is lost, funds are blocked and kept on the account of a card holder);
- Carry out transactions in both national and foreign currencies (multi-currency cars);
- Make payments on the round-the-clock basis in different countries.

Large volumes of financial transactions carried out with the use of payment cards are the factor that attracts criminals who invent various methods for stealing funds from credit card holders. These methods may involve, in particular:

- Devices installed on ATMs for getting possession of payment card or money;
- Devices that read payment card information or information entered by a card holder on the ATM keyboard;
- Infection of computers with special viruses for obtaining information on payment cards (by creating fake websites or hacking websites, using botnets for distribution of malicious spam);
- Counterfeiting payment cards using the stolen information;
- Phone fraud (fraudsters identify themselves as bank officers and try to get necessary information).

There are many types of payment card and ATM fraud (phishing, pharming, thrashing, skimming, trapping, phantom, shutter, shimming, etc.) but all of them are intended for stealing money, payment card or payment cards details, such as:

- Card number;
- Card issue/expiration data;
- CVV2 number (a 3 digit number on the back of a payment card for validation of transactions carried out over the Internet or phone);
- Customer’s first and last names in Latin;
- PIN-code.

Criminals may use the stolen information not just for counterfeiting a payment card or for stealing funds, but may also sell this information on special websites and Internet forums.

Case Study (Ukraine)

In order to get possession of other person's property in a deceptive manner, individual M used the computer to place the order online for purchasing a Samsung TV set of behalf on individual B. Individual M paid for the ordered TV set by transferring funds to the account of individual entrepreneur K using the details of a bank card owned by an unidentified person. Therefore, individual M was not the holder of this card.

On the same day, individual B received the UAH 16.6 thousand (USD 2.1 thousand) worth Samsung TV set and paid UAH 7.0 thousand to individual M who told him that the seller offered a discount. Thus, individual M disposed of the property at his discretion.

Besides that, in order to get possession of other person's property in a deceptive manner, individual M used the computer to place the order online for purchasing another Samsung TV set and a notebook. Individual M paid for the ordered goods by transferring funds to the account of individual entrepreneur K using the details of a bank card owned by an unidentified person. Therefore, individual M was not the holder of this card.

On the same day, the ordered goods which cost amounted to UAH 14.4 thousand (USD 1.8 thousand) were delivered to the place of residence of individual M who disposed of them at his discretion.

Later on, the banking institution, through which the unauthorized transaction were carried out, confirmed that money was transferred illegitimately and, therefore, individual entrepreneur K incurred losses in the aforementioned amount.

The court convicted individual M for committing the criminal offence punishable under Article 190 (3) (Fraud) of the Ukrainian Criminal Code and sentenced him for 4 years of imprisonment. However, pursuant to Article 75 (Remission of Sentence with Probationary Period) of the Ukrainian Criminal Code individual M was sentenced to a term of probation of 3 years.

Case Study (Ukraine)

The director of a banking institution reported to the law enforcement agencies about unauthorized installation of skimming devices on the ATMs of his bank and further theft of funds from customers' card accounts.

The detective operation resulted in detention on the spot of a Bulgarian national who installed the home-made skimming devices on the ATMs of the aforementioned bank for further stealing funds from bank accounts with the use of counterfeit payment cards.

The pre-trial investigation discovered that the perpetrator was the member of the criminal gang consisting of 5 Bulgarian nationals who committed similar offences in Ukraine and other CIS countries.

After that, being detained on the spot was another Bulgarian national who installed the home-made skimming devices on the ATMs of another bank for further stealing funds from bank accounts with the use of counterfeit payment cards.

The home-made skimming devices were seized in his hotel room.

The criminal proceedings were instituted against those individuals for committing the criminal offences punishable under Article 190(3) (Fraud) and Article 200(2) (Illegal Actions in Respect of Remittance Documents, Payment Cards and Other Means Providing Access to Bank Accounts, E-Money and Equipment for their Production) of the Ukrainian Criminal Code.

Case Study (Ukraine)

In course of the pre-trial investigation, the law enforcement officers discovered that the skimming device intended for reading bank card magnetic strip and the video camera for capturing card PIN-codes were installed by the group of Romanian nationals on the entrance door of a banking institution. Using this information, these individuals forged duplicates of payment cards issued by the Ukrainian banks and withdrew from the ATMs UAH 14.7 thousand (USD 1.8 thousand) kept on the accounts of the bank customers.

Two Romanian nationals were detained when they attempted to remove the earlier installed skimming device.

The court convicted those individuals for committing crimes punishable under Article 185(2) (Theft), Article 190(3) (Fraud), Article 200(2) (Illegal Actions in Respect of Remittance Documents, Payment Cards and Other Means Providing Access to Bank Accounts, E-Money and Equipment for their Production) and Article 231 (Collection for Use of Use of Information Constituting Commercial or Bank Secret) of the Ukrainian Criminal Code and sentenced them to 3 years of imprisonment with imposition of fine in amount of UAH 85.0 thousand (USD 10.6 thousand) on each of them.

Case Study (Belarus)

Four Belarusian nationals conspired to steal money. For this purpose they installed skimming devices capable of reading magnetic strip of bank cards on ATMs of one of the Belarusian banks and copied, in unauthorized manner, information of the card holders. After that, they stole a total of 98 million rubles from banking institutions' customers (committed 260 thefts). In course of the search of the suspects' homes, the law enforcement officers found the underground lab where skimming devices were manufactured. Three ready-to-use and 69 prefabricated skimming devices were seized.

Case Study (Kazakhstan)

Individual G, holding the position of credit policy manager in one of the Belarusian banks, discovered that STL software used for generating loan applications was faulty. She shared her discovery with individual C who had criminal record for murder.

Individual C set up the organized criminal group consisting of 4 members that forged 24 counterfeit credit cards (on which 1.4 million tenge were credited) using personal data of real people. This criminal activity resulted in theft of 395 million tenge, while other funds were blocked.

Individual C was convicted for committing this criminal offence and was sentenced to 10 years of imprisonment and his accomplice, individual P (the bank security officer), was sentenced to 8 years of imprisonment. Criminal prosecution of other individuals was terminated after they had reach settlement with the victims.

Case Study (Kazakhstan)

In April 2013, a Moldavian national who came to Kazakhstan for stealing money from card accounts of individuals by installing skimming devices on ATMs was detained in Almaty city. Following the investigation, he was found guilty in committing four thefts and was sentenced to 3.5 years of imprisonment. In April 2013, a Bulgarian national was detained in Almaty city for committing similar criminal offence and was sentenced to 5 years of imprisonment.

2.4. Non-Financial Cybercrime

For the purpose of this report non-financial cybercrime means criminal offences that are committed in cyberspace but are not directly related to financial services and money transfers. However, the main goal of such crime is to gain illicit proceeds.

Such criminal offences include:

- Disabling computers and computer networks (DDoS attacks against websites, knocking competitors' websites off-line, etc.);
- Theft of commercial or personal data;
- Cyber extortion, intimidation, defamation and dissemination of false information on the Internet;
- Infringement of copyright and related rights by illegal reproduction and use of computer software and posting audios/videos and other types of digital products on the Internet;
- Content-related offences, including child pornography, child exploitation and sexual abuse, racism and xenophobia.

Case Study (Ukraine)

A group of persons conducted a series of online attacks and stole commercial data from business computers of Turkish, US and German nationals.

To get the stolen data back the victims were required to pay money. They transferred the required funds to Ukraine via Western Union for the benefit of the criminal scheme organizer. The received funds were cashed out by his representative from the card account.

A total of USD 20.0 thousand were illegally obtained by the individuals involved in this scheme.

Based on the information provided by the Ukrainian FIU the law enforcement agency launched the pre-trial investigation under Article 209(3) (Legalization (Laundering) of Proceeds of Crime) of the Ukrainian Criminal Code.

Case Study (Ukraine)

Individual M conducted online (DDoS) attacks against websites of Ukrainian and foreign business entities. He utilized special modified malware for creating botnets (large number of infected computers).

The attacks were conducted, in particular, with the use of DirtJumperV5 which allowed him to remotely control more than five thousand zombie (infected) computers in different countries. Overall, individual M conducted over 50 botnet-based DDoS attacks.

The attacks were conducted at the request of competing business entities.

Individual M used the virtual payment systems (the e-purses were registered in the names of front men) to receive remuneration for his services. He used wireless modem (Wi-Fi) for accessing the Internet on a prepaid basis.

The court convicted individual M for committing the criminal offence punishable under Article 361(1) (Unauthorized Interference with Operation of Computers, Computer-Aided Management Systems, Computer Networks or Telecommunication Networks) of the Ukrainian Criminal Code and imposed fine in amount of 700 non-taxable minimum wages (UAH 11.9 thousand / USD 1.5 thousand) and confiscated the hardware and software used for unauthorized tampering.

Case Study (Belarus)

On October 2012, an unemployed graduate of one of the Belarusian Universities (who had Master degree in engineering) was detained at his home as a result of the detective operation. Since June through July 2012, the said individual used malware for blocking operation of personal computers in Belarus.

During the aforementioned time period, the High-Tech Crime Department of the Belarusian Interior Ministry received multiple reports from individuals who complained that after accessing the Internet their computers became disabled, i.e. when the operating system was downloaded, all I/O devices (keyboard, mouse) became disabled and the message stating that the computer was blocked by the Belarusian Interior Ministry for viewing and distributing pornography was displayed on the screen. The message also stated that in order to get the computer unblocked the user should transfer 100,000 Belarusian rubles to the EasyPay e-purse account or to the Life mobile phone account.

Those actions discredited the Belarusian Interior Ministry and seriously damaged the reputation of the law enforcement agencies.

Case Study (Belarus)

Since March through December 2012, a Belarusian national used personal computer and independently developed software for accessing computer data stored in the computer system of one of the Belarusian companies.

Besides that, the said individual copied, in unauthorized manner, information stored in personal computers of Minsk residents, including Internet banking access passcodes and information on email boxes and personal pages in social networks.

He also personally developed and used malware for copying, in unauthorized manner, information stored in the computer network of the Belarusian National University.

The criminal proceedings were instituted under Article 348 (Unauthorized Access to Computer Data), Article 352-3 (Gaining Unauthorized Possession of Computer Data) and Article 354 (Development, Use or Distribution of Malware) of the Belarusian Criminal Code.

Case Study (Uzbekistan)

The law enforcement agencies launched investigation under the criminal proceedings instituted against a foreign national A under Article 278-3(2)(a) (Production for Sale or Sale of Special Equipment for Illegal (Unauthorized) Access to Computer Systems) of the Uzbek Criminal Code.

The investigators established the following. Individual A conspired with two unidentified persons to illegally access the secured computer-based international phone communication system. For this purpose he installed and connected, in breach of the applicable legislation, a special device to the Internet. Since November 2011 through January 31, 2012, the said persons used that device for making international phone calls by-passing the equipment of the telecommunication company.

Total duration of those phone calls was 5,002,843 minutes and the telecommunication company incurred losses in amount of USD 280,159.21.

Individual A was accused of committing the criminal offence punishable under Article 278-3(2)(a) (Production for Sale or Sale of Special Equipment for Illegal (Unauthorized) Access to Computer System) of the Uzbek Criminal Code. On November 29, 2012, pursuant to Article 381 (Referral of Criminal Case to Prosecutor) of the Uzbek Criminal Procedure Code the matter along with the indictment was turned over to the prosecutorial authority.

3. CYBERCRIME AND MONEY LAUNDERING

Unlike the "traditional" money laundering methods, which rely on the banking system, cyber-laundering depends on the use of various types of transactions and financial services providers, ranging from wire transfers, cash deposits/withdrawals and e-money transactions to "money mules" and remittance services.

Typically, the chain is broken on a cash transaction, which is generally carried out by "money mules", followed by the use of traditional payment systems. If the chosen payment system has integrated online payment capabilities, the money may then get converted into electronic cash prior to being transferred instantly and almost anonymously abroad, making the task of identifying and tracing the illegal funds by law enforcement extremely challenging.

The intricacy of these schemes poses a challenge to the powerful, but traditional AML/CFT data compilation software based on the patterns of customer behavior.

Another challenge faced by law enforcement officials seeking to identify and trace criminal revenue comes in the form of online payment systems with remote transaction execution capabilities.

3.1. Principal Mechanisms for Laundering Cybercrime Proceeds

When laundering the proceeds of crime, criminals need to be quick and efficient. For this reason, and also given the specificity of cybercrime, the majority of organizers and perpetrators of cybercrime-related criminal schemes tend to be well-educated and technically competent individuals, meaning that the money laundering methods developed by them can also be quite complex and unconventional.

The choice of tools and mechanisms used by criminals to launder cybercrime proceeds is quite diverse. Among the most common of them are:

- use of accounts opened with the help of lost documents or nominees;
- use of fictitious (transit) companies;
- use of remote access to carry out financial transaction via multiple bank accounts;
- use of cash in the final stage of the chain of financial transactions;
- use of alternative payment systems (e-payments), both national and international;
- purchase of electronic money and use of e-wallets;
- conversion of illegal proceeds into goods through the purchase of the latter over the Internet.

Conversion of stolen funds into cash is common because the movement of cash outside the banking system is nearly impossible to track. Another popular money laundering method involves cash withdrawals via ATMs, as it allows criminals to avoid face-to-face contact with bank employees. Later, the withdrawn cash can be channeled unhindered to the cybercrime organizer using the services of money couriers (mules).

Criminal proceeds are used to purchase readily marketable goods or prepaid cards, which can later be sold for cash. Also dirty money can be used to purchase tickets, travel documents, household items, etc. over the Internet for subsequent use or resale.

Part of the criminal proceeds are invested into the purchase of new equipment and development of even more powerful malicious software designed to bypass security systems.

Also noticeable is the citing by criminals of different reasons for payments related to unauthorized debiting of funds. This is done in order to make such payments indistinguishable from other financial transactions.

At the same time, criminals sometimes give rather unusual reasons for the crediting of funds from abroad, i.e. casino winnings, sale of intellectual property rights, web sites, online stores or virtual casinos, etc.

Case Study (Ukraine)

Law enforcement officials uncovered a case involving unauthorized debiting of funds totaling UAH 900,000 (equivalent to $112,500) from the current account of Company C to the account of Company G using a stolen Client-Bank electronic access key.

The account to which the funds were credited had been opened 10 days prior to these transactions. In the space of just one day, the stolen funds were transferred through the accounts of several companies.

As the result of timely intervention, all stolen funds were returned to the account of Company G and blocked their by the Ukrainian FIU.

In addition, Company G also attempted to transfer the illegally acquired funds to the account of Company L, but failed to receive the bank's authorization for the transaction.

The Company G director and founder – Mr. N – has been charged under Section 1 of Article 191 "Appropriation and embezzlement of property or seizure thereof by malpractice" of the Criminal Code of Ukraine.

Case Study (Ukraine)

Law enforcement officials uncovered several unauthorized transfers of funds from multiple companies to the accounts of private entrepreneur Mr. W held in banks A and B.

In the space of one day, the funds from the accounts of four companies were transferred to the account of private entrepreneur Mr. W held in bank A. Subsequently, part of that money was withdrawn in cash by private entrepreneur Mr. W.

The fraudulent transfers were carried out by hacking into the Client-Bank system and altering the details of the recipient.

According to the available information, private entrepreneur Mr. W acts as a front man and leads antisocial lifestyle.

Additionally, the account of private entrepreneur Mr. W was credited with UAH 280,000 (equivalent to $35,000), which were transferred without authorization from the account of Company C. The money was sent back to the sender during the same day.

Within hours, unauthorized transfers of funds were made from the account of Company C to the card accounts of seven Ukrainian nationals.

The Ukrainian FIU suspended all financial transactions carried out through the accounts of the said Ukrainian nationals. The uncovered evidence was used to initiate criminal proceedings under Section 4 of Article 190 "Fraud" of the Criminal Code of Ukraine.

Case Study (Ukraine)

A group of individuals opened a chain of clandestine gambling halls specializing in online gambling (gambling is banned in Ukraine).

As a result of these activities, one of the group ringleaders generated revenue in excess of UAH 1 million (equivalent to $125,000).

With the goal of laundering this revenue, the said person purchased jewelry and placed it in safe deposit boxes available for rent in commercial banks. Following the discovery of the clandestine gambling establishments, the police opened a criminal case under Section 1 of Art. 203-2 "Gambling" of the Criminal Code of Ukraine.

Searches of the gambling halls, the office and the private properties of the defendants resulted in the seizure of a total of UAH 317,000 (equivalent to $39,600), $19,800, EUR 7,100, 56 slot machines, 526 items of computer equipment (PC towers, monitors, laptops and modems), 57 mobile phones, 2 electronic roulettes and a 9mm handmade revolver-type handgun with a silencer and 15 rounds of ammunition for it.

Following the investigation, one of the criminal scheme organizers was charged under Section 2 of Article 209 "Money laundering" of the Criminal Code of Ukraine.

Case Study (Ukraine)

Mrs. L, a leading expert at the Bank, committed fraud and breach of trust by using the bank computer equipment, i.e. her workplace computer connected to the Client-Bank system, to take possession of the funds in the bank account belonging to Mr. W. In order to conceal the origin of the illicit funds, Mrs. L transferred them to the bank account of her husband.

Mrs. L used the criminally obtained funds to boost her family budget, pay bills, purchase household goods and services and to support her husband's business activities.

The total amount of funds laundered by Mrs. L totaled UAH 307,100 (equivalent to $38,400).

To guarantee redress, Mrs. L's property totaling UAH 200,000 (equivalent to $25,000) was seized. The measures undertaken resulted in the payment of damages totaling UAH 123,600 (equivalent to $15,500).

Mrs. L was found guilty under Section 3 of Article 190 "Fraud" and Sections 1 and 2 of Article 209 "Money laundering" of the Criminal Code of Ukraine and sentenced to 5 years imprisonment with deprivation of the right to hold positions related to the provision of money services at credit and financial institutions and ordered to pay UAH 307,100 (equivalent to $38,400).

Case Study (Tajikistan)

After obtaining information about non-resident entrepreneur Mr. H's plans to transfer $106,000 to country Z, Mr. B hacked Mr. H's email account from his computer and diverted the funds to a different beneficiary bank in country Z. Mr. B then flew to country Z and collected the transferred funds. Mr. B was charged under Section 3 of Articles 244 "Theft", Section 1 of Article 298 "Illegal access to computer data" and Section 1 of Article 299 "Modification of computer data" of the Criminal Code of Tajikistan.

Case Study (Slovenia)

Several Slovenian banks and their customers fell victim to a series of hacker attacks against information systems, resulting in significant losses. A total of 50 such attacks were carried out, costing customers more than EUR 1,500,000. The ensuing investigation identified one person responsible for all of these attacks and a group of individuals involved in the laundering of the stolen proceeds. The defendants are expected to be charged with criminal offences committed as part of an organized criminal group (OCG).

Attacks carried out by the criminals were very sophisticated in their nature and relied on the use of computer viruses and hacking programs to steal customers' bank account data (passwords and digital certificates). The stolen funds were laundered using bank accounts of individuals (nominees) disguised as corporate accounts. Some of the men of straw involved were members of organized criminal gangs, others were "innocent victims" hired to do this job through the

Internet, often because they had personal financial problems. The scheme involved the transfer of criminal proceeds to the nominees' bank accounts for subsequent cash withdrawals and handover to the scheme organizers.

Following the receipt of the first STRs concerning this scheme, the FIU conducted an analysis of data aimed at identifying the scheme and finding ways to suppress it. It was revealed that all attacks against information systems were carried out between 00:00 and 6:00 am. The fraudulent transactions were hidden among thousands of legitimate transactions (payment of wages and interest, direct debit, etc.) conducted during the same time period. As it turned out the weakest part of this scheme were cash withdrawals, which were typically made on the same day immediately after the opening of banks, usually between 8:00 and 12:00 am. In some cases, the time difference between the commission of a predicate offence and a cash withdrawal was just 3-4 hours. The FIU informed the banks of the established facts, while the Association of Banks of Slovenia issued guidance aimed at preventing and detecting such cases. Banks were instructed to be on the lookout for cases involving execution of a large number of transactions in a short period of time, as well as transfers of large sums to "dormant" and newly opened accounts. Since the time factor played a crucial role in this case, the banks, the FIU and the police agreed to use informal methods and channels of communication. For example, it was agreed that the FIU would initiate an investigation and suspend transactions after receiving a telephone call, without waiting for the arrival of STRs. The banks, in turn, agreed to submit the required information and documents to the FIU upon a telephone or email request. All this was done in order to speed up the investigation process, block the transaction and apprehend the nominees. After several more attacks, the FIU managed to halt several large-scale transactions, although transactions featuring small amounts remained undetected.

In response, the criminal group immediately began using more bank accounts and execute transactions with smaller amounts. In one instance, criminals attempted to launder EUR 50,000 by splitting the amount into more than 10 transactions involving 6 bank accounts of two individuals and two legal entities before converting it into cash and withdrawing. It became obvious that the success achieved by law enforcement agencies forced criminals to alter the very nature of their attacks against information systems.

In total, the FIU issued more than 20 transaction suspension orders related to the activities of this criminal group, amounting to aprx. EUR 800,000. However, this was only half of what was stolen by them. In the end, the group ringleader was charged with 32 counts of large-scale embezzlement and 17 counts of money laundering. He faces a prison sentence of 22 years, as well as the prospect of charges linked to other offences. In addition, more than 30 money-laundering charges were brought against other members of the gang. For example, one of the criminals who participated in this scheme and personally withdrew aprx. EUR 200,000 was sentenced to 4 years imprisonment for money laundering.

3.2. Use of Alternative Payment Systems and E-Money for Money Laundering

Remittance systems (both national and international) and electronic money allow criminal to quickly and effortlessly launder cybercrime proceeds.

Electronic payment systems have a number of advantages contributing to their growing popularity, i.e.

- accessibility – electronic accounts are free to any user;
- ease of use – opening and using electronic accounts is easy and requires no special knowledge;
- mobility – electronic accounts can be operated by users remotely over the Internet;
- efficiency – account transactions are executed within seconds;
- security – transferred data is encrypted.

Anyone wishing to become a payment system user needs to register and open an electronic account (e-wallet), where information about the user's funds in the electronic system is stored.

Financial transactions are carried out using the funds previously uploaded into the electronic system, i.e. your e-wallet. Different payment systems offer different options for adding money to e-wallets, ranging from wire transfers, postal orders, prepaid cards, payment terminals, etc.

Electronic payment systems operate using electronic money, i.e. a financial instrument that enables the user to exchange the right of claim for values using virtual accounts and electronic records (e-mail, etc.), as well as to convert this right of claim into cash and other highly liquid instruments.

Electronic money can be used to carry out the following transactions:

- intrasystem payments to the accounts of individuals and legal entities;
- online purchases;
- payment of mobile phone bills;
- payment of utility bills;
- payment for Internet access;
- payment of state taxes, duties and fines;
- purchase of train/airline tickets;
- purchase of fuel;
- hotel bookings, etc.

Criminals value electronic money for their anonymity in opening and replenishing e-wallets, round-the-clock availability and speed of transactions

(within seconds). The e-wallets of private persons tend to be connected to such persons' e-mails or mobile phone numbers.

In addition, in order to transfer cash between various scheme participants, criminals often use international money transfer systems. The process of sending remittances is very straightforward and highly efficient.

To send money, a customer must come to one of the system agents, show his ID, fill out a remittance form, specifying the recipient's name, surname and destination country, and present the amount he wishes to send. In return, the customer is given the remittance number for communication to the recipient.

To receive the remitted funds, the recipient must come to one of the payment system agents in his country, show his ID and fill out the RECEIVE MONEY form, specifying the sender's name and surname as well as the name of the country the money is sent from and the remittance serial number.

It takes only a few minutes to send or receive remittances.

Case Study (Ukraine)

The card account of one Ukrainian national was illegally debited. As the result of several unauthorized transactions, the funds were transferred to the card accounts of two Russian nationals.

Transactions were made through the electronic payment system LIQPAY, which supports mobile phone and online payments.

Criminal proceedings were initiated under Section 1 and 2 of Article 361 "Tampering with computers, automated systems, computer networks or telecommunications networks" and Section 3 of Article 190 "Fraud" of the Criminal Code of Ukraine.

Case Study (Ukraine)

One organized criminal group used telephone threats and intimidations directed against the health and safety of the victims' relatives to persuade private individuals to top up e-wallets of unknown persons, extracting a total of UAH 30,000 (or about $4,000).

In order to conceal the origin of the criminal income, the funds deposited to these e-wallets by the victims of blackmail were then transferred to other payment systems and deposited into e-wallets there.

The investigation of the case, initiated by the police based on the materials provided by the FIU of Ukraine, is still ongoing.

Case Study (Ukraine)

Three individuals committed fraud by remotely debiting accounts of legal entities using the latest information technologies.

The funds stolen from the accounts of the three legal entities registered in different regions of Ukraine were then transferred through the accounts of several private individuals prior to being credited to the accounts of third parties. Subsequently, part of the funds were converted into electronic money and withdrawn as cash. The incident is now subject to a pre-trial investigation conducted under Section 3 of Article 209 of the Criminal Code of Ukraine "Money laundering".

4. METHODS AND TECHNIQUES FOR PREVENTING AND COMBATING THE LEGALIZATION OF CYBERCRIME PROCEEDS

4.1. Identification of Financial Transactions Suspected of Being Linked to the Laundering of Cybercrime Proceeds

Despite the increasing sophistication and range of money laundering tools at cyber criminals' disposal, all financial transactions can be split into groups based on the level of risk. Furthermore, it is also possible to define the areas and services that are most at risk and therefore in need of extra attention.

It should be noted that customers who establish business relationships with banks or use banking services remotely with the help of modern technologies tend to be placed in groups with a higher money laundering risk.

A list of suspicious financial transaction indicators in this area include the following:

- login attempts made from a banned/new IP-address;
- attempted use of expired primary/operational or old keys after the certification of new ones;
- use in banking transactions of IP-addresses or user names suspected based on preliminary monitoring of being involved in fraudulent transactions;
- execution of transactions in unusual time or connecting to the system in the evening;
- unusual terms or complexity of a transaction: a large number transfers occurring within a short period of time, a large number of different sources of funds and payment methods (instruments);
- a person is not aware of the nature of the legal entity's activities he represents;
- a person cannot explain the need for a particular banking service;
- involvement in the execution of transactions of young people and/or newly established enterprises;
- carrying out transactions using lost documents;
- opening an account which is soon credited as a result of unauthorized debit transactions;
- attempts to withdraw funds on the day of their crediting;
- attempts by a customer to obtain two or more credit cards when it is inconsistent with the nature of his business or its turnover;
- crediting of funds to the card accounts of individuals followed by their withdrawal from ATMs (including third party's);

- execution of transactions that are different from previous transactions of the customer;
- the lack of information about the customer's business activities or the use of online instead of traditional payment systems;
- atypical international transfers that are inconsistent with the customer's business activity.

To identify suspicious financial transactions related to cybercrime, the FIUs may, in addition to the above indicators, also use the following:

- no apparent relationship between the foreign sender of the money and the individual receiving it;
- private remittances to a private person that are indicative of possible commercial activities (e.g. Bitcoins or Web Money exchange services provider, etc.);
- transfer by the customer of funds to another person's bank account using remote access;
- cross-border transactions carried out using remittances or Internet banking;
- transfer of funds to/from remote locations that do not have a direct or obvious connection with the customer's activities or account;
- involvement of a large number of foreign third parties, both individuals and legal entities;
- use of dummy companies;
- intelligence received from foreign FIUs and law enforcement.

4.2. Main Areas of Anti-Cybercrime Activities

In the context of rapid advances in information and computer technology, resulting in the proliferation of cybercrime, the task of cybercrime prevention and combating takes on added urgency.

Prevention of cybercrime is based on activities aimed at reducing the risk of such offences and eliminating the harmful consequences for society and the private sector. An effective cybercrime prevention strategy must combine multiple legal (legislative), technical, organizational and informational activities.

As a first step towards the creation of an effective legal framework for combating cybercrime, it is important to develop the correct conceptual apparatus. The challenge of coming up with the accurate definition of the word "cybercrime" must be approached carefully, and not only because any inaccuracy in its wording can potentially result in a "dead" or poorly enforceable legislative provision. In view of the specific nature of this type of crime, the proposed anti-cybercrime legislation must be drafted based on the specific international instruments (such as

the Council of Europe Convention on Cybercrime), given that achieving success in the fight against cybercrime within the boundaries of single country without international cooperation is no longer possible.

It is important to add institutions issuing prepaid cards and electronic money to the list of institutions that are subject to AML/CFT requirements and compile a list of suspicious transactions for them.

It is necessary to strengthen the responsibility of service providers in order to ensure that they monitor the use of their services and as a means of encouraging them to reduce the risk of illegal use of their services.

Regulatory support for the prevention and counteraction of the legalization of cybercrime proceeds can also be boosted by:

- strengthening accountability for computer and information technology-related crimes;
- introducing compulsory identification for face-to-face contacts with customers who use remote access services or electronic payment systems;
- allowing the use of electronic documents and other electronic data as evidence in investigations into cybercrimes;
- addressing jurisdiction-related issues in the area of online services;
- reducing the number of anonymous payments and transfers of funds;
- introducing mandatory certification for electronic means of payment;
- developing clear mechanisms of interaction between the customer and the bank as well as between the beneficiary's bank and the sender's bank in the event of unauthorized debiting of the customer's account.

Among the technical and organizational anti-cybercrime measures that can be implemented by banks are:

- regular inspection of ATMs for the presence of any illegally installed devices;
- introduction of customer plastic cards with embedded microchip technology for better protection against counterfeiting;
- blacklisting of fraudsters' accounts (identification codes, IP-addresses) to ensure rapid suspension of transactions;
- introduction of two-factor/two-channel authentication requirements;
- use of tokens for storing digital signatures;
- mandatory notification of customers of all transactions carried out on their accounts;
- confirmation of payment over the phone;
- involvement of the customer in the generation of a customer key as a means of preventing any wrongdoing by bank employees;

- the linking of the customer key to the serial number of the hard disk/flash drive/floppy disk makes it impossible to copy the Client-Bank keys or access the customer's page from other computers;
- use of multiple logical rules for typical/atypical/suspicious Client-Bank system payments;
- use by the customer of a dedicated Client-Bank system (Internet banking) computer with customized line filters;
- statistical analysis of traffic (Netflow) for the presence of anomalies;
- introduction of online transaction limits;
- introduction of limits on transactions carried out in high-risk jurisdictions;
- introduction of limits on the frequency of transactions.

It should be noted that much of cybercrime is due to the lack of knowledge among members of the public and customers of financial institutions and their disregard of basic safety rules. Among such factors are:

- limited availability of information on cybercrime;
- poor awareness of the risks posed by the new payment systems and services as well as of the associated money laundering;
- installation and use of unlicensed software (operating systems, antivirus, etc.);
- insecure storage by bank customers of digital signatures and access codes (passwords);
- violation of the basic safety rules for the use of Internet banking and online payment instruments;
- failure to comply with the code (password) and information security policy.

In this regard, a significant role in preventing cybercrime is played by awareness-raising activities dedicated to new risks and threats to information and computer systems.

Other important factors include the secure handling of electronic data which is of considerable economic interest to other companies, implementation of measures aimed at restricting access to it, and the use of licensed, anti-virus and anti-hacking software.

Also essential is the work to improve the legal and regulatory framework for information security, both at the state and at private level. In particular, each public and private company and institution needs to develop and improve its own information security system, as well as to draft internal regulations designed to address the issues of information security and establish liability of employees for non-compliance with them. Access to the information constituting state, banking

and other secrets should only be granted to those employees whose work duties necessitate the use of such information and who are duly authorized to access it. It is also important to exercise proper supervision and control over the observance of the information security guidelines.

CONCLUSIONS

Despite the absence of a universally accepted definition of cybercrime, there is a broad and thorough understanding of its essence, modus operandi as well as risks and threats associated with it. This allows us to develop and implement measures designed to combat this type of crime.

The lack of physical contact with the victim or financial institution employees coupled with anonymity, speed and low cost mean that cybercrimes are very popular among criminals.

Cyberspace has become not only the scene of crime and the source of illegal proceeds, but also the place where these proceeds are laundered. The sheer diversity of cybercrimes coupled with the multitude of money laundering schemes make the task of solving such crimes particularly challenging.

The identified cybercrime proceeds laundering schemes and mechanisms suggest that the movement of funds is carried out using both conventional money transfer methods and more modern mechanisms such as express money orders, electronic payment systems and electronic money.

The illicit funds are then used to purchase prepaid cards to finance online purchases of goods and services, or they are converted into casino chips or electronic money for subsequent transfer to e-wallets and cash withdrawals.

Conversion of funds into cash, on the other hand, remains one of the most common ways of concealing the future destination of illicit income and the areas of its investment, as well as the origin of such funds during their input into the banking system. This allows criminals to maintain anonymity acquired at the stage of the criminal income acquisition also during money laundering.

An effective anti-cybercrime strategy consists of a series of legal, technical, organizational and informational activities, with the role of each of these activities being neither primary nor secondary.

Therefore, the success of any money laundering and crime fighting measures in this area depends on the timely detection of financial transactions possibly linked to the laundering of cybercrime proceeds and the effectiveness of international cooperation, as well as cooperation between the public and private sectors.