The future of e-money laundering in the Republic of Macedonia

Snezana Mojsoska
Faculty of Security,
Department for Social-political and Legal Sciences,
Skopje-University ‘St. Kliment Ohridski’-Bitola,
st. Idrizovo B.B., Republic of Macedonia
Email: mojsoska@gmail.com

Abstract: This paper analyses the statistics and reports dealing with various aspects that link e-money and money laundering, in order to identify the major challenges and possible solutions to the problem of electronic money laundering. Though referred to as electronic money laundering, this does not differ from the classical money laundering. The research in this paper proves that e-money laundering in Macedonia is a matter of a future analysis because at the moment electronic payments are little used, and the internet is poorly used specifically for payments, etc. Macedonia has no regulations that control or prevent e-money laundering. This paper will provide recommendations to improve the prevention of e-money laundering in Macedonia, such as the establishment of appropriate bodies and procedures to operate and control the international e-payment systems, of regulatory authorities to monitor the activities of these systems through the implementation of a framework for user registration and identification, etc.

Keywords: electronic money; e-money; electronic money laundering; positive and negative aspects; regulation; system; software.


Biographical notes: Snezana Mojsoska is Vice Dean for Finance and Assistant Professor at the Faculty of Security of Skopje-University.

1 Introduction

“Electronic commerce will become the 21st century’s mainstream trade and trade form. Electronic payment is the electronic commerce core; it will be the brand-new means of payment that develops in the commercial activity process and the electronic credit foundation. The electronic payment will be the 21st century’s main financial payment pattern.”1 This payment pattern will bring an enormous convenience for the work and lives of people on one hand, and on the other, criminal offenders will inevitably use it to launder money, thus introducing a new challenge to the traditional counter-money-laundering system. For example, in 2003, the world’s biggest network payment company, PayPal, was charged with the provision of conveniences for money laundering, shifting
illegal gambling stake of USD 6,000,000. As an outcome, the PayPal Corporation was imposed a USD 10,000,000 fine.2

Trade via the internet has increased the application of new technologies, and thus increases the demand for new electronic payment methods. However, what is really new is the electronic payment in retail and the use of the internet as a new monetary market. As a result of this, the geography of money is changing.3 Due to the information revolution, a new form of electronic payment has emerged, which soon attracted the attention of the world’s electronic money (e-money) (also known as electronic cash, e-bag, e-currency, digital currency, digital money or digital cash). Money laundering is a complex system which is still developing; new techniques are being used and money launderers are becoming more and more sophisticated. Criminals hide themselves behind complex transactions, which include international transfers, dispersion into smaller amounts or transfers made to the accounts of different persons, changing the shape of money and advice received from banking experts, brokers, investment bankers, accountants, consultants, notaries public and lawyers.4 E-money laundering can be simply defined as using the e-money for the purpose of money laundering.

2 E-money, definition and characteristics

The development of science and technology is followed by an increase in transfers through financial systems. Cyber banking and mobile payments are the new technological progress.

E-money is the greatest technological achievement in the development of e-banking. It represents a substitute for paper money and as such can be used for payment of products and services online, or in the business of banking networks (e.g., SWIFT).5

According to the relevant articles of the 2nd E-Money Directive 2009/110/EC, the definition of e-money or ‘electronic money’ covers the electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions and which is accepted by a natural or legal person other than an electronic money issuer.” “E-money issuer means the entities and institutions benefiting from a waiver and legal persons benefiting from a waiver.”6

E-money is issued by a bank or other financial institution. For this purpose, the user first deposits money in the bank and receives in return e-money for the value of the deposited money. E-money bears identification numbers that are unique (similar to the serial numbers on paper money). Then, using the appropriate user programs, one can withdraw e-money and set the local computer. Thus, marked digital money can be used to purchase certain products (thus, the store where the product is purchased must accept e-money, meaning that it should have a specific infrastructure). A merchant who has received electronic money can later re-use it for any transaction or exchange it for paper money in a bank that operates with e-money.7

One of the most important features when using e-money is that there is no exchange of information for the buyer (same as with paper money). This increases reliability in transactions. This feature of the e-money is a key difference between the e-money and credit and debit cards. Also, e-money can be re-used, i.e., once e-money is received, it can be used for another transaction.8

In general, there are two different types of e-money:
identified e-money

• anonymous e-money.

Identified e-money contains information about the identity of the user (i.e., the person who originally borrowed the money from the bank). Identification enables the bank to follow the money moving through the economy in a similar way as in the use of credit cards.

Anonymous e-cash works in a similar way as the actual paper money. Once anonymous e-money is withdrawn from the account, it cannot be spent without the possibility for monitoring or monitoring of transactions involved. Anonymous e-money will be checked only when the merchant bank deposited turn them into real paper money. However, the bank can only identify the owner of the e-money, or the person to whom the bank initially issued the money.

The process of paying with e-money can be:

• online

• offline.

In an online payment, the transaction involves three parties: a customer, a merchant and a bank. For example, a customer wants to buy a product with e-money. For this purpose, he allocates one part of his e-money and sends it to the merchant. The merchant, however, cannot complete the transaction until he sends the e-notes to the bank so as to check their authenticity. The bank checks the money and, if it had not been spent before, the bank informs the merchant that the transaction is in order. At that point the merchant can charge the product, or close the transaction.

Offline payment can be made directly between the buyer and the merchant, without the bank being involved. However, the authenticity of the money will be checked at the time the merchant wishes to convert the e-money in the bank in the actual paper money. Offline anonymous e-money is most complex form of e-money because of the problem of double spending (the double-spending problem). 9

Money in an electronic transfer may be used by individuals, banks, stock exchanges, brokerage houses, vendors and all other bodies involved in the economic exchange. There are three major e-money transfer systems: electronic funds transfer, chips, and SWIFT and FEDWIRE, which, according to statistics, transfer USD 2 billion a day.

Each electronic transfer uses a different central monitoring system (CEN) of the transaction. The large-scale daily transfers of funds make it impossible to follow the daily transactions and entering schemes.

The reason for the greater prevalence of these products is exactly their great possibility compared to the traditional way of payment. But statistics confirms that the development of e-money is in its initial stage, and cash is still the most important form of payment in retail transactions. The use of e-money depends on two factors. The first one is the network externalities and the double nature of e-money market (application and use). The second factor is the problem of old habits and the psychological momentum which refers to the time required for the development and use of e-money. Quite contrary to some expectations, cash has not yet replaced any form of electronic payment. This project answers why the use of e-money has not started to live. One reason is precisely the fact that e-money is very sophisticated form of payment that it something requires investments in new technology, as well as the development of new experiences between
users. Practice shows two additional reasons. The first reason is network externalities, and the second one is innovations. The number of users has to reach a certain critical mass so as the use can become rewarding for all participants in the system. The other reason is the persistence of habits in the use of traditional forms of payment, such as checks and cash payment.

According to the Macedonian legislation pertaining to payments, E-money is the monetary value represented as a demand issuer, which is: located on an electronic device; issued on the basis of admission of cash in an amount no less than the value of the e-money issued, and accepted as means of payment by persons who are not the publisher of that money.

1 An issuer of e-money can only be:
   • a bank based in the Republic of Macedonia which has received prior approval by the Governor of the National Bank to issue electronic money
   • a branch of a bank based in a Member State of the European Union, in compliance with the Law on Banks
   • a branch of a foreign bank that has received a license from the Governor of the National Bank to found an office and operate, in compliance with the Law on Banks
   • a company issuing electronic money, which has received a license from the Governor of the National Bank to found and office and operate, in compliance with this Law.

2 The receipt of cash for the issuance of electronic money means receiving deposits or other repayable sources of funds in terms of provisions of the Law on Banks, when the electronic money is issued immediately at receipt of funds. (1) The electronic money issued on the basis of an electronic money issuance agreement made between the electronic money issuer and an individual – the owner of the electronic money (hereinafter: the owner).

3 Based on the agreement and upon payment of specified amount of cash, the owner shall be issued electronic money which he can use to make payments in the amount of the coverage for the issued electronic money.

4 The holder of the issued electronic money pays a provision to the publisher. In electronic money payment commission and other costs are free of charge.

5 Covered electronic money issued in the amount of paid funds, less the amount of executed payments and collected commissions.

The rapid development of electronic cash leads to its increased importance. However, we can say that the initial predictions that this would cause the paper money to disappear did not materialise; even in the developed countries paper money is the most common means of payment, especially for small payments.11

3 E-money laundering

The process of globalisation, new technological advances and greater mobility of people and resources across national borders, contributed for the transnational crime to emerge
in new forms of so-called non-traditional forms of crime, one of which is the e-money laundering or cyber-laundering.

The appearance of cyber-laundering and e-money laundering started in the 1990s, simultaneously with the development of the internet. The term cyber-laundering includes money laundering via the internet, electronic banking (e-banking) and e-money/cash. In order to enter into the substance of the term and potential benefits of laundering money through the internet, first it is necessary to define e-money and its application.

The very short time required to complete the electronic transfer of funds has helped conceal and move the revenues from illegal, criminal activities. Modern information technology makes it easier to hide the traces of the criminal origin and destination of the transfer of these funds. In this way, the dirty money comes in regular, legal flows.

As the physical world of money laundering began to erode, the tendency to use electronic transfers to avoid detection gained a loyal following. Electronic transfers of funds are known as wire transfers.\(^{12}\) Wire transfer systems allow criminal organisations, as well as legitimate businesses and individual banking customers, to enjoy a swift and nearly risk free conduit for moving money between countries.\(^ {13}\) Considering that an estimated 700,000 wire transfers occur daily in the USA, moving well over USD 2 trillion, illicit wire transfers are easily hidden.\(^ {14}\) Federal agencies estimate that as much as USD 300 billion is laundered annually, worldwide.\(^ {15}\) As the mountain of stored, computerised information regarding these transfers multiplies, the ability to successfully launder increases to as the workload of investigators also rises.\(^ {16}\)

### 3.1 Technological advantages in e-money laundering

E-money laundering involves three steps in turning dirty money into clean money, same as in classical money laundering:

- **positioning**
- **layering**
- **integration.**

#### 3.1.1 Positioning

As previously noted, e-money is the money that was presented digitally and can be changed via the internet or smart cards without the need for intermediaries. One of the key benefits is anonymity. Income from criminal activities in the form of e-money, for example, can be used to purchase foreign currencies and expensive goods. E-money can also be used for disposing of dirty money without having to smuggle cash and personal transactions.

#### 3.1.2 Layering

Layering involves changing the illicit origin of the resources or separation of illegal revenues from their illegal source. Layering is done by implementing a series of financial transactions so as to make their size, frequency and complexity resemble the legal financial transactions. This may involve the transfer of money through a series of offshore companies or the purchase of goods for resale. In this step, the internet is found
most helpful. As in most of the online bank account opening procedures, this does not require personal contact or an existing traditional bank account, and users do not even need to give real personal information: a money launderer may so easily open accounts under false names, which do not relate to him. Money launderer can control transactions through computers by currently transferable money from one account to another, and thus create long audit trail in a very short period of time. Transfers can be made through multiple jurisdictions, making it difficult for single authorities to track it.

With the internet, there is the additional problem of the jurisdiction where the transaction is performed: whether this should be the location of the pressure washer, or that of the server where the bank accounts are. For the French Banking Commission, the transaction is carried out in the place where the account is held.

Layering is even easier if the money can be transferred between banks that do business with e-money. It is important to note that anonymity can completely erase a clue to the real illegal sources.

3.1.3 Integration

The last step is refined to fit the illicit funds into the economy and present it as obtained from a legitimate source. In this step counterfeit accounts are used for purchases of goods. The owner of the money can use a company provided by the internet service provider (ISP) to present that services are provided in exchange for the money that has gone through a process of disintegration. For example, laundered money may be available in the accounts of fictitious or non-existent person company.

Payments could be made from that account to an account provided by the ISP company that services hosting of internet to a casino, but the service would never be delivered; it does not get to the account of the fictional company. Payments are shown as profit of account holders in the ISP company and the money from the owner is shown as a legitimate – profit of ISP company. This kind of integration of monetary fund has wider use than traditional provision of goods and services where, in order to legitimise counterfeit invoices, one must use many documents as evidence of delivery of goods and the purchase of raw materials. Transferred money from foreign banks can, too, cause suspicion when it comes to fictional companies that engaged in the production or sale.

3.2 Suspicious transaction reports

The advantage of the ‘electronic money’ laundering for criminals is much larger than the mere elimination or reduction of the accounting trace. Intermediaries may, depending on regulatory requirements or jurisdiction, have an obligation to report any suspicious transaction. These applications can result in an investigation and ultimately prosecute money launderers. If the washer can reduce risk report suspicious transactions, he may also reduce the chances for the surveillance organs to detect him, and that is exactly where the internet plays a major role. Banks and other companies are compelling online businesses through lower overhead costs. Online banks and e-commerce companies can thus handle much larger number of transactions per account, but by traditional methods. This fact further complicates the tracking of suspicious transactions, even with the use of monitoring software. Those transactions are realised without human intervention, removing another potential source application. Anonymity of the online transactions also reduces the risk of application transactions.
Theoretically, depositing large sums of money in foreign accounts by family members of a statesman would arouse more suspicion than depositing by an anonymous cyber customer. The most common reasons for application transactions can be associated with money laundering in the geographic native resources. If the origin of the funds can be covered, one of the key indicators of money laundering can be removed.

Choosing an electronic payment system for illegal activities, such as money laundering or terrorist financing, depends on many factors, for example, the duration of the operation, the amount of money to be transferred, the international or local character of the transfer and, furthermore, it also depends on such individual preferences of the money launderers or smugglers as their attitude to new technologies, risk aversion to electronic payment methods, and many others. Therefore, an electronic payment system cannot be analysed by means of a universal pattern or matrix containing specific features, but rather intuitively and considering the definition of money laundering (concealing or disguising the origin, location, use, nature of assets, etc.). Hence, a number of payment systems were selected for the analysis, ones that possess such characteristics that make it possible to carry out international money transfers with them in a convenient, fast, and flexible way, through anonymous accounts.17

4 Money laundering regulation in the Republic of Macedonia

The legal framework regulating the problem of money laundering in the Republic of Macedonia was completed with the adoption of the Law on Prevention of Money Laundering (the Official Gazette of the Republic of Macedonia No. 70/01 of 5 September 2001), which was adopted at the session of the Parliament held on 29 August 2001, and entered into force on 13 September 2001. With this law, the provisions contained in 35 articles define the measures and actions to detect and prevent money laundering, as well as the organisation and control of their application. During the two-year implementation of this law, certain deficiencies and non-compliances with international regulations were identified. As a result, in 2004 the Law on Prevention of Money Laundering and Proceeds of Crime was adopted (the Official Gazette of the Republic of Macedonia No. 46/04 of 20 July 2004) in line with international regulations. This law established the measures and actions to detect and prevent money laundering and terrorist financing, as well as the organisation and control of their application. The amendments to the Criminal Code (the Official Gazette No. 37/96, 80/99, 4/02, 43/03 and 19/04), align the Article 273 relating to money laundering and other criminal proceeds with international regulations.

The law criminalises all acts of placing into circulation, receiving, downloading, converting, layering, or transmitting of money, and selling, buying, receiving in pledge or other circulation of property or items whereby hiding their true source, location, movement or ownership.

For the purpose of adjustment to the recommendations by the EU, the legislature prepared a new law on prevention of money laundering and other criminal proceeds and financing of terrorism. In early 2008, the Parliament adopted the Law on Prevention of Money Laundering and Proceeds of Crime and Terrorist Financing (the Official Gazette of the Republic of
Macedonia No. 04/08) (hereinafter the Law). The law is largely harmonised with the provisions of:

The 2005 Warsaw Convention – convention on laundering, seeking, seizure and confiscation of proceeds obtained by terrorist financing.

The Third EU Directive on prevention of the use of financial systems for the purpose of money laundering and terrorist financing and the FATF 40 recommendations and nine special recommendations on terrorist financing prevention. This law established comprehensive measures to prevent money laundering and financing of terrorism that debtor entities are required to implement. These measures include the implementation of the client analysis, complex and dynamic process aimed at better understanding the client. The law clearly provided for cases where the entities may implement the measures of simplified analysis, and cases when such an analysis should be enhanced. The enhanced measures are applied when the risk of money laundering is higher, i.e., in three different situations: when the client is not present for identification purposes, when banks establish correspondent banking relationships, and when banks establish business relationship with a politically exposed person. In order to better meet its obligations, the law imposes an obligation for the debtor entities, within their internal organisation, to establish special departments working on the implementation of this law and its protection system.

Also, the law prescribes a mechanism to monitor and control the implementation of measures for the prevention of money laundering and financing of terrorism. For the purpose of strengthening the surveillance system, the Office for Prevention of Money Laundering and Terrorist Financing (hereinafter the Office) may implement its authorities independently or in cooperation with the National Bank of the Republic of Macedonia, the Public Revenue Office, the Securities and Exchange Commission, the Insurance Supervision Agency and the Capital Pension Insurance Agency to supervise the debtor entities. In performing its supervision, the Office exerts preventive influence on the subjects, in order to provide better organisation in the implementation of measures and actions that reduce or prevent the risk of transactions and other acts of money laundering and financing of terrorism.

Based on the recommendations by the Third Evaluation Moneyval Committee and based on the shortcomings identified in the practical application, the need was identified to amend the Law on Prevention of Money Laundering and Proceeds of Crime and Terrorist Financing in order to achieve full compliance with the new EU directives and regulations.

These amendments to the law were prepared by a working group consisting of employees of the Department. Also, the preparation included experts from the EU, engaged in the framework of the Twinning Project and experts from the TAIEX program.

5 Money laundering in Macedonia

The starting point for explanation of e-money laundering in Macedonia is the use of e-money and the internet for payments or e-trade. The development of internet trade in Macedonia is on a very low level. If we consider the reports from the National Bank of the Republic of Macedonia we can see that Macedonia is still a cash society. In
Macedonia there are already models of electronic commerce that are applicable on a small scale with no defined requirements for safety and security for the users. Online shopping by credit card is used since 2007, but there are also a significant number of companies that do not use e-commerce or e-payments. The number of companies that sell via the internet or by electronic means was about 35 and these include companies for computer equipment, pharmaceutical products, and books. According to business claims, banks are the biggest problem for the underdevelopment of electronic commerce, because they want a portion of their earnings, and they want to charge large commissions. In Macedonia it has been estimated that e-commerce through e-banking reaches around EUR 10,000, and according to the statistics of the National Bank of the Republic of Macedonia only 22,819 companies deal with e-commerce. In other words, e-trade is not a challenge for the banks in our country. Although everywhere else in the world it is the banks who are the drivers of economy, in our country this is not the case. However considered, the problem is not in the authorities, but in the banking industry which provides no better offer for the institutions. Banks want bigger profits and higher commissions that cover greater part of a company’s profit. The development of electronic commerce should encourage the banks to enable the companies have their own online stores, and methods for online verification of credit cards issued by them, thereby enabling confirmation of the validity of the transaction. However, it is the banks that hinder the implementation the most. In the Republic of Macedonia, since the end of 2009 onwards, the number of e-banking users has increased and people are more informed about new products, they can verify the status of accounts in banks, they can perform various types of transactions, etc.

If we consider Tables 1, 2 and 3, we can see that e-money laundering is but a future for Macedonia. The use of credit cards as a means of electronic money is equal to 0 denars, the number of transactions in e-money also equals 0, and the value of transactions with e-money is 0 denars. When the Law on the Payment System in Macedonia was amended, the use of credit cards was on very low level. People did not have the habit of using credit cards. Ten years later, the use of cards instead of cash started to grow. Today, according to the statistical reports by the National Bank of the Republic of Macedonia, 76% of the people in Macedonia are using debit cards, 79% of the transactions are realised by way of debit cards, and the value of those transactions is about 86%.

<table>
<thead>
<tr>
<th>Table 1</th>
<th>Types of cards used in Macedonia in 2012</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Type of cards</th>
<th>In thousands</th>
<th>In %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>1,507,142</td>
<td>100</td>
</tr>
<tr>
<td>Cash cards</td>
<td>54,765</td>
<td>3.63</td>
</tr>
<tr>
<td>Debit cards</td>
<td>1,156,562</td>
<td>76.74</td>
</tr>
<tr>
<td>Credit cards</td>
<td>295,815</td>
<td>19.63</td>
</tr>
<tr>
<td>E-money cards</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Combined cards</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Source: National Bank of Republic of Macedonia, author’s calculations
Table 2  Volume of realised transactions in Macedonia in 2012

<table>
<thead>
<tr>
<th>Volume of realised transactions</th>
<th>In thousands</th>
<th>In %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>3,611,166</td>
<td>100</td>
</tr>
<tr>
<td>Cash transactions</td>
<td>65,861</td>
<td>1.82</td>
</tr>
<tr>
<td>Debit transactions</td>
<td>2,861,605</td>
<td>79.24</td>
</tr>
<tr>
<td>Credit transactions</td>
<td>683,700</td>
<td>18.93</td>
</tr>
<tr>
<td>E-money transactions</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Combined transactions</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Source: National Bank of Republic of Macedonia, author’s calculations

Table 3  Value of realised transaction in Macedonia in 2012

<table>
<thead>
<tr>
<th>Value of transaction</th>
<th>In MKD</th>
<th>In %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cash transactions</td>
<td>284,153,763.00</td>
<td>2.53</td>
</tr>
<tr>
<td>Debit transactions</td>
<td>9,718,153,914.00</td>
<td>86.64</td>
</tr>
<tr>
<td>Credit transactions</td>
<td>1,214,533,910.50</td>
<td>10.83</td>
</tr>
<tr>
<td>E-money transactions</td>
<td>0.00</td>
<td></td>
</tr>
<tr>
<td>Combined transactions</td>
<td>0.00</td>
<td></td>
</tr>
</tbody>
</table>

Source: National Bank of Republic of Macedonia, author’s calculations

Another issue relating to the e-money laundering in addition to using e-money is the use of the internet in Macedonia (Tables 4, 5 and 6).

Table 4  Use of the internet in first quarter, by sex and age (in %) in Macedonia in 2012

<table>
<thead>
<tr>
<th>Total</th>
<th>Sex</th>
<th>Age groups</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Male</td>
<td>Female</td>
</tr>
</tbody>
</table>
| 11.2  | 10.6| 11.8       | 5.7   | 13.7  | 11.1  | Services related to travel and accommodation
| 4.7   | 5.9 | 3.3        | 5.2   | 4.3   | 5.4   | Sales of goods or services, e.g., via auctions
| 13.6  | 14.1| 13.0       | 5.0   | 17.1  | 16.6  | Internet banking

Source: State Statistical Office

Table 5  Individuals who have ordered/bought goods or services for private purposes over the internet in Macedonia in 2012 (in %)

<table>
<thead>
<tr>
<th>In %</th>
<th>Buying or ordering of goods or services by country of origin/residence of the seller</th>
</tr>
</thead>
<tbody>
<tr>
<td>54.8</td>
<td>National sellers</td>
</tr>
<tr>
<td>36.2</td>
<td>Sellers from EU countries</td>
</tr>
<tr>
<td>24.9</td>
<td>Sellers from other parts of the world</td>
</tr>
<tr>
<td>5.3</td>
<td>Sellers whose country of origin is unknown</td>
</tr>
</tbody>
</table>

Source: State Statistical Office
Table 6   The use of ICT by activities in Macedonia in 2012 in %

<table>
<thead>
<tr>
<th>Activity according to the National Classification of Activities</th>
<th>Division</th>
<th>Division</th>
<th>Division</th>
<th>Division</th>
<th>Class</th>
<th>Group/class</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturing; electricity, water supply</td>
<td>84.2</td>
<td>88.8</td>
<td>91.1</td>
<td>98.0</td>
<td>87.5</td>
<td>100.0</td>
</tr>
<tr>
<td>Construction</td>
<td>4.8</td>
<td>4.8</td>
<td>7.5</td>
<td>17.4</td>
<td>11.7</td>
<td>24.3</td>
</tr>
<tr>
<td>Trade</td>
<td>16.7</td>
<td>24.3</td>
<td>16.7</td>
<td>24.3</td>
<td>16.7</td>
<td>24.3</td>
</tr>
<tr>
<td>Information and communication</td>
<td>51.1</td>
<td>51.1</td>
<td>51.1</td>
<td>51.1</td>
<td>51.1</td>
<td>51.1</td>
</tr>
<tr>
<td>Other non-financial activities</td>
<td>51.1</td>
<td>51.1</td>
<td>51.1</td>
<td>51.1</td>
<td>51.1</td>
<td>51.1</td>
</tr>
<tr>
<td>Financial activities</td>
<td>51.1</td>
<td>51.1</td>
<td>51.1</td>
<td>51.1</td>
<td>51.1</td>
<td>51.1</td>
</tr>
<tr>
<td>ICT sector</td>
<td>100.0</td>
<td>100.0</td>
<td>100.0</td>
<td>100.0</td>
<td>100.0</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Source: State Statistical Office

In the first quarter of 2010, 46.1% of households had internet access from home. According to the State Statistical Office, in the first quarter of 2010, the share of households with internet access has been increased by 4.3% points compared to the same period in 2009. The share of households with broadband in the total number of households increased from 33.8% in 2009 to 37.2% in 2010, while their share in the number of households with internet access is on the same level in both comparative periods (about 81%).

However, merely 9.3% of all internet users in Macedonia in first quarter of 2010, are using internet connection for e-banking. But 13.6 % (office, 2012) of all the internet users in Macedonia in the first quarter of 2012 were using the internet connection for e-banking.

In 2011, banks began to work on harmonisation of their operations with applicable regulations that should provide protection and eliminate all the consequences that may arise as a result of the failure to observe or incorrectly apply the applicable regulations. In 2011, this goal was to be accomplished by taking the following actions:

- permanent monitoring of the regulations governing the operations of the banks and activities necessary to be undertaken on that basis
- monitoring the compliance of a bank’s internal regulations with legal and other external regulation
- giving opinions about organisational units of a bank in relation to the consistent compliance and enforcement of regulations
- identifying and monitoring of the risks of non-compliance of a bank with the regulations
- proposing corrective measures
- constant and regular reporting to the Board of Directors, Supervisory Board and other bodies on the condition
- training of employees in relation to the application of the regulations
activities relating to the prevention of money laundering, and financial
synchronisation and alignment of a bank to the announced new changes:

a Law on Prevention of Money Laundering and Proceeds of Crime and Financing
of Terrorism

b Rulebook on the Characteristics of Software for Automatic Processing of Data
on the Prevention of Money Laundering and Terrorist Financing

c other national and international regulations in the field of PP/FT

harmonisation of internal regulations by:

a reviewing a bank’s program for the prevention of money laundering and
financing of terrorism in accordance with the prescribed requirement in existing
law on WFP/FT

b active participation in the revision of the internal working guidelines of the
business areas with a full range of procedures required to implement measures
and actions to prevent fire/FT

c identifying and monitoring the risks of non-compliance of a bank’s operations
with the SPP/FT regulations and a bank’s exposure to operational risk: money
laundering and financing of terrorism

training of employees in the SPP/FT department and the bank to operate a new level
software solution pursuant to the SPP/FT

regularly informing the bank’s management and administrative bodies about the
established conditions and giving proposal for corrective measures, etc.

according to Article 29 of the Law, the Office receives the following information:

a banks; data on all loans that exceed the legally defined limit of the MKD
equivalent of EUR 15,000

b notaries; data on compiled notarial acts authenticating private documents and
notarising signatures on contracts whereby property is acquired the worth of
which exceeds the MKD equivalent of EUR 15,000

data from insurance companies for insurance policies concluded the value of which
exceeds the MKD equivalent of EUR 15,000

from legal entities and individuals whose businesses deal with the purchase and sale
of vehicles data on contracts for the purchase of new vehicles in the amount that
exceeds EUR 15,000.

During 2011, the Department has identified a total of 33,921 entities who, under the Law,
are obliged to undertake measures and actions to prevent money laundering and terrorist
financing. The following table gives a representation of the entities by type and number
(Table 7). In Macedonia, there are insufficient data about money laundering and STR: the
Financial Intelligence Directorate lacks data on for suspicious transactions using.
Another important issue to consider when analysing e-money laundering in Macedonia is the position of this type of crime in the crime statistics by the State Statistical Office. According to the 2011 statistics, seven persons were charged for money laundering and six persons were found convicted. Macedonian prosecutors have no understanding for the criminal act of money laundering.

<table>
<thead>
<tr>
<th>Charged</th>
<th>Female</th>
<th>Guilty</th>
<th>Stopped</th>
<th>Prison</th>
<th>Fee</th>
<th>Alternative measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>1</td>
<td>6</td>
<td>1</td>
<td>2</td>
<td>14</td>
<td>4</td>
</tr>
</tbody>
</table>

It is very difficult to prove money laundering because very often it is confused with tax evasion. Also, before the introduction of the new I2 system of today, the old software could not make distinction between real STR and the really suspicious transactions were sometimes investigated for years.

6 Recommendations

Regardless of the fact that changes have been made to Article 4 of the Law on Money Laundering, entities shall be bound to pay special attention to the threat of money laundering and financing of terrorism arising from the use of new technologies or developing technologies and to prevent their use for money laundering or financing of terrorism.

There is an immediate need to supplement the law with a wider consideration of e-money laundering. This should be regulated by a new, more precise article that will clearly use the phrases “protection and measure against risks from new technological advances that allow for anonymity of parties” (e.g., e-banking, the use of ATMs, telephone banking, etc.), and the part on taxpayers who are required to establish procedures and take additional measures to eliminate risks and prevent abuses from new technological developments for the purpose of money laundering or financing of terrorism should also be regulated. The amendments to the Law on E-Trade should also regulate the protection and notification of cases where e-money laundering is detected.

In the course of writing of this paper, the Macedonian Government started a project worth EUR 1,730,000 that will in a two-year’s time establish, following the Norwegian example and for the purposes of the Macedonian Financial Intelligence Department, an electronic connection to all parties involved in the fight against money laundering and
terrorism financing. This new system will be efficient tool for rapid analysis and should increase the efficiency of data analysis and generating reports. A software solution will be developed for the electronic exchange of information between the Ministry of Interior, the Public Prosecutor’s Office, the Financial Police, the Customs and the Public Revenue Office. The first set of planned activities relates to the cooperation and compliance of entities and institutions in data submission and information exchange. The project will develop a modern ‘web application’ with a complete design and functionality for use by consumers, banks, exchange offices, fast money transfer, notaries and all other entities, for the purpose of a faster, safer and more efficient data delivery. The second component will be working on the implementation of automatic data processing in the Office, advanced case management, visual analysis, the flow of information, intelligent packages and intelligence reports. The system should be operational within 14 months, followed by a one-year test period. For the project purposes, the Macedonian state will provide funding for hardware equipment, facilities, and staff salaries etc. The application of this system will significantly improve the communication and reduce the time for analysis of the cases that are the subject of this work. Such software is already used by some developed countries and is known as I2 software.

7 Conclusions

The development of the internet has offered the possibility to leave the old traditional way of communication and to develop a new electronic way of information exchange, known as electronic.

Electronic money is the greatest technological achievement in the development of e-banking. It represents a substitute for paper money and as such can be used for payment of products and services online, or in the business of banking networks. Advances in information and communication technology allow for the development of new forms of electronic payment, both in the real world (card products) and in the virtual world (software products). The process of globalisation, technological advances and greater mobility of people and resources across national borders, contributed for the transnational crime to create a new form of a so-called non-traditional forms of security, one of which is the e-money laundering or cyber-laundering.

The advantage of the ‘electronic money’ laundering for criminals is much bigger than the mere elimination or reduction of the accounting trace. Electronic money laundering involves three steps in turning dirty money into clean money, which are the same as in the classical money laundering (positioning, layering and integration).

The starting point for the explanation of e-money laundering in the Republic of Macedonia is the use of electronic money and the internet for payments or e-trade. The level of development of internet trade in Macedonia is very low. There is still no use of electronic money or electronic payments in Macedonia. Even the e-banking is seldom used.

To put it simply, in Macedonia we cannot talk about any use of e-money laundering. There is an urgent need to supplement the law with wider consideration of e-money laundering. It should be regulated by a new, more precise article that will use the phrase “protection and measures of risks against new technological advances that allow for anonymity of parties” (e.g., e-banking, the use of ATMs, telephone banking, etc.), and the part on taxpayers who are required to establish procedures and take additional
measures to eliminate risks and prevent abuses from new technological developments for the purpose of money laundering or financing of terrorism should also be regulated. The amendments in the Law on E-Trade should also regulate the protection and notification of detection and reporting of e-money laundering. It is necessary to establish appropriate bodies and procedures for operation and control of international e-payments systems, regulatory authorities to monitor the activities of these systems through the implementation of a framework for user registration and identification, etc.

Notes
1 In December 1996, United Nation’s Commission on International Trade develop and adopt ‘Electronic commerce Demonstration Law’.
10 Banking Law of Republic of Macedonia (Official Gazette of RM No. 67/07, 90/09 and 67/10).
12 A wire transfer is simply the transfer of funds by electronic messages between banks. U.C.C. Article 4A Prefatory Note (1991) defines a wire transfer as “a series of transactions, beginning with the originator’s payment order, made for the purpose of making payment to the beneficiary of the order.”
13 There are three major electronic funds transfer systems:
   1 SWIFT: the Society for Worldwide Interbank Financial Telecommunication, is a Belgian-based association of banks that provides the communications network for a large number of international funds transfers, as well as intra-country transfers within the USA.
   2 CHIPS: the Clearing House Interbank Payments System, is a funds settlement system operated by the New York Clearing House.
   3 Fedwire: the funds transfer system operated exclusively by the Federal Reserve System.
15 Ibid.
16 In 1994, the number of CTRs was approximately 10,765,000. The IRS, who is in charge of checking on suspicious transactions, does not have enough investigators to consistently check these reports. However, FinCen, in its desire to keep the IRS up to speed, is currently attempting to process every CTR by means of its artificial intelligence system. See Id. at 6–7.

Note: Money laundering is also regulated in the provisions of the following laws: the Law on Criminal Procedure (Official Gazette of RM No. 15/97, 44/02 and 74/04), Law on Financial Police.