

**ΑΛΕΞΑΝΔΡΕΙΟ ΤΕΙ ΘΕΣΣΑΛΟΝΙΚΗΣ**  
**ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΑΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ**  
**ΤΜΗΜΑ ΛΟΓΙΣΤΙΚΗΣ ΚΑΙ**  
**ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗΣ**



**ΘΕΜΑ: E – BANKING**

**ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ**  
**Του Κυριάκου Υφαντίδη**

**Επιβλέπων καθηγητής**  
**Θεόδωρος Γκιούρης**

**Θεσσαλονίκη 2014-2015**

## TABLE OF CONTENTS

	page
<b><u>INTRODUCTION</u></b> .....	2
<b><u>CHAPTER ONE</u> Basics of electronic banking</b> .....	3
1.1. History of e-banking.....	3
1.2 Forms of e-banking.....	4
1.3 Activities offered to clients.....	7
1.4 Benefits of e-banking.....	7
1.4.1 Benefits for banks.....	7
1.4.2 Benefits for customers.....	8
1.5 Drawbacks of e-banking.....	8
1.6 Dangers hiding in e-banking.....	9
1.7 Internet Banks.....	10
1.7.1 Banking internet sites functionality.....	11
<b><u>CHAPTER TWO</u>..E-Banking in Greece</b> .....	12
2.1 Internet Banking in Greece.....	12
2.2 Classification of Internet Banks.....	13
2.3 The Development of Internet Banking Services in Greece.....	13
2.4 Cases of Banks using E-banking.....	14
2.4.1 ALPHA BANK.....	14
2.4.2 COMMERCIAL BANK OF GREECE.....	15
2.4.3 EUROBANK.....	15
2.4.4 NATIONAL BANK OF GREECE.....	16
2.4.5 WIN BANK.....	17
<b><u>CONCLUSION</u></b> .....	17
<b><u>REFERENCES</u></b> .....	19

## INTRODUCTION

Advances in information and communication technologies in particular, the growing use of the internet for business transaction, have had a profound effect on the banking industry. While this is a global phenomenon, creating a truly global marketplace, penetration of internet banking into less developed countries lags behind that of the developed Western countries.

Banking has always been a highly information intensive activity that relies heavily on information technology (IT) to acquire, process, and deliver the information to all relevant users. Not only is IT critical in the processing of information, it provides a way for the banks to differentiate their products and services. Banks find that they have to constantly innovate and update to retain their demanding and discerning customers and to provide convenient, reliable, and expedient services. Driven by the challenge to expand and capture a larger share of the banking market, some banks invest in more bricks and mortar to enlarge their geographical and market coverage. Others have considered a more revolutionary approach to deliver their banking services via a new medium: the Internet. Since the introduction of the Internet in 1969, it has evolved from the sole domain of the computer nerd and the academic to a mainstream channel of communication. Recently, it has been rapidly gaining popularity as a potential medium for electronic commerce. The rapid growth of the Internet has presented a new host of opportunities as well as threats to business. Today, the Internet is well on its way to become a full-fledged delivery and distribution channel and among the consumer-oriented applications riding at the forefront of this evolution is electronic financial products and services.

With the rapid diffusion of the Internet, banking in cyberspace is fast becoming an alternative channel to provide banking services and products. In the USA, banks are already providing services on the Internet and Internet banks, such as Security First National Bank, are beginning to appear. The Internet is now being considered as a strategic weapon and will revolutionize the way banks operate, deliver, and compete against one another, especially when competitive advantages of traditional branch networks are eroding rapidly. As "*Business Week*" noted, "Banking is essential to a modern economy, banks are not" (quoted in Financial Times, 1996). This statement is supported by a recent report from Booz Allen & Hamilton (Warner, 1996) that claims the Internet poses a very serious threat both to the customer base of the traditional banking oligopoly and to its profits. Their belief is that the Internet promises a revolution in retail banking of monumental proportions. High street or brick and mortar banks as we know them may largely disappear.

Indeed, the emergence of Internet banking has prompted many banks to rethink their IT strategies in order to stay competitive. Customers today are demanding much more from banking services. They want new levels of convenience and flexibility (Birch and Young, 1997; Lagoutte, 1996) on top of powerful and easy to use financial management tools and products and services that traditional retail banking could not offer. Internet banking has allowed banks and financial institutions to provide these services by exploiting an extensive public network infrastructure (Ternullo, 1997). Despite the many potential benefits, many teething problems will need to be addressed before Internet banking can become widely adopted. It is believed that, in the future, Internet banking will recede in importance as a strategic

application to become a competitive necessity that must be adopted by most if not all banking and financial institutions.

## **CHAPTER 1 : BASICS OF ELECTRONIC BANKING**

### 1.1 History of e-banking

The precursor for the modern home online banking services were the distance banking services over electronic media from the early 1980s. The term 'Online' became popular in the late '80s and referred to the use of a terminal, keyboard and TV (or monitor) to access the banking system using a phone line. 'Home banking' can also refer to the use of a numeric keypad to send tones down a phone line with instructions to the bank. Online services started in New York in 1981 when four of the city's major banks (Citibank, Chase Manhattan, Chemical and Manufacturers Hanover) offered home banking services using the videotex system. Because of the commercial failure of videotex these banking services never became popular except in France where the use of videotex (Minitel) was subsidised by the telecom provider and the UK, where the Prestel system was used.

When the clicks-and-bricks euphoria hit in the late 1990s, many banks began to view Web-based banking as a strategic imperative. The attraction of banks to online banking are fairly obvious: diminished transaction costs, easier integration of services, interactive marketing capabilities, and other benefits that boost customer lists and profit margins. Additionally, Web banking services allow institutions to bundle more services into single packages, thereby luring customers and minimizing overhead.

A mergers-and-acquisitions wave swept the financial industries in the mid-and late 1998s, greatly expanding banks' customer bases. Following this, banks looked to the Web as a way of maintaining their customers and building loyalty. A number of different factors are causing bankers to shift more of their business to the virtual realm.

While financial institutions took steps to implement e-banking services in the mid-1990s, many consumers were hesitant to conduct monetary transactions over the web. It took widespread adoption of electronic commerce, based on trailblazing companies such as America Online, Amazon.com and eBay, to make the idea of paying for items online widespread. By 2000, 80 percent of U.S. banks offered e-banking. Customer use grew slowly. At Bank of America, for example, it took 10 years to acquire 2 million e-banking customers. However, a significant cultural change took place after the Y2K scare ended. In 2001, Bank of America became the first bank to top 3 million online banking customers, more than 20 percent of its customer base. In comparison, larger national institutions, such as Citigroup claimed 2.2 million online relationships globally, while J.P. Morgan Chase estimated it had more than 750,000 online banking customers. Wells Fargo had 2.5 million online banking customers, including small businesses. Online customers proved more loyal and profitable than regular customers. In October 2001, Bank of America customers executed a record 3.1 million electronic bill payments, totaling more than \$1 billion. In 2009, a report by Gartner Group estimated that 47 percent of U.S. adults and 30 percent in the United Kingdom bank online.

The UK's first home online banking services known as Homelink was set up by Bank of Scotland for customers of the Nottingham Building Society (NBS) in 1983.

The system used was based on the UK's Prestel viewlink system and used a computer, such as the BBC Micro, or keyboard (Tandata Td1400) connected to the telephone system and television set. The system allowed on-line viewing of statements, bank transfers and bill payments. In order to make bank transfers and bill payments, a written instruction giving details of the intended recipient had to be sent to the NBS who set the details up on the Homelink system. Typical recipients were gas, electricity and telephone companies and accounts with other banks. Details of payments to be made were input into the NBS system by the account holder via Prestel. A cheque was then sent by NBS to the payee and an advice giving details of the payment was sent to the account holder. BACS was later used to transfer the payment directly.

Stanford Federal Credit Union was the first financial institution to offer online internet banking services to all of its members in October 1994.

Today, many banks are internet only banks. Unlike their predecessors, these internet only banks do not maintain brick and mortar bank branches. Instead, they typically differentiate themselves by offering better interest rates and more extensive online banking features.

### 1.2 Forms of E-banking

Clients use modern communication media for remote communication with the bank: a modem, telephone, computer or payment card. A characteristic feature of these services is the client's uninterrupted round-the clock account access, i.e., independent of banking business hours and the ability to execute local and international payments directly from the comfort of the home or office. This reduces cash handling and transport costs, lowers the risk of theft or accepting counterfeit bank notes, increases speed and enhances the comfort of making payments.

Electronic communication means are particularly coming to the forefront. These are more convenient, faster, and often cheaper for clients. Banking experience shows it is suitable to use combinations of several communication means, depending on individual segments, clients, and types of operations, products and situations. Electronic banking is a service that specifically uses electronic communication forms.

Electronic banking can be divided on the basis of the instruments used: **telephone banking, internet banking, mobile banking, SMS banking mail banking**, etc.

**Phone banking** is the provision of banking services using a classic telephone line. A bank client can obtain the necessary information on dialing a telephone number specified in advance. Before the requested banking service information is provided, the client's identity is determined using contractually agreed terms. Using this banking service enables bank clients to obtain information concerning active and passive banking products, but a client can also actively use the bank payment system and request, for example, a payment order or a collection order, open or cancel a term deposit or a current account. In this case a fax connected to the telephone serves as an output communication channel.

The client advisor or so-called telephone banker is a bank employee capable of providing any information about products and services and, following verification that he is speaking with an authorized person, can also perform any passive or active operation. He can provide advice to the client and offer further banking products.

One advantage of this service is that it requires no additional technical equipment apart from a telephone. As a rule bank telephone center (call center) operators work 24 hours a day nonstop and it is thus possible to use their services from any place at any time.

**Internet banking** can be used from the home or the office, as well as an internet café, although the latter is not recommended for security reasons. In order to handle his account a user just needs an internet browser (such as MS Explorer or Netscape Navigator). A client cannot avoid visiting the bank though, because he must first ask for an identification code. After opening the bank's web site the client simply selects internet banking and, further to proper identification, can perform passive or active operations. Good internet banking should provide a maximum of services. No less important are the graphic interface, clarity, simplicity, and unambiguity of usage. The intelligibility of texts determines simplicity and speed of understanding of the meaning of menu items, data fields, and general text information displayed to the client.

Safety for concrete applications is assured by client authentication, verification of data and data protection by encryption. Client identification is done using passwords or codes. The client chooses some of these and the bank assigns others. It is recommended to choose a password made up of various types of characters, which can be a combination of numbers, lower case and capital letters, and special symbols.

Banks usually protect large volume transactions with additional security means, such as an encryption (authentication) calculator, or a token, which generates nonrecurring random passwords, which a client types on confirming an order. The token itself is protected by certain security features. Work with it is only enabled after the client types a four-digit PIN code, whereby the user can change the PIN at any time. In the event of three failed attempts to type the correct PIN the token blocks itself. After 60 seconds of inactivity a token automatically switches itself off and once switched back on, it again requests the PIN.

When a client generates several (for example 10) authentication codes in succession and types none of them into the client system, the key becomes desynchronized. This protection serves to prevent use of the key for other purposes. A cheaper and, based on its dimensions, more practical alternative to a token is a grid card. This is a card with a mesh drawn on it with fields with random generated characters. The user authorizes an active operation by typing the right code from the field of the card the operator requests from him.

**Mobile banking** is a system that allows customers of a financial institution to conduct a number of financial transactions through a mobile device such as a mobile phone or tablet.

Mobile banking differs from mobile payments, which involve the use of a mobile device to pay for goods or services either at the point of sale or remotely, analogously to the use of a debit or credit card to effect an EFTPOS payment.

The earliest mobile banking services were offered over SMS, a service known as SMS banking. With the introduction of smart phones with WAP support enabling the use of the mobile web in 1999, the first European banks started to offer mobile banking on this platform to their customers.

Mobile banking has until recently (2010) most often been performed via SMS or the mobile web. Apple's initial success with iPhone and the rapid growth of phones based on Google's Android (operating system) have led to increasing use of special client programs, called apps, downloaded to the mobile device. With that said,

advancements in web technologies such as HTML5, CSS3 and JavaScript have seen more banks launching mobile web based services to complement native applications. A recent study (May 2012) by Mapa Research suggests that over a third of banks have mobile device detection upon visiting the banks' main website. A number of things can happen on mobile detection such as redirecting to an app store, redirection to a mobile banking specific website or providing a menu of mobile banking options for the user to choose from.

**SMS banking** uses short text messages sent through the client's mobile phone. SMS text messages can be used for both passive and active operations similarly as with classic telephone banking. A client can automatically receive information about his account balance: an SMS is sent to the client immediately after a certain operation is performed, or on request: a client sends the bank a correctly formatted message which processes it and answers the client's request by SMS.

Information sent on request mostly concerns current interest rates or currency exchange rates. Providing these is simple for the bank because this is publicly accessible information that needs no protection. A client however can request information about the balance in his account, which is not public information and must be protected when it is provided. Passwords are used for this purpose or technologies based on the principle of an electronic key. A client however is required to know the code of every transaction including constant and variable symbols. The whole message containing data separated by # symbols sometimes has up to fifty characters. Users can easily make mistakes. This is frequently a limiting factor for clients, reducing the comfort factor in this service.

**Mail banking** is another electronic banking service that makes it possible to communicate with the bank by electronic mail or e-mail. The most frequently used service is sending account statements at agreed periodicity to the client's mailbox. E-mail is not used for more complex operations.

Apart from those already mentioned, there are other more or less widely known forms of electronic banking, including a **payment card, an electronic wallet and a self-service zone**.

A payment card is currently one of the most widely used payment instruments designated for authorized holders through which they can perform non-cash payments or cash withdrawals from an extensive network of automated teller machines. An electronic wallet represents a chip card similar to a payment card that contains a record of a financial sum that is available to its owner. A self-service zone is a fully automated alternative work place of a bank with terminals and devices that clients can use to get various bank services. It enables active and passive operations offered by the bank to be made without the presence of a bank employee. Devices are constructed for very easy use with simple intuitive controls (user friendly). Equipment includes modern security systems outside and inside a self-service zone. A payment card in combination with a password is used to access a self-service zone. It is also possible to use other authentication devices, such as an electronic key, but also

a fingerprint. Self-service zones are available 24 hours a day, 7 days a week.

In expert circles it is sometimes possible to encounter another form of electronic banking: fax-banking. A fax is however mostly used as an addition to other forms, such as telephone banking, when a client agrees with the bank that all output would be sent to him by fax.

### 1.3 Activities offered to clients

Online banking uses the internet as the chief medium of delivery by which banking activities are executed. The activities clients are able to carry out are can be classified to as transactional and non-transactional.

#### *Non transactional activities*

- 1) Account balance viewing
- 2) Viewing of previous bank transactions
- 3) Bank statement downloading
- 4) Check book ordering
- 5) Viewing of images of paid cheques
- 6) M banking and E banking applications downloading
- 7) Provision of account/ bank statements

#### *Transactional activities*

- 8) Electronic funds transfer
- 9) Bill payments and wire transfers
- 10) Loan application and repayments
- 11) Buying investment products

### 1.4 Benefits of e-banking

#### 1.4.1[For banks]

Internet banking offers many benefits to banks and their customers. The main benefits to banks are cost savings, reaching new segments of the population, efficiency, enhancement of the bank's reputation and better customer service and satisfaction.

According to a global survey conducted by Booz-Allen and Hamilton (1997), the establishment of specialized Internet Banking requires only US\$1-2 million, which is lower than branch-based banking setup. The traditional bank's running costs account for 50% to 60% of its revenues, while the running costs of Internet Banking is estimated at 15% to 20% of its revenues.

According to Robinson (2000) the cost of an electronic transaction is dramatically less when done online compare to at a branch. According to Robinson (2000) the cost of an electronic transaction is dramatically less when done online compare to at a branch.

Sheshunoff (2000) says further that the single most important driving force behind the implementation of full service Internet banking by banks is the need to create powerful barriers to customer exiting. He argues that once a customer moves to full-service Internet banking, the likelihood of that customer moving to another financial institution is significantly diminished. The main reasons for this behavior can be found in the consumer behavior theory: switching always requires much time and effort from the individual consumer. He concluded that the competitive advantage of Internet banking for banks is very significant.



Mols (1998) conducted a survey in Denmark argued that Internet Banking might be useful for strengthening cross-selling and price differentiation. Internet banking makes it possible for banks to offer consumer a variety of services 24/7. Internet banking is attractive because the consumer are more satisfied with their banks, are less price sensitive have the highest intention to repurchase, and provide more positive word of mouth information than other bank customers.

#### 1.4.2 [For customers]

Internet banking offers also new value to customers. The emergence of the Internet has had a significant impact on the diffusion of electronic banking. With the help of the Internet, banking is no longer bound to time or geography. Consumers all over the world have relatively easy access to their accounts 24 hours per day; seven days a week. It makes available to customers a full range of services including some services not offered at branches. The greatest benefit of Internet banking is that it is cheap or even free to customers. However, price seemed to be one factor militating against Internet banking. Two important factors in the price debate are on the one hand geographical differences and on the other hand disparities between the costs of e.g. Internet connections and telephone call pricing. It has also been argued that electronic banks are more likely to change in response to customers' demands. Internet banking has the advantage that the customer avoids traveling to and from a bank branch. In this way, Internet banking saves time and money, provides convenience and accessibility, and has a positive impact on customer satisfaction. Customers can manage their banking affairs when they want, and they can enjoy more privacy while interacting with their bank. It has been claimed that Internet banking offers the customer more benefits at lower costs.

Internet banking is extremely beneficial to customers because of the savings in costs, time and space it offers, its quick response to complaints, and its delivery of improved services, all of which benefits make for easier banking.

To summarize, electronic banking in general and Internet banking in particular offer many benefits to both service providers and their customers.

#### 1.5 Drawbacks of E-banking

##### **Security**

While banks typically offer secure web pages to conduct your business transactions, this doesn't guarantee complete safety. All websites, even secure ones, may be susceptible to Internet criminals who try to hack into your account and gain access to your business private financial information. This can lead to fraudulent use of your business identity and potentially cost you thousands of dollars.

##### **Site Disruption**

A technical glitch could cause the bank website to go offline for a period of time, possibly resulting in problems for you and your business. For example, you may need immediate funds after normal banking hours to make a payment or emergency business purchase. Routine site maintenance also occurs, although this normally takes place during off-peak hours.

### **Site Navigation**

If you're new to online banking, it may take some time to get used to it, taking valuable time out of your work day. Online banking offers a large number of transactions, so frustration may occur while you're learning to navigate the site. Banks also update web pages to add new features, requiring additional learning and possibly the need to change account numbers or passwords. If you need help, you might encounter a lengthy wait when using the bank telephone customer service line.

### **User Apprehension**

Some business owners may not feel comfortable with the idea of placing vital financial information into an online account, or may be apprehensive about using the Internet. If you're a longtime small business owner who is used to doing banking in person or even by telephone, this hurdle might be difficult to surmount.

### **Accessibility**

If your business is located in a rural or remote area, your Internet options could be limited. Depending on your type of business, this can make conducting transactions difficult. For example, if you operate a home-based business and you do not have access to a high-speed cable connection, you may have to use a slower dial-up service. As a result, your business banking may take more time, or you might even experience times where you cannot get online.

## 1.6 Dangers hiding in E-banking

Whereas online internet banking has created a convenient way for us to handle our business without leaving our home, inherent dangers associated with internet banking must be taken into consideration, too.

### **Identity Theft**

A financial institution may use state-of-the-art security measures to protect your information, but once you have your account available online, your information is at risk from hackers, according to the article titled "Online Banking--Advantages and Disadvantages" as published on Financial Web. Computer criminals are always working to bypass existing security systems, and if your financial accounts are held on a bank's server then they could be fair game to being stolen. All of your personal information, including your Social Security Number that is associated with your account is as risk as well.

### **Up-to-Date Information**

One of the lesser thought about dangers is the actual information. Many banks offer up to the minute transaction activity, and others don't. It's a slippery slope if we start relying on the balance information shown on our internet accounts, we could easily overdraft our accounts. Many people will toss out the check registers, and with debit cards, this can be very easy to forget to update them if we do keep them.

### **Secure Logins**

You need to make sure that your bank has completely secure log in areas. It's unfortunately not uncommon to end up with a virus that redirects your web browser to a mirrored site. These sites can look identical to the banks sites. Many sites that hold sensitive information have included extra security measures that are hard to mimic. Even though they are hard to mimic they aren't fool proof. Ensure you know the banks log in address and that your browser was pointed there before you log in. Also keep your virus protection up to date to help avoid this.

### **Phishing**

Phishing is when a criminal sends out emails to people with fake links trying to get those people to click on the links and give away their personal information, according to the article titled "Banking Securely Online" published by the US Computer Emergency Readiness Team. When you set up an online bank account, you may get one of these emails. If you click on the fake link, it will take you to a website that looks and acts like your bank's login page. The page was actually set up to steal your login information. Within minutes of having your login information, the hacker will log in to your account and begin stealing your money and your personal information.

### **Internet banking might "dehumanize" banking**

Some people think that Internet banking can "dehumanise" banking activities by removing the social, human contact aspect of banking (Hennigan and Gourvenec 1996). There are many people, especially older, that see standing in a queue waiting to have banking transactions at a branch as a great social event where they can meet their friends or even make new ones. However, banking through the WWW does not intend to replace completely traditional banks. It just offers an additional service channel that customers can use together with phone banking, PC home banking, ATMs and physical branches. Finally, Internet banking is here and sooner or later is going to change our perceptions and attitudes of managing our money. As a result, it is important for the people to know its weaknesses but there is not any way of preventing it since many banks all over the world have either launched an Internet banking service or announced their intention to do so in the near future.

## 1.7 Internet banks

There are four different categories of banks that are currently present on the Internet.

The first category is Internet presence, which is the most basic one because it describes sites, which focus on providing information but fail to identify the complete advantages that the Internet gives in comparison to paper-based information.

The second category is interactivity, which is the following step of describing sites that attempt to be interactive with the user. In this category a feedback form and an email address are provided. In order for these sites to make the user's visit more interesting and useful, they need to be well designed and easily navigable, while having a combination of features such as Java, Java Script, animated graphics, sound and video.

The third category is PC Home banking, which is the use of proprietary financial software running on a computer at home, to perform transactions such as fund transfer and bill payment.

The fourth category is full Internet banking, which is accessing accounts from a browser, without the need for proprietary software that PC Home banking requires.

### 1.7.1 Banking internet sites functionality

Banks are trying to take advantage of three different opportunities that Internet technology offers (Diniz 1998): i) to provide information, ii) to conduct banking transactions like the ones held in branches or in ATMs, iii) to improve customer relationship. However, sometimes these opportunities become blurred, which makes difficult the classification of the Web sites.

Each of these different categories can be splitted in three levels of interaction to classify the various kinds of applications of the banks' Web sites. There are three levels of interactivity: i) Basic or incremental, where a bank reproduces the way it works with other media than the Web, ii) Intermediary, where particular features of the Web are used to improve banking services and activities, iii) Advanced, where business opportunities are created. The categories of activities and the levels of interactivity can be seen clearly in the following table:

	<b>Basic (incremental)</b>	<b>Intermediary (improvement)</b>	<b>Advanced (transformation)</b>
<b>Information delivery</b>	<ul style="list-style-type: none"> <li>• electronic brochure</li> <li>• institutional</li> <li>• promotional</li> <li>• contact</li> <li>• offers</li> </ul>	<ul style="list-style-type: none"> <li>• search engines</li> <li>• report download</li> <li>• recruitment forms</li> <li>• hot links</li> </ul>	<ul style="list-style-type: none"> <li>• customise</li> <li>• subscription</li> <li>• advertisement</li> <li>• discussion groups</li> </ul>
<b>Transaction</b>	<ul style="list-style-type: none"> <li>• open account</li> <li>• product and service request</li> <li>• investment and credit application</li> </ul>	<ul style="list-style-type: none"> <li>• balance</li> <li>• statement</li> <li>• fund transfer</li> <li>• bill payment</li> </ul>	<ul style="list-style-type: none"> <li>• banking service by</li> </ul>
<b>Customer relationship</b>	<ul style="list-style-type: none"> <li>• e-mail</li> <li>• suggestion forms</li> </ul>	<ul style="list-style-type: none"> <li>• calculator</li> <li>• investment advisor</li> <li>• software download</li> </ul>	<ul style="list-style-type: none"> <li>• product and service development</li> <li>• video conference</li> </ul>

Table 3.5: Framework for Banks' Classification (Diniz 1998)

## **CHAPTER 2: E-BANKING IN GREECE**

### **2.1 Internet Banking in Greece**

Internet technology can provide cost-effective banking solutions and Greek banks are trying to take advantage of the opportunities that this technology and computers offer by enhancing competitiveness and expanding market base via Internet banking. Although Internet use in Greece is still not as high as in other European countries, online banking transactions continue to increase because Greek customers are seeking for convenience. They are tired of the sometimes-endless queues at the cashiers' desks and the strikes, they want to minimize their transaction time, they are afraid of bank robberies and they don't want to carry cash with them. According to the Hellenic Bank Association, the daily turnover is about 100 million Euros and the number of transactions for 2004 was about 7 million. Moreover, there are 20 credit institutions and 10 branches of foreign banks in Greece with presence on the Internet. Although the numbers are constantly changing, in the Greek market the Internet offers an alternative distribution channel, which at the moment only 16 banks are taking full advantage of with approximately over 500,000 online banking customers. However, soon more Greek banks are expected to follow, which shows that Internet banking is poised for rapid growth in the country.

Cyberbanks are advancing all across Europe and online banking represents about 24% of all European bank customers (European Banker 2006). Greek institutions are already comfortable in a culture that offers complete financial services, such as loans, credit cards, insurance and investments under one roof. Greek spending for Internet - delivered financial services areas will contribute to big changes in Europe's financial services industry. Bankers have realised that traditional branches have a high cost due to the expenses for staff's salaries, which can be up to two thirds of total running costs, while the Internet has dramatically cut transaction costs (European Banker 2006). As a result, banking fees and margins are being driven down and the use of the Euro in the EMU countries make Internet banking across different countries even easier. This situation puts more pressure to Greek banks to establish or to improve their Internet banking technology faster and to gain a higher market share in neighboring countries, mainly in the Balkan region.

All the Greek sites provide information with or without interactivity, regardless of the size of the bank. Most of the banks offer addresses, phone numbers etc. in order to make the customers contact with the physical branches. Others have press releases, newsletters and welcome letters to improve their public relations. Big banks depend on their brand names so they like to show their successful managers and financial information concerning assets and profits, while smaller banks provide information on fees and rates of products and services, where they are more competitive. Moreover, many banks provide economic information about the financial market, job offers and promote other channels of providing banking services.

Concerning the transaction channel, banks are trying to create an alternative method to deliver products. Customers can open accounts and request products and services. They can ask for credit cards and apply for investments. They can have access to bank databases to look up account balances and statements or transfer funds between accounts and pay bills (electricity, water, fixed phone, mobile, insurance premiums). At the advanced level of interactivity, full-fledged transactions are being

handled. However, some transactions (transfers within the same bank) are being executed in real time while others (transfers to other than the customer's bank or remittances) occur late at night depending on the bank. In addition, corporate customers can pay VAT and social security contributions, personnel's salaries, suppliers and cooperators fees, while setting different levels of Internet banking access and transactions execution for various users.

Concerning improving customer relationship, all the banks provide e-mails and feedback forms to the clients, so that they can make suggestions, complaints or general queries. Electronic communication can eventually save banks money because it is cheaper than mailing information or providing phone services. With this method, the banks get structured information from their customers in order to find out what the clients want and build a better relationship with them. Once they identify the investment profile of the customers, they can offer them specific products and services tailored to their needs.

Regarding security, Greek banks are very concerned, especially after the phishing attack towards the customers of Alpha Bank, Emporiki Bank and the National Bank of Greece that took place during autumn 2005 and they use firewalls and special software such as IDS-Intrusion Detection System.

## 2.2 Classification of Internet Banks

Generally, there are two categories of full Internet banks. First, there are some traditional banks that decided to expand their activities in the field of Internet banking, including respectable Greek banks like the National Bank of Greece, Alpha Bank or EFG Eurobank-Ergasias. Second, there are pure Web banks, which exist only in the cyberspace and have no physical branches. However, in Greece only the first category of banks exists.

## 2.3 The Development of Internet Banking Services in Greece

Greece has a concentrated banking sector, where the five biggest banks dominate the market. During 2005 their profits exceeded 2.1 billion Euros, which accounts to 1.5% of the Greek GNP- see table below.

	<b>Bank Profits</b>	
	<b>(Biggest 5 in million Euros)</b>	
	<b>2004</b>	<b>2005</b>
<b>National Bank of Greece</b>	441.2	715
<b>Alpha Bank</b>	408	502.2
<b>EFG Eurobank Ergasias</b>	368	501
<b>Piraeus Bank</b>	127.3	263.8
<b>Emporiki Bank</b>	-67	90

Table 4.1: Bank Profits of 5 biggest Greek Banks (Ziotis 2006)

Due to high competition between banks, banking institutions in Greece are seeking to expand market base via Internet banking. On-line banking is evolving rapidly because of the low operating and maintenance costs that are associated with the Internet. Although most Greek banks use static Web sites, which are simply interactive brochures that promote services and products, they can make the banks to close user groups according to their preferences, offer specific products to them and result in a more intense customer commitment.

During the first period of Internet expansion in Greece, most Greek banks had static or interactive Web sites. E-banking first appeared in the Greek market in 1997 but it was adopted by major Greek banks after 1999 (Lymperopoulos et al 2004). For example, Alpha Bank launched a Web site in December 1995, Emporiki Bank in December 1997, Egnatia Bank in February 1998 and EFG Eurobank-Ergasias in May 1998 (Alimonos et al 1998). Nevertheless, Egnatia Bank was the first bank to introduce full Internet banking in 1998. In addition, Alpha Bank started offering full Internet banking services in November 1998, EFG Eurobank-Ergasias in February 2000 and Piraeus Bank in April 2000.

#### 2.4 Cases of Banks using E-banking

Below there is an investigation and brief presentation of the e-banking solutions of five Greek Banks: Alpha Bank, Commercial Bank of Greece, Eurobank, National Bank of Greece and Win Bank.

##### 2.4.1 ALPHA BANK

Alpha Bank has invested in the two-factor authentication using the OTP token technology. Today the authentication of its e-banking retail clients is based on the OATH compatible (OATH) deployment of VASCO Digipass GO 3. It is a token with a simple touch button, which generates a unique one-time password, in every press. For its corporate customers, Alpha Bank invested to a USB token, manufactured by Gemplus (GEMPLUS), so that a digital certificate could be placed in it.

Alpha Bank's e-banking services are classified. Users can use Alpha Bank's information services and receive statements about the balance and the transactions for their accounts providing only their username and password. Providing also an one-time password the users are granted the right to perform transactions involving fund transfers. Moreover, when the fund transfers concern accounts of other banks, the clients should provide a fresh one-time password in every transaction. With regard to corporate customers, Alpha Bank imposes double authorization. One or more of the corporate users initiate the transaction and the legal representative user authorizes the transaction to proceed. The Bank perception of secure e-banking includes also filtered and monitored access to the Bank's systems, protected by the latest security mechanisms. Encryption is also used (SSL 128-bit).

For the future, Alpha Bank considers the incorporation of PKI technologies to its two-factor authentication. Other future mechanisms may include systems that will

demand second level authentication (OTP, PKI, a phrase etc) not beforehand but only when the user's behaviour is abnormal.

#### 2.4.2 COMMERCIAL BANK OF GREECE (EMPORIKI)

Currently, Emporiki Bank's e-banking system uses a single factor authentication based on the combination of a user id and a password. The bank has issued to its customers a high number of smart credit and debit cards. Emporiki Bank has decided to benefit from the distribution of these cards and integrate them to an One Time Password mechanism. The corresponding token (Todos eCode Signature) facilitates event-based mechanisms and smart cards in order to generate one-time passwords. Besides the event – based algorithm, the token also uses the secrets stored in the card chip in order to create and encrypt the password, which is displayed in the token's screen. After that, the user enters the password in an appropriate field of the e-banking application and it is transferred to the eCode server. The eCode server decrypts its input and performs a similar procedure to generate the one-time password. If this matches to the transferred one then the request is enabled.

There is an issue that needs some explanation. How the event counter is synchronized between the eCode signature (token) and the eCode server? The main cause for breaking synchronization is that the user can request a new OTP and never use it. The solution is to set a look-ahead parameter on the server. Synchronization of counters in this scenario simply requires the server to calculate the next event values that exist in the look-ahead window and determine if there is a match. The system may also require the user to send a sequence of OTP values for resynchronization purposes.

A remarkable advantage of using smart card tokens is the simplification of the "logistics" concerning the distribution of the tokens to the e-banking users. There is no need for personalization of the token, as all required secrets (the event counter and the smart card keys) are kept in the smart card. This means that the user can obtain a token from any branch. The same customer can also use more than one token. At the first rollout of the new e-banking version, OTP will only be used as an additional security mechanism, for high-risk transactions. In the future, Emporiki Bank intends to use the eCode system for more complex forms of authorization, as Challenge-Response.

#### 2.4.3 EUROBANK

Eurobank perceives on-line security as a very complex issue since it involves addressing potential risks, which can originate or manifest themselves from either the customer or the financial institution. Therefore, Eurobank has been implemented a combination of technologies, policies & procedures, employee awareness and appropriate enabling organization to secure their e-banking environment. These involve Strict internal processes and security policies, Bank's website verification (via Certificate of Authenticity), Secured data transfers through encryption (128 bit SSL), User's authentication, Secured transactions through digital certificates (PKI), Further enhanced security in high value transactions through USB Digital Certificate tokens (Aladdin), Protected access to the bank's systems by the latest firewall technology,



Intrusion detection systems, Virtual keyboard usage, Personalized transaction limits and Customized transaction workflows.

Another perception of Eurobank is that security cannot be complete unless the customer is aware of basic security behaviour to maintain secure the on-line transactions environment. Therefore, Eurobank aware its customers for safekeeping passwords, verifying websites and protect PCs.

Eurobank, the first and maybe the only Greek Bank engaged PKI, today has the perception that Certificates, especially hardware-based PKI, are the most secure way of doing transactions on internet, however it is less convenient. Now the perception is that security and friendliness should be well balanced. Their strategic decision is to increase the convenience and therefore the attractiveness of e-banking without compromising security by replacing the basic reliance on certificates with a mixture of technical, administrative and operational measures and techniques. At the same time the aim is to build customer trust and perception of security. In this direction, Certificates, OTPs and other identification techniques can be employed to customize appropriately the use of the e-Banking service. The Eurobank's new e-banking system, currently under development, is based on multi-channel architecture where all the above mechanisms are used together with revised transaction limits. Their plans include also adoption of real-time anti-fraud systems, which will analyse user's transactional behaviour and build personalized patterns, allowing real-time control of "suspicious" transactions.

#### 2.4.4 NATIONAL BANK OF GREECE

National Bank of Greece (NBG) provides advanced methods of safeguarding transactions via alternative channels (Internet, Mobile and Phone). They cope with the security of all alternative channels in a united and uniform manner. The security policy that is being applied, guarantees the secrecy and inviolability in transactions. The parameters of security policy focus mainly on User authentication, Transaction authentication (with TANs and lately with OTPs) for each monetary transaction or when important elements are modified, Encryption of data (128 bit encryption), Bank's certification authenticity, Filters of access in the IT systems (Firewalls) and Personalized access / transaction control for corporate customers.

The recently introduced OTP devices of NBG are time-based and they are producing OTPs, which are active for only 32 seconds. For retail customers, NBG introduced the Vasco GO3 (Coresight) device (the brand name NBG uses is e-Code). For the corporate customers, NBG introduced the Vasco DP260 device. It is a small device with numeric keypad, simple 1-button operation and 8-digit LCD screen. The later device is PIN based, for the owner's safety. The owners can also change it at any time. The DP260 initially designed to support also two other functions: signature operation and challenge-response. The NBG considers the utilization of these functions.

NBG, in order to boost the sensation of security for its users, it confirms the transactions by sending back to the user a Host Authentication Code. The host code is a proof of identity of the central system to the user. By pressing once the button of the e-Code device, the user generates a one-time password (6 or 8 digits). The user enters the password to the central system for proofing his identity. The central system then verifies the correctness of this one-time password. If it is valid, the central system calculates the host code (3 digits). The host code is returned to the user who verifies if

it matches the second part shown on his e-Code device (after a second press). Now the user is certain to be logged on to the correct Host and the Host knows to be in contact with the correct user. (Marinakis and Karanikolas, 2007) present the security of NBG's e-banking systems in more detail.

#### 2.4.5 WIN BANK

Win Bank bases its two-factor authentication of customers in the OTP token technology. The RSA SecureID (RSA SecureID) time-based tokens that Win Bank users use to generate one-time passwords embody a USB connector and smart chip. The selected token is a lightweight and extremely easy to use token. It always displays a six digits OTP and without any user intervention (there is no button) renew it every 60 seconds. The passwords can be used only once. Alternatively, Win Bank customers can get an OTP to their predetermined mobile phone number through SMS message.

Win Bank's e-banking services are classified. Users can use Win Bank's information services and also perform money transactions under an upper daily limit of 600 Euros providing only their username and password. For transactions ranging from 600 Euros to 7000 Euros OTP is required. For money transactions cross the limit of 7000 Euros a second OTP is required. The Bank's confrontation of secure e-banking includes also a fraud detection system that is developed in house (Aggelis 2006).

For the future, Win Bank considers the incorporation of PKI technologies to its two-factor authentication mechanism. Towards this vision, Win Bank made the right selection to use tokens that permit to add a digital certificate to the token.

### CONCLUSION

The Internet and the WWW have attracted a great deal of attention during the last years because they are superb channels of displaying information cheaper and more effectively than any other traditional channel. The Net involves communication between computers on networks that allows the users direct communication with each other regardless of time or place factors. As a result, it has become a popular distribution channel. To compete successfully in today's dynamic marketplace and manage the complexities of diverse banking operations, Greek banks must deliver superior value to target customers and be able to adapt in a continuously changing marketplace through market-oriented strategic planning. Fear of losing market share forces financial institutions that do not provide on-line banking to speed up online Internet banking plans. Internet banking is finally progressing in Greece fast. With its low-cost structure, attractive demographics and innovative services, the Internet is going to present a real challenge to traditional forms of banking. Internet banking offers a great deal of advantages both to the banks and to the customers. Clients are becoming more and more demanding and they are expecting even higher levels of service from their bank. On the other hand, Internet banks by offering ease of use,

ease of access, choice and competitive pricing, they add depth and breadth of functionality to meet the expanding needs of their diverse customer base. They increase customer loyalty and cross selling by targeting smaller and smaller groups until ultimately the banks offer tailored products for individual customers.

Four out of the five banks we investigated are basing their two-factor authentication to the OTP token technology, while one out of five banks bases its security to PKI. All banks desire to be able to provide, in parallel with the currently used technology, alternative authorization methods. More specifically, in order to improve their security, two banks out of the four based on the OTP token technology have introduced, for their corporate customers, more sophisticated tokens. In one case the token can produce challenge/response OTPs and in another case a digital certificate can be placed in the token. The other two out of the four banks based on the OTP token technology have introduced from the beginning, and consequently for all of their Internet customers, tokens able to provide alternative authorization methods. In one case the token has the option to produce either challenge/response OTPs or event-based OTPs and in the other case the OTP time-based token can also host a digital certificate. The need for alternative authorization methods is also alive for the bank that bases its security to PKI. In that case the need comes from the perception that OTP tokens are more adoptable from the masses and especially from less educated customers.

Another remarkable point is that Banks are steadily adopting the fraud detection technology or improve their existing fraud detection systems. PKI obtain the interest of more banks but they are expecting to be set up a common PKI CA by the Hellenic Bank Association or some other Institution. As a final conclusion the alternative authorization methods, which banks aim to provide (challenge / response OTPs and PKIs), can satisfy the non-repudiation requirement

To conclude, the potential for on-line banking is present for all banks to utilize. This thesis has shown that the Internet is a unique opportunity and a major channel for distributing banking services in Greece. The banks that stand to gain full advantage of this are the ones who have done their marketing and demographic research and who are able to attract their targeted group by devising interesting and memorable homepages to benefit from the increase in e-banking services.

## REFERENCES

- Aggelis, V. (2006). *Offline Internet Banking Fraud Detection*, 1st International Conference on Availability, Reliability and Security (ARES2006), DAWAM Workshop, Vienna, Austria.
- Aladdin. *eToken Strong Authentication and Password Management*, <http://www.aladdin.com/eToken/default.asp>
- Allan, A., Heiser, J., Litan, A., Newton, A. and Wagner, R. (2006). *State of the Art for Online Consumer Authentication*, Garthner Research G00139254.
- Allan, A. and Litan, A. (2006). *Transaction Verification Complements Fraud Detection and Stronger Authentication*, Garthner Research G00141750.
- Coresight. *VASCO GO3*, <http://www.coresight.com.au/vasco-go3-token.html>
- GEMPLUS. *ID & Security*, [http://www.gemplus.com/pss/id\\_security/](http://www.gemplus.com/pss/id_security/)
- InCard Technologies. *The ICT DisplayCards*, <http://www.incardtech.com/products.html>
- Marinakis, C. and Karanikolas, N.N. (2007). *Strengthening the security of e-banking transactions. The case of NBG*, 11<sup>th</sup> Panhellenic Conference in Informatics, 2007, Patras, Greece.
- OATH. *Initiative for open authentication*, <http://www.openauthentication.org>
- .RSA. *RSA SecureID*, <http://www.rsa.com/node.aspx?id=1156>
- Todos. *eCode Signature*, [http://www.todos.se/Todos/products/products\\_eCode\\_Signature.html](http://www.todos.se/Todos/products/products_eCode_Signature.html)
- Todos. *TAN Reader*, [http://www.todos.se/Todos/products/products\\_TANReader.html](http://www.todos.se/Todos/products/products_TANReader.html)
- Tsai, Chii-Ren (2002). *Non-Repudiation In Practice*, 2<sup>nd</sup> International Workshop on Asia PKI, Taipei, Taiwan, <http://dsns.csie.nctu.edu.tw/iwap/proceedings/proceedings/sessionD/6.pdf>
- Weib, J. (2003). *Mobile TAN*, [http://www.novosec.com/documents/eCommerce\\_MobileTAN\\_en.pdf](http://www.novosec.com/documents/eCommerce_MobileTAN_en.pdf)
- Wikipedia PKI. *Public key infrastructure*, [http://en.wikipedia.org/wiki/Public\\_key\\_infrastructure](http://en.wikipedia.org/wiki/Public_key_infrastructure)
- Wikipedia TAN. *Transaction authentication number*, [http://en.wikipedia.org/wiki/TAN\\_\(banking\)](http://en.wikipedia.org/wiki/TAN_(banking))
- Bank of Greece. <http://www.bankofgreece.gr>

Consumer Internet Barometer

<http://www.consumerinternetbarometer.us/press.cfm>

Αγγέλης, Γ. Βασίλης, “Η Βίβλος του e-banking”, Εκδόσεις Νέων Τεχνολογιών, 2005

Γεωργόπουλος, Πανταζή, Νικολαράκος, Βαγγελάτος, “Ηλεκτρονικό επιχειρείν, προγραμματισμός και σχεδίαση”, Εκδόσεις Μπένου, 2001

Γλύκας, Ξηρογιάννης, “Στρατηγική ηλεκτρονικού επιχειρείν χρηματοπιστωτικών ιδρυμάτων”, Εκδόσεις Ελληνικά γράμματα, 2004

<http://www.uth.gr/main/help/help-desk/internet>

<http://www.technowatch.aueb.gr>

<http://www.observatory.gr>

<http://www.go-online.gr>

<http://www.e-pso.info>

<http://www.hba.gr>

<http://www.webbank.gr>