Identity Theft and Internet Banking Protection

Chief Assist. Prof. Silvia Parusheva, Ph.D.

Summary: This article is dealing with one of the pressing problems about Internet banking until now – users' identity theft and drawing money from their accounts due to gaps and negligence in the ways of their verification by the banks. Here are given the opportunities for its solving by realization of projects for multifactor authentication of bank customers in accordance with the levels of risk. By comparing the practice used in the developed countries (mainly after the British example) and the same in Bulgaria summaries have been made and recommendations given to enhance the security of the online banking systems.

Key words: identity theft, phishing, multifactor authentication, bank chip cards, tokens.

JEL: C88, G21.

Electronic financial services expand their presence in all sectors of the financial markets – bank, insurance, trade with securities and currency exchange. Because of their significant advantages, their b popularity has been gradually growing among customers. Consumer confidence in them, however, has been put to a serious test during the last few years because of the growing number of identity theft cases in more and more countries in the world.

Identity theft ("**Identity theft**") can be defined as abuse of personal data or documents with the purpose of using somebody else's identity and performing illegal acts like, for example, abuse of the person's bank account or other securities. Popular types of bank operations like debit and credit card transactions on automated teller machines (ATM[1]), POS[2] devices, or the usage of bank cards for electronic trade payments in the Internet, are among the most affected by illegal practices. An alarming trend lately is that the typical online banking – performing bank operations on customer accounts in the Internet environment – is becoming a target for attacks.

It is accepted to label network-based fraud by the term "**phishing**". It represents an identity theft using *false e-mail* addresses and *false Internet sites* inciting naïve customers to reveal personal information like user names (user ID), passwords, credit cards numbers, PIN codes, addresses, bank account numbers, etc. Most often, the false e-mail addresses are similar to the e-mail addresses of the banks in question and they contain a link re-directing the user to false Web sites, identical with the bank's site.

Another identity theft variety is related to the use of different types of criminal software, performing actions without the knowledge of the user. It includes "Trojan horse" type viruses (Trojans), worms or programs of the "keylogger" type, which self-install on the computer of the customer without his knowledge. They capture

[1] Automated Teller Machine
[2] Point-of-sale

and record passwords entered by the keyboard, as well as other personal and financial data, and send them to phishing servers. Such criminal acts are labeled by the term "**pharming**". Some of these virus technologies attack the address bar of the Internet browser and are more advanced than phishing [9]. When customers enter a valid URL[3] address, instead of the valid sites they are re-directed to criminal Web sites. The re-addressing to fraudulent sites is realized through infecting the local Domain Name Server (DNS). It includes a change of the specific domain record, which results in directing the customer to a site different from the desired (expected) one.

Cases of identity theft are most widespread in the USA, Canada, Australia, and South Africa. In the European Union, the problem is most acute in Great Britain. The use of phishing attacks started a few years ago. The first registered attacks were in March 2003. Since then, the threats based on viruses and worms have been quickly growing, and the application of "Trojan horses" for illegal use of personal information, as a relatively new phenomenon, was registered in the criminal practice after the middle of 2004 [6].

According to latest data in *the USA* for 2005, about 109 mln. computer users were subject to phishing e-mail attacks, which is a 100 % growth compared to 2004. The average value of fraud has increased five times in comparison to 2004 [3]. According to Garthner[4], for one year (from the middle of 2005 to the middle of 2006), 15 mln. Americans became victims of fraud related to identity theft, which represents growth by approximately 50 % with respect to the reported 9.9 mln. deceived customers in 2003 [8].

The commercial banks association (APACS[5]) in *Great Britain* reported that losses from false transactions in online banking in the first half of 2006 had increased by 55 % with respect to the same period of the previous year, reaching 22.5 mln. pounds. For all 2006, fraud as a result of Internet banking demonstrated 44 % growth, mainly because of the increased phishing attacks. According to CIFAS[6] data, identity thefts have grown by 500 % since 2000. According to the Federal Criminal Office in *Germany*, 3500 phishing attacks were carried out in 2006.

Data have been published about serious growth, observed in the use of malicious software of the "spyware" type. As stated in a report, presented at a European Commission Conference, the number of "keylogger" programs increased approximately 3 times during the period May 2005 – May 2006 [3]. Furthermore, the number of "keylogger distribution sites" – Web sites stealing passwords and counting on malicious codes to receive personal financial information, increased by more than 400 % for the same period of time.

Although incomplete, the data mentioned above show a general trend towards significant increase in the abuse of personal data in online banking. This fact threatens to a great extent the activity of the bank institutions. It is possible to observe a falling trend in the number of users of Web-based bank services with all resulting negative consequences.

The solution of the problem may be sought in several directions: secure authentication of bank customers, additional legal guarantees, informing customers, increasing their vigilance and responsibility, etc.

The present article explores some possibilities for application of modern information technologies

[3] Universal Resource Locator
[4] http://www.id-protect.co.uk/fraud_statistics.php - Garthner Study 2007
[5] Association for Payment Clearing Services
[6] Association in Great Britain, created for prevention of financial fraud.

to ensure reliable authentication of Internet banking users.

Ways of secure user authentication in online banking

Important aspects of Web banking security are ensuring protection of the data transfer between the customer's computer and the bank servers, as well as reliable user authentication.

The problem of authentication is related to the proof of authenticity of the customer, or the confirmation of his true identity. Banks have difficulties as to the way of establishing for sure whether online bank operations are ordered by the authentic customer or by a person, who has misappropriated his personal data through spy software.

Mainly cryptographic techniques are used for protection of the data transfer between the bank and the customer in Internet banking. The most widely applied protocol is "Secure Socket Layer" (SSL) is. It encrypts the data, ensuring in this way their protection during Internet transfers. However, SSL does not have the tools of authentication of the customer, which makes necessary the use of additional techniques.

The "Secure Electronic Transaction" protocol (SET) provides good opportunities, allowing both data encryption and reliable authentication of users to the system server. Unfortunately, the great sophistication and high installation and exploitation costs are the reason that the protocol is not widely recognized and applied.

Taking into account that in bank practice the protocol SSL is widely applied, there is an obvious necessity of additional and reliable means to confirm the identity of the customer.

There are three main ways of authentication – something the customer *knows* (*knowledge* – password, PIN); something the customer *owns* (*possession* – bank chip card, hardware devices, the so called "secure tokens"); something the customer *represents* – specific physical, i.e. biometrical characteristic (fingerprint, iris or retina scan, etc.) [1, p. 48].

Each of the three ways has its advantages and disadvantages, the disadvantages being quite conscientiously used for premeditated criminal intrusion and security breaks. This is the reason why the financial industry is trying to find a combination of different ways of user authentication and, as a result, **multifactor authentication** is being already applied in practice – in its different varieties – 2-factor, 3-factor, etc.

2-Factor authentication includes, in addition to user names and passwords (ID/password), i.e. "something the customer knows", the application of one more factor, most often of the type "something the customer owns", for example, a **hardware security device**, called "**token**". In general, 3 types of devices are used – *USB tokens*, *smart cards and smart cards readers, and password-generating tokens* [4, p. 8].

The USB token device is inserted in the USB port of the customer's computer so there is no need for special hardware installation. After the automatic recognition of the token, the customer must enter a password as a second authentication factor, in order to gain access to the computer system. Moreover, this device has features, which allow the storage of digital certificates that can be used in the ß PKI[7] infrastructure.

A smart card contains a microprocessor, able to store and process data. The microprocessor

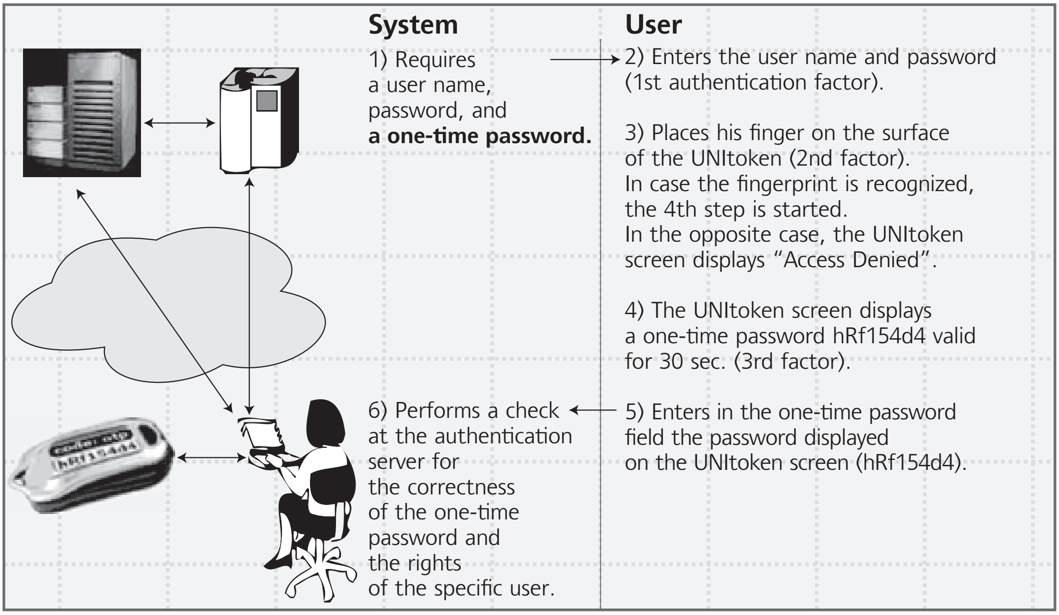
[7] Public Key Infrastructure

allows software developers to use a stronger authentication scheme. The application of smart card requires a respective reader connected to the client computer. If a smart card is recognized as valid (first factor), the customer must enter a password (second factor) in order to complete the authentication process.

Both devices are difficult to reproduce or forge and, in this way, they are a more secure combination for sensitive data storage. The main shortcoming of smart cards as an authentication tool is that they require the installation of a hardware reader and accompanying software drivers on the client computer. The advantage of the USB token device is the easier exploitation as there is no need for installation of special hardware.

The passwords-generating token creates unique passwords known as one-time passwords each time it is used. They are presented on the small screen of the token and their life duration is between 30 and 60 seconds. The customer enters first a user name and the normal password (first factor), followed by the one-time password generated by the token (second factor). This type of devices are much more secure because of the time limits of validity, as well as for the fact that there is no physical contact between the device and the computer (the token is fed by batteries). The accidental, unpredictable, and unique character, as well as the short duration of passwords, guarantees that their possible capturing by "keylogger" programs does not present any threat to users.

Another version of an authentication sign in 2-factor authentication is **the method of "shared secrets"**. The shared secrets ("something the customer knows") are information elements, known or shared by both sides – the customer and the authentication



System

1) Requires a user name, password, and **a one-time password.**

6) Performs a check at the authentication server for the correctness of the one-time password and the rights of the specific user.

User

2) Enters the user name and password (1st authentication factor).

3) Places his finger on the surface of the UNItoken (2nd factor). In case the fingerprint is recognized, the 4th step is started. In the opposite case, the UNItoken screen displays "Access Denied".

4) The UNItoken screen displays a one-time password hRf154d4 valid for 30 sec. (3rd factor).

5) Enters in the one-time password field the password displayed on the UNItoken screen (hRf154d4).

Figure 1. Example of a 3-factor authentication procedure [10]

institution. Latest developments of the shared secrets technique include answers to *questions* requiring specific user knowledge or a *picture* selected by the user from a series of presented pictures. The security of the shared secrets methods can be increased by periodical change, because in the case of "static secrets" (never changing) the risk of compromising increases with time. The use of a few shared secrets also ensures increasing security.

2-factor authentication can turn into **3-factor,** if it comprises **biometrical recognition**. The authentication procedure presented in Figure 1 includes a device token with embedded fingerprint recognition, in which the fingerprint check is the second factor, and entering a one-time password is a third factor. In this way, the user is protected from the possibility of the hardware device (respectively a chip card and its reader together with the access PIN code) to be stolen and also against the possibility of stealing access information or consciously transferring it to third parties.

Biometrical detection is increasingly recognized as a secure authentication mechanism. It can be performed by detection of the person's fingerprint, iris scan or another biometrical technology. The first two techniques are more and more widely applied [4, p. 10]. It is extremely important, however, to ensure the observance of legal protection of biometrical data. The existing, though minimal, potential possibility of theft based on biometrical user data leads to huge problems. Compromising such information means introducing a new identification system because of the impossibility of changing biometrical user characteristics.

Multifactor authentication in practice. The example of Great Britain

Because of the fact that the highest number of fraud cases as a result of identity thefts are registered in the USA, the processes of introducing multifactor user authentication in Web-based financial services are at the most advanced stage there. This stage corresponds to the regulations introduced by the bank supervisory institution in the USA – the Federal Financial Institutions Examination Council (FFIEC)[8].

According to the "Guidance on Authentication in an Internet Banking Environment", published by the Council in 2005, all banks and other financial institutions offering Web banking and other online services must establish correspondence between the level of authentication and the risks related to the offered goods and services. For this reason, the financial institutions should organize risk management related to the identification of the type and levels of risk associated with their Internet banking applications. Where the risk assessment shows that the use of one-factor authentication is insufficient, the financial institutions must use multifactor authentication and offer security at different levels.

In conformity with these requirements, the biggest bank in the USA – Bank of America, has introduced multifactor authentication using the so called "SiteKey security feature" based on the "shared secrets" method, and made of 3 parts: unique picture, selected by the customer, unique phrase, accompanying the picture, and three questions, the answer

[8] FFIEC – the Council was established on March 10, 1979 to prescribe uniform principles, standards, and report forms for and to promote uniformity in the supervision of financial institutions.

to which is known only by the customer. According to the risk assessment required by regulations in force, different security levels are established – for example, at the entry into the online banking system – from the usual IP address (computer) to the requirement for the user to recognize the picture and text and then enter a password. In case he tries access to the application from an unrecognized computer, the system asks him to enter a user name, answer one of three questions, make a correctness check of the picture and text, and only then enter the password. In this way, flexible multifactor authentication allows the customer to access Internet banking from another computer, different from the one he normally uses, and at a satisfactory security level.

The multifactor authentication practice in **Europe** is various and based on the use of a combination of different methods. One of the prevailing trends is to apply different technical security devices of the type of **tokens** mentioned above.

One of the versions of multifactor authentication includes the usage of bank chip cards[9]. A precondition for this in the European Union is the advanced phase of migration to chip-based debit and credit cards technology rooted in the EMV project.

The name of the project is formed by the initials of the consortium of three companies – Europay International, Mastercard International, and Visa International[10], which develops the new global standard of electronic financial transactions, based on chip cards. The new standard is introduced only for the use of pay cards at ATM and POS terminal devices, as an obligatory requirement together with the PIN code (personal identification code), but the new generation of smart cards can find applications in online transactions using a computer or a mobile device in case the customer has a reader device. Thanks to the computer chip technology embedded in the cards, the data are encrypted and high level of protection is ensured in this way. In practice, to copy/paste them into a new device is impossible – unlike the magnet band cards used so far.

For banks, the EMV-migration is a complicated and rather expensive process, not quite at a voluntary basis. It is being actively implemented by economic sanctions from the part of two main card organizations – Visa and MasterCard. The extremely high bank investment in the EMV – migration compel banks to use some additional features of chip cards by storage of new applications in their memory. Among them is the possibility of their **use for secure user recognition in online banking systems operations.** This guarantees to banks the achievement of a higher return to investment from the implementation of chip cards.

This possibility will soon be used by some banks in Great Britain in order to ensure more reliable protection to users of services through the Internet communication channel. At the end of January 2006, 99 % of card holders in Great Britain (i.e. 41.5 mln. card holders) had at least one chip card [7]. A total of 128 mln. chip cards have been issued since the start of the migration in October 2003, of which 65 mln. debit and 63 mln. credit cards. This allows bank institutions to actively use them as a tool for multifactor authentication of online banking customers.

[9] The terms chip card and smart card are used as synonym.

[10] At present, the third large card system JCB is a part of the Consortium.

Until the end 2007, some of the biggest banks in Great Britain – **Barclays**, **NatWest** and **Nationwide**, had implemented projects of supplying their customers (private persons and representatives of small and medium businesses) with *smart card readers* and *password-generating tokens,*. Under the **Barclays** project, for example, the bank will first supply free of charge chip cards readers to more than 500 thousand of Internet banking customers. In market capitalization, Barclays is the third biggest bank in Great Britain and ninth in the EU. Data provided by the bank show that at the end of 2006 its online banking service had more than 1.7 mln. customers and processed 214 mln. transactions[11]. The project of using chip cards for authentication, named "PINsentry" will be implemented by stages. The level of authentication is separated into different sublevels according to the risk level assessment. For example, users performing only information inquiries or those who make regular payments (for example, regular utility payments), will not need PINsentry. The system will be obligatory for private persons and small and medium business representatives, who make payments to third party accounts *for the first time*, as well as for new customers. In this case, in addition to the standard entry of the user name and password, when logging in the bank Web site, the customer will have to insert his EMV debit or credit card in the reader and to enter a PIN code, then the token device will generate an accidental 8-digit number that must be also typed in before the transaction is authorized. A new number is generated for each transaction. In this way, secure confirmation of customer identity is achieved by the use of several authentication factors.

The other two banks in the group of the five biggest banks in Great Britain – **NatWest** u **Nationwide**[12] also have similar projects of multifactor authentication in online banking. Another representative of the most powerful credit institutions – **Lloyds TSB**, develops a project that does not include the use of bank chip-cards, but the supply to users of token devices with embedded chip and generating accidental numbers.

Ensuring high level of protection allow banks to provide to their customers an "Online Banking Guarantee" (by Barclays[13], for example, or "Internet Banking promise" by Nationwide) to cover possible losses caused to the customer by Internet fraud. Thus, customers can use the Web based distribution channel with absolute confidence and the banks can rely on growing numbers of customers for their innovative services, bringing about considerable financial benefits.

The practice, however, shows that successful authentication methods in online bank services depend not only on the applied technology, but also to a high degree on the actions of customers and their level of information, vigilance, consciousness and sense of risk. Therefore, in addition to investments in secure user authentication projects – completed or in the process of implementation, the banks in Great Britain are extremely active in training their customers. Their sites pay great attention to dangers related to online protection, types of malicious software and potential ways of infection, the necessary

[11] http://www.newsroom.barclays.com/content/detail.asp?ReleaseID = 1013&NewsAreaID = 2

[12] Nationwide ("Nationwide Building Society") is a construction company, organized according to a cooperative principle, in which the participants have rights similar to shareholders. In April 2007, its assets were 137 mlrd. pounds and, according to this indicator, it is one of the first banks in Great Britain.

[13] http://www.personal.barclays.co.uk/BRC1/jsp/brccontrol?site = pfs&task = homefreegroup&value = 13491

measures for prevention of stealing personal data, recommendation on specific antivirus and other programs, etc.

Special sites like **Banksafe Online** (http://www.banksafeonline.org.uk) and **Get Safe Online (**http://www.getsafeonline.org) have been developed in order to support customer training and to counteract more successfully the network based bank fraud. They offer ample information on secure banking in real time and ways of self-defense. Sites offer detailed explanation of the types of fraudulent software and many specific examples of fraudulent phishing of e-mail addresses. In addition, they gather feedback information on suspicious electronic mail and false Web sites.

Protection against identity theft in Bulgarian banks

Cases of identity theft are registered not only among foreign Internet banking users, but also among Bulgarian bank customers. In our country, however, there is no statistics of the number of cases or the amount of money withdrawn from bank accounts. Only printed and electronic media report from time to time some cases, without trying to analyze them. According to information from the Department of "Computer crimes" at the Chief Directorate "Combating Organized Crime", more than 50 cases of withdrawal of big sums from Bulgarian bank accounts were registered only for half a year in Bulgaria[14]. The Statements of the Prosecutor General also mention some cases of identity thefts committed by Bulgarian citizens, where the victims have been foreigners[15]. It is considered that, as a whole, the level of these crimes in our country is significantly lower than in the developed European countries.

For the moment, only one Bulgarian bank – First Investment Bank AD, has announced in its site and, by sending special letters, notified the customers of its Virtual Banking Branch about several cases of breaching the security of the Internet banking system. The insistent recommendation of the bank to the users is to purchase a universal electronic signature from some of the four suppliers of authentication services and, in particular, from InfoNotary EAD, where the use of the signature is free-of-charge during the first year.

Most of the banks operating on the Bulgarian market and offering Internet banking services to their customers do not pay attention to the necessity of explaining problems and potential dangers for systems' security to their customers.

If we consider the *group of the first five biggest banks* based on the size of their assets, we will find out that three of them ignore the potential problem and, in their sites, do not mention possible breakdowns threatening their customers, or the ways unauthorized access can be realized – **DSK Bank** (on **DSK Direct**), **UniCredit Bulbank** (the system Bulbank Online) and **United Bulgarian Bank** (U-online). The fourth big bank – **Raiffeisen Bank (Bulgaria)** offers to its customers a "Security Instruction", where it gives advices related to the use of "Raiffeisen ONLINE" that are short and not comprehensive enough. The customers are advised not to pay attention to electronic

[14] The information is quoted after BTV, 17.10.2007 - http://btv.bg/news/?magic = bulgaria&story = 61245

[15] Source: Prosecutor General of the Republic of Bulgaria. News.
http://www.prb.bg/php/newspage.php?news = %20 %20 %20 %20 %20873

messages similar to possible messages from the bank and asking for personal data; the fact that the bank has no practice of exchanging electronic mail information is emphasized. **First Investment Bank** offers a more exhaustive document – "General Recommendations for Higher Security in the Work with Internet Banking of FIB AD", in which the bank provides instructions to its customers how to enter the site and recognize its validity, what are the recommended browser adjustments in working with the system, etc.

There are also *positive examples from the practice of our banks,* some of them assuming the necessary responsibility on security problems of Internet banking systems, the information of customers, and explaining the possible dangers to them. The advices provided by **ING Bank N.V. – Sofia branch** in the "Security" section (published in the file 2007_Security BG.doc) are at the level of Western bank practice. Following these advices is in the best customers' interests and they are quite exhaustive; updated in 2007, they contain detailed instructions on what the customers should do to support higher security in the use of Internet banking. The added security protection glossary is also an improvement in the bank security policy. Another positive example can be found in the instructions provided by **Piraeus Bank Bulgaria** in the "Security" section[16] of Piraeus Online Banking. They include an explanation of the term "phishing", of the necessity to use anti-virus and anti-spy software, and a firewall, at the client computer, of the essential importance of customers' vigilance, etc.

As to the incidence of projects implemented in **secure multifactor authentication in the online banking systems of the banks in Bulgaria,** we can note that for now such projects are relatively rare. Without pretending to be exhaustive, we will mention some banks in our country, which offer to their customers higher security based on more authentication factors. At **City Bank N.A. – Sofia branch** – an office of the American bank in Bulgaria, each Internet banking customer (of CitiDirect Online Banking) receives a *personal device generating dynamic passwords* (Safe Word card). The use of one-time passwords eliminates the danger of possible spy software presence on the client computer and ensures secure authentication with more factors.

ProCredit Bank (Bulgaria) – the Bulgarian-American Credit Bank – and Teximbank both work with unique *one-time six-digit codes* – the so called TANs (transaction identification number) used by customers to sign payment orders to the bank. Each Internet banking customer receives a TAN-code list and after it is used, the bank provides a new one. The requirement of correspondence between risk levels and authentication is thus fulfilled. This way of ensuring secure authentication is relatively old; it is widely used by the banks in Germany and is related to some difficulties for the customer because of the necessity to get new TAN-code lists on paper and the danger for these lists to be lost or stolen.

In the bank with Slovenian share capital – **NLB West-East Bank,** the use of hardware authentication devices is required – these are token devices (in particular, SafeNet Security iKey 2032). The customer digital certificate, required for entry into the Internet banking system, is stored in their chip. The device is inserted into the USB-port of the client computer . The payment orders sent by customers are necessarily "signed" using an

[16] https://www.piraeusonline.bg/include/login/showWindow.asp?id = 78.lang = BG

electronic signature by the device. 2-factor user authentication is ensured in this way. However, customers must pay a one-tome tax according to the bank tariff list for using the device and the sum is not negligible, especially for individuals[17]; therefore, it has a limiting effect on the use of the service.

The same technology is applied in **ING Bank N.V. – Sofia branch** since March 2007. For all corporate customers, access into the Internet banking system ING Online requires a digital certificate, installed on a smart card issued by the bank. The purpose is to increase the security level through 2-factor authentication.

According to the author's own research, there are some other banks preparing projects of introducing multifactor authentication based on one-time transaction code. One of them is **Raiffeisen Bank (Bulgaria),** which intends to provide to its customers personal token devices of the Vasco type[18]. The work method consists in validation by a request-response in real time – i.e. the internet banking site generates a request number made of 6 or 8 digits, which the customer must enter by the keyboard of his personal device. On its turn, the device generates a response (6 or 8 digits again), which is then entered by the customer back into the site.

Summary and recommendations

Banks and other institutions, interested in the fight with identity thefts, must be more **active** and **synchronize** their actions, first at the level of the European Union and then at the world level, for the prevention of such illegal acts by cyber criminals. At the moment, 6 of 10 European citizens consider that such theft happens often in their countries, and about half of them do not believe that the national measures are sufficient and hold the opinion that **solving this issue at the EU level** would be far more efficient than at the national level [2].

Some steps are made in this direction, i.e. the adoption in 2001 of the European Convention on Cybercrime, signed by 29 countries, among which the USA, Japan, and Bulgaria.

The danger of breaches in Internet banking systems and of identity thefts in banks operating on the Bulgarian market should not be underestimated. At present, there is information in our country mainly on cases of Bulgarian cyber criminals operating outside Bulgarian borders – generally as there are larger sums of money on customer accounts in Western banks. This does not mean, however, that our banks can afford lagging behind in the prevention of such adverse events.

The process of introduction customer secure multifactor authentication in conformity with different risk levels is at an advanced stage in the banks at world scale. Credit institutions in our country should start working, respectively, accelerate their actions, on these problems in order to overcome the present gap.

Bulgarian customers are still not acquainted with the immense dangers they may encounter while using Internet banking. Therefore, *the banks in our country must lay the foundations of customer education in this field*. For the moment, most banks just warn their customers – mainly about the fact that they do not communicate through electronic mail. Their sites, with a few exceptions, contain

[17] For the moment, the tax is EUR 70.
[18] http://www.vasco.com/products/product.html?product = 48

no explanations, glossaries, or examples, i.e. pictures, with regard to the essence and ways of e-crimes involving identity theft – phishing, pharming, etc. A good example in this respect could be the site of **Barclays** bank in the sections "Online Personal Banking", "Online security"[19].

Bulgarian legislation needs to introduce protection of Internet banking customers from losses occurring as a result of unauthorized transfer or withdrawal of funds from their accounts in the way Federal bank regulation in the USA imposes such protection. These regulations detail customers' responsibility in three cases – up to *$50, $500* or *the whole sum*, depending on the time period, during which the customer knows and notifies his bank about unauthorized online transactions. At present, Bulgarian customers themselves bear the responsibility and the consequences of possible adverse events resulting from online banking systems and affecting their funds.

Unlike banks in developed countries, which provide on their own initiative full guarantee for the 100-percent coverage of their customers' losses from unauthorized transactions, banks in our country declare in advance in their General Internet Banking Terms and Conditions or in the contracts that they are not responsible for damage caused by the intrusion of third parties in the systems. Such texts can be found in the terms and conditions of online banking, for example, of UniCredit Bulbank and Bank DSK, both being part of the group of the biggest banks in Bulgaria. Such declarations do not correspond to the standards of good bank practice and are in the interests neither of customers, nor of the banks, as if the latter protect their customers, they will ensure protection of their business as well.

It is necessary to create an institution with coordinating functions in the cooperation between commercial banks, BNB, bank customers and software developers of electronic financial services systems with respect to cyber crime in online banking – the institution will be gathering statistical data on different cases, jointly implementing prevention measures, introducing common security standards, initiating proposals for legal changes, etc. The organizational form could be an association, workgroup, or a committee. In our opinion, commercial banks should have the leading role in it; therefore, if the organizational form is a committee, it can be created by the Commercial Banks Association only.

As a conclusion, we would like to mention that investments from the part of banks in projects for the implementation of multifactor user authentication for online bank services is a reliable way of preventing identity thefts and ensures the necessary high level of protection. The use of such methods will guarantee the stability of the ascending trend in the numbers of Web-based banking users.

Literature

1. Arsenov, A., Biometrics comes back to business // CIO, 2005, № 4, p. 48-52.

2. Press release about a conference on the topic: "Maintaining the integrity of identities and payments: two challenges to fraud prevention", Brussels, 22.11.2006

[19] http://www.personal.barclays.co.uk/BRC1/jsp/brccontrol?task = channelFWgroup&value = 8722&target = _blank&site = pfs

http://www.evropa.bg/bg/del/info-pad/news.html?newsid = 2337

3. Andersen, N., The Threat of Cybercrime: The Challenge of Online Identity Theft and Strengthening the Public-Private Partnership in a Changing Threat Environment // Report, presented at a conference on the topic "Maintaining the integrity of identities and payments: two challenges to fraud prevention", Brussels, 22.11.2006

4. Federal Financial Institutions Examination Council: Guidance on Authentication in an Internet Banking Environment – October 2005.

5. http://www.barclays.co.uk

6. http://www.banksafeonline.org.uk

7. http://www.chipandpin.co.uk

8. http://www.id-protect.co.uk/index.php

9. http://www.michigan.gov/cybersecurity/0,1607,7-217-34415---,00.html

10. http://www.unidentity.com

11. http://www.vasco.com ИА