E-COMMERCE: BARRIERS AND LIMITATIONS

Bogdan Pilawski

Hetmańska 62/7, 60-219 Poznań, Poland
e-mail: bogdan.pilawski@wbk.com.pl

Abstract

This paper concentrates on those threats and limitations, which are capable to impact the development of electronic banking. The various definitions of electronic banking are reviewed. The threats, barriers and limitation likely to affect electronic commerce in general, and electronic banking in particular, are classified initially as internal and external to the organisation. Only the latter are discussed in the paper, for which purpose these are further subdivided into three groups: technical, structural and systemic.

To stay in business banks once again need to re-consider their own position: there is a strong need not to give up on the new opportunities offered by continuous and fast development of new facilities, and to expand into areas entirely new to banking. Otherwise banks could be further pushed to the marginal areas of business, with their operational scope limited to collection and wholesale of money.

Introduction

There are more and more supporters of banking operations and transactions performed at any time around the clock, without physical presence in the bank itself, what is often called "electronic banking". On one hand there is a sheer enthusiasm of followers, on the other – the scepticism and multiple doubts of observers. In fact the banking itself never tolerated hasty actions, which were not thoroughly validated, or even makeshift.

According to British Telecom forecasts, in year 2000 we have reached the number of about 300 million Internet users worldwide. They used Internet to perform transactions of the value of almost 300 billions of US dollars. The market of that size can't be ignored neither by sales people nor by bankers.

The electronic banking, undoubtedly creates numerous conveniences and enables services which were almost unknown yesterday. However it also brings new problems, in the face of which it remains absolutely helpless. There is not a single day without news on an electronic banking system, the security of which has been severely compromised. In most instances these security incidents are to be blamed on banks, which in many instances are very reluctant to admit it. This threat to security of electronic financial transactions is commonly seen as risk of getting the credit card information into wrong hands, while transferred over network. [BT2000] The security

concerns of transactions called "*card not present*" are rarely mentioned, although these constitute significant risk to both buyers and sellers.[1]

Electronic Banking

The terms e-commerce and e-business are often used interchangeably, however the term of e-commerce should be seen rather as synonymous with simply transacting business over the Internet, whereas e-business involves fundamental change to business model in order to transform an organisation into a digitally networked enterprise. [Auer2000] Electronic banking tries to combine both – traditional approach, still supported by many banks' customers, and the most modern, exploiting the latest in technology.

There are many definitions of a phenomenon called electronic banking. These are discussed in detail in [Kard2000]. The views on what is, and what is not an electronic banking, or – in wider sense – electronic commerce, are also presented in [Gospod1999, p.9], [Junge1999, p.18], [JancKot1999, p.67], [Łysak1999, p.24] and [Rogow1999, p.88].

The scope of electronic banking is not limited to contacting a bank via Internet. It includes also other forms, like:

- Traditional phone (directly or via call centre),
- ATM,
- Electronic kiosk,
- POS terminal,
- Personal computer,
- Mobile phone (and equipment of similar functionality),
- Cable TV.

The status of both ends of remotely performed banking operation, that is that of the bank and of its customer, has at least one thing in common: this operation is *impersonal*. To all those taking part in such a transaction it results in some doubt about identity of partners and about their real intentions.

Risks to Electronic Banking

Each activity results in some risk. In the areas of long established tradition (like construction industry) this risk is well known, what allows to control it well and keep its level permanently low.

Stormy and difficult to control development of electronic economy, and the competition accompanying it, results in putting in use of new, immature solutions, which are expected to match from the outset a difficult, and to some extent unknown, operational conditions. There are number of factors increasing the risk involved in that and potential difficulties likely to result:

[1] This subject is discussed in detail in [Pila97b]

- The IT systems are taken out of control of organisations using them, and are introduced into the environment in which this control is limited, and the freedom of choice of time and place of operation on the user side results in existing security measures being ineffective and insufficient,
- The users of a new systems are thousands of people of very diverse knowledge, consciousness, technical and social culture, of different hopes and expectations, usually living in various countries of the world, and speaking various tongues,
- The number of users of a given system in total, and the number accessing it at any particular moment in time is difficult to predict,
- Every single failure, every flaw and above all – every breakdown – immediately becomes commonly known news, usually mercilessly and accurately exploited by competitors.

Another view on risks to any e-commerce activity distinguishes between risks internal and external to the organisation. According to some authors, the cases when external attempts are made to compromise an IT system, are usually well known to the media and – as a result of that – to the public. However there are the quiet internal attacks which result in real, substantial financial losses. [Proct2000]

The openness necessary to be a player in electronic banking becomes source of new threats and limitations, which are further complicated by lack of appropriate technical standards and of legal regulations. One can divide these threats and limitations into three categories: technical, structural and systemic. Examples of these are presented in Table 1.

The said limitations and threats come mainly from weaknesses of equipment and its software, or from the organisation of the process of their usage. These have resulted in e.g. Internet denial of service attacks in the beginning of year 2000. These attacks virtually closed the popular Internet shops (e.g. *Amazon* bookstore) and services (e.g. *CNN*) for number of hours. These attacks have been carefully prepared and – in order to hide individuals behind them – have been carried using computers of other users, which were usually unaware of what was going on. So far there are no effective methods of prevention against attacks of that kind.

The networks of mobile phones were also targets of similar attacks. In Spain a computer virus was detected, capable, while running on Internet connected computers, of sending SMS messages to randomly generated numbers of mobile phones of *Movistar* network, run by mobile operator *Telefonica Moviles*. [see Gdwn2000] The sole reason behind it was to deny access, exactly as in similar Internet attacks. According to some opinions the SIM card software of mobile phones will become the next target of attacks using computer viruses. The growing complexity of those phones and the holes in their software resulting from fast expansion of this area, can lead to development of viruses also in this field.

Spectacular virus attacks with widespread effects and also denial of access type of attacks receive media coverage of unprecedented scale, where those effects are usually significantly exaggerated. This affects public opinion and makes the confidence in Internet security even lower.

Table 1. Classification of electronic banking threats and limitations

Group of limitations	Examples
Technical	Computer viruses Operating systems Application software Unauthorised access to hardware Theft of Internet sites Identity theft Unauthorised access Disclosure of data Removal or replacement of data Data interception Illegal transactions
Structural	Insufficient infrastructure High usage cost Low efficiency Limited accessibility Low security level Operational errors Limited usage Lack of, or immaturity of standards
Systemic	Lack of professionals High implementation costs Struggle to win customer's heart Attempts to eliminate banks from the process of financial transactions

Source: authors design

A relatively new but already common threat is the theft of Internet sites. Theft of this kind results usually from unauthorised changes applied to computer systems handling Internet domain names and associated addresses. Such a change redirects all calls to a particular service to some other service, usually presenting contents insulting by purpose to the original owner of this address. In a manner similar to denial of service attacks one uses here somebody else's computers, and exploits relatively week security of Internet domain name server software. The most popular software of that kind - *Berkeley Internet Name Domain (BIND)* belongs to 10 biggest IT systems security threats specified by *System Administration, Networking and Security Institute* (*SANS*). [Farm2000] Many companies, organisations and government agencies became victims of those thefts in year 2000. Among these were *VISA International, Nike, Goodyear*, governments of *USA, Israel* and *Saudi Arabia*, and also tens of universities around the world.

The available data (www.attrition.org) say, most of identity theft attacks target banks and companies. Such an attack is carried without any knowledge whatsoever of the targeted organisation, and implementation of corrections necessary to restore the proper operation of the

system usually takes couple of hours. During that period of time the potential customers can not access the service they require, and they often find information humiliating to the site owner or insulting to themselves as users of this site.

The data encryption systems are meant to be a protection of data in transfer against interception and substitution. Of two most often used systems one (*Secure Sockets Layer*) is simple and relatively cheap to use, however it protects only the contents of messages while in transfer, and the other (*Secure Electronic Transaction*) which goes well beyond encryption and covers also authorisation of parties of transaction, what, as a matter of fact, means the authorisation of encryption keys used by these parties. Usage of the latter method may eliminate most threats resulting from the de-personalisation of financial electronic transactions. Authenticity of consumer is checked, seller will receive the amount due, but will never gain access to such information, which at later time would allow for another transaction to be carried without any knowledge of the owner of the payment card.[2]

Solution of that kind, known as *Public Key Infrastructure*, allows not only for the identity of both parties of the transaction to be validated, but also provides the means to repudiate that the party have ever entered such a transaction. This constitutes basis of another solution known as *electronic signature.* System of that kind, however, requires also regulatory support and appropriate legal acts, regarding transactions carried that way as binding to the parties, and to regard hand-written and electronic signature as having equal legal force.

The threats to electronic banking (and electronic economy) categorised here as "structural" are behind banks' reach and relate equally to all participants in that area. In many countries some of these threats constitute now severe obstacles to further development in this field.

The undeveloped technical infrastructure not matching the growing needs remains the main menace in that category. This factor results in many consequent limitations and threats. This infrastructure first of all means reliable and resilient connections reaching every single user.

Limited throughput of network connections requires longer period of time to send data across the net, increases the costs involved and limits the availability and effectiveness. All these factors taken together do significantly limit the development of electronic banking in many countries. Making electronic banking available while ignoring these reasons adds insult to injury: frustration of potential customers resulting from access limits (which needs to be paid for anyway) is becoming the major factor resulting in aversion to those services and in lack of confidence in them.

In Poland the network limitations are gradually becoming no. 1 of all limits likely to be faced while attempting to carry electronic transactions. On traditional shopping days (weekends, public and religious holiday periods) the system of electronic retail payments usually becomes totally clogged, leaving many angry customers with transactions on hold and never ending. This is a direct effect of low throughput of the networks available there. In most of those cases an IT

[2] exhaustive but at the same time accessible presentation of history and current state of information encryption is presented in [Kipp2000]

system comes up with message "*No authorisation*", what is easily interpreted as an attempt to wheedle money.

The low cost of Internet banking is often presented as one of major arguments of support to this way of performing financial transactions. This might be true as long as costs of the bank are considered, however the customer sees it the other way: for him major factor is the Internet access cost to bear. In case of e.g. personal computer this cost embraces the proper equipment and software, and also the network access cost, which depends on operator's pricing policy. The effectiveness of the IT system of the bank can also have significant role in this, since it can significantly prolong the connection time to be paid for.

In March 2001 the organisation of leading supermarkets in Poland raised the protest based on Consumer Protection Law against Polish subsidiary of Visa International, and also against Polish Branch of Europay/MasterCard. They claim those two organisations, along with leading Polish banks, maintain pricing cartel and keep charges on electronic transactions on exceptionally high level. While foreign banks charge no more than 1% of transaction value, Polish banks require between 1,7 and 1,85%. According o that source the total cost of handling cash, including insurance and specialised transportation never exceeds 0,25% of its value, and usually stays on the level of 0,12%. In conclusion they say electronic transactions are up to 15 times more expensive than cash deals.[3]

Many banks make a mistake by applying to Internet banking the measures used to evaluate efficiency of traditional branch banking. Systems to serve customers over the Net must be prepared to run with high resilience and to be able to cope easily even with peak loads: this applies to both, to the part under bank's control and equally to the services along the whole path between customer and the bank.

New systems which are tested superficially and to limited extent, and are prematurely launched, become source of spectacular failures. The examples of that are the cases of two British banks – *Prudential* (Internet banking system named *EGG*) in October 1998, and *Abbey National* in June 2000.

In that latter case a new electronic banking system named *Cahoot*, which was to affect young, Internet literate customers, did not stand the load during first day of its operation. Two weeks after this unsuccessful launch system was still inoperable, and the bank and the authoring company were blaming each other for failure.

One of the most serious threats to electronic banking is now the phenomenon called *Identity Theft*. Identity Theft does not mean using someone else's name and number of credit card or bank account, but also exploiting social position of that person, his/her address, banking history, and his/her relations with credit companies, various dealers etc. In classical branch banking environment there is a serious risk for such mystification to be detected at the outset, and there are almost no chances to avoid prosecution. Dealing via phone or Internet brings that risk down to the level where it can be ignored whatsoever. Stealing of identify is a process of gathering identity fragments coming from various sources (healthcare registers, employers records, banking

[3] see: Karty zmonopolizowane, in: Trybuna, p.10, 21/3/2001

files, state and public registers, marketing data etc.). Victims of this kind of crime find it very difficult to defend themselves, since all pieces of information relating to questionable transactions (usually of high value – like purchases of cars, furniture, expensive home utensils, luxury holidays etc.) point to them. T. Arnold of *Cyber Source Corporation* says, a fit crook exploiting security gaps on various levels, and acting over Internet only, can earn some 50 thousand dollars a week. [Arn2000, p.4]

First to be blamed in this case are the banks themselves, which with the aim of gaining customers for any price, neglect appropriate checks and measures of control, and try to make customers to bear consequences of this negligence.

During last year many security holes in software were discovered and revealed. Most of that software was especially designed to serve in e-commerce and in electronic banking applications. The most spectacular of these software weaknesses were:

- Errors in both MS Internet Explorer and Netscape Navigator browsers allowing the external intruder to gain access to discs of computers on which they run, by just using appropriate scripts, and in a way not raising attention of the user of such a computer [Krat2000],
- Unpublished back door in CART32 software, which is used to drive a virtual shopping cart in numerous Internet shops; this back door is protected with constant password, which cannot be changed, and allows for access to all customers passwords and data, like addresses, numbers of credit cards, details of orders past and current, journals of transactions etc. [Lemos2000, Kapp2000]
- Various errors and holes in popular encryption software PGP (Pretty Good Privacy) [Harr2000],
- Possibility of unauthorised access to decrypted form of WAP messages [Nob2000].

Lack of specialist, already painfully felt in many countries, that's the last group of barriers and limitations to development of electronic banking.

This lack of specialist results from electronic banking itself being young discipline, and that has left little opportunity for its workers to gain wider experience. Creating Internet systems has its own specifics and requires different skills than traditional batch or transactional systems. One faces here entirely new design and programming requirements, which didn't exist before. Also different are the methods and rules of testing.

The electronic banking technology is far from cheap. The data often presented at various occasions, showing low cost of electronic transactions, are usually limited to current operational costs only. However to become operational one needs to make huge investments, and to gain appropriately high number of users to bring expected returns. Bearing in mind all the limitations already discussed here this is not an easy task, and the return is rather slow. E.g. Hewlett-Packard says to start a banking WAP service requires spending some half a million US dollars per every hundred customers in categories of hardware, software and organisational undertakings. This needs to be extended with operational costs, risk higher than average and with requirement to stay abreast with fast changing technology and maturing standards.

The attempts to make electronic banking profitable as soon as possible lead strait to the phenomenon called struggle for winning customer's heart. In electronic banking for this purpose one uses not only traditional methods of collection and analysis of data on customers and their behaviours, but also marketing, technical and organisational means. This enters entirely new areas, like e.g. micro-payments via mobile phones. During Spring 2000 a facility of this kind was offered by British mobile operator *BT Cellnet*. Similar, but limited in scope, services are available to customers of *Virgin Mobile* in the US (e.g. purchase in this way of an airline ticket of *Virgin Airlines* gives a 10% discount).

The effects of these activities are creating a direct menace to banks: the mobile operators attempt to enter payments for purchases of that kind directly onto their own bills, and to handle all financial clearing operations involved themselves, bypassing banks altogether. Virgin Mobile predicts that after full expansions of necessary technologies, the opportunity will arise to eliminate from that process not only retail banks, but also organisations like *Visa International* and *Master Card*. The operators of mobile telephony are proud to run the most sophisticated billing systems ever designed, and they claim it is easy for them to extend these systems with further facilities, to enable them to handle payments for goods and services. The clearing operations involved may become a huge source of income on the payments themselves, let alone the interest on huge financial turnover involved.

Close

In the past banks have already lost the battle with supermarket chains and large stores. These organisations began with binding the customers on benefits of loyalty cards, and gradually became credit institutions, financing the instalment purchases in its own stores, and providing customers with credits for daily shopping. Some car manufacturers go even further. They have raised specialised banks of their own to finance car purchases, and also travel bureaux and travel insurance companies.

The banks need to reconsider whether they are to give up further areas of what once was their sole and reserved territory, and limit their activity to financial guarantors and wholesalers, or will they overcome their aversion, and – exploiting infrastructure in hand and opportunities offered by electronic economy – will go far beyond the market of purely financial services.

Literature

[Arn2000] Arnold, Tom, Internet Identity Theft, The Software & Information Industry Association, Washington DC, 2000

[Auer2000] Hackbarth, Garry, Kettinger, William J., Building an e-business Strategy, Auerbach Publications, September 2000

[BBC2000] BBC (Internet Service), Security glitch at BT broadband, 28/4/2000

[Bobe2000] Bobecki, Ryszard, Zatkane komputery polskiej nauki, Przegląd tygodniowy, 5/4/2000, s. 20

[BT2000] British Telecom, BT TrustWise - Securing Your Web Site For Business, April 2000

[Chan2000] Chan, Karen, Podłączanie komórek do Internetu otworzy puszkę Pandory?, The Wall Street Journal of Europe, loco "Gazeta wyborcza", 19/6/2000
[Cov2000] Cover, Robin, The Essence and Quintessence of XML. Retrospects and Prospects, 31/12/1998, www.oasis-org.html
[CW2000a] WAP's double whammy, Computer Weekly, 23/3/2000
[CW2000b] Mobile banking will eradicate the need to queue, Computer Weekly, 16/3/2000
[DePalma] DePalma, Donald A., Profiting from the Global Web, Idiom Inc., Cambridge (USA), 2000
[e-handel] e-handel, IT Supplement of "Polityka" weekly, 18/3/2000
[Farm2000] Farmer, Melanie, Agency lists top 10 security threats, CNET News, 2/6/2000, http://news.cnet.com
[Gdwn2000] Goodwins, Rupert, Mobile phone viruses are coming, 8/6/2000, http://www.zdnet.co.uk/news/2000/22/ns-15867.html
[Good1996] Goodell, Jeff, Hacker i samuraj, Gdańskie Wydawnictwo Psychologiczne, 1996
[Good2000] Goodspeed, Peter, The new space invaders, National Post Online, 19/2/2000
[Gospod1999] Gospodarowicz, Andrzej, Zastosowania rozwiązań informatycznych w bankowości - Wstęp, Wydawnictwo Akademii Ekonomicznej, Wrocław, 1999, s.9
[Gray2000] Gray, Douglas F., Group pursues mobile e-commerce, IDG News Service, 11/4/2000
[Harr2000] Harrison, Ann, Flaw found in PGP 5.0, serwis Computerworld, 26/5/2000
[Hayes2000] Hayes, Ian, Ensuring IT Is E-Business Ready, Cutter Consortium, Arlington, 2000
[ISTF2000] Internet Security Task Force, Initial Recommendations For Conducting Secure eBusiness, ISTF, 1/3/2000
[JancKotl1999] Janc, Alfred, Kotliński, Grzegorz, Determinanty wykorzystania bankowości elektronicznej w rozwoju wybranych usług bankowych, in: Gospodarowicz, Andrzej (ed.), Zastosowania rozwiązań informatycznych w bankowości, Wydawnictwo Akademii Ekonomicznej we Wrocławiu, 1999, s. 66
[Junge1999] Locarek-Junge, Herman, Electronic Banking in Germany: the Past, the Present and the Future, in: Gospodarowicz, Andrzej (ed.), Zastosowania rozwiązań informatycznych w bankowości, Wydawnictwo Akademii Ekonomicznej we Wrocławiu, 1999, s. 13
[Kane2000a] Kane, Margaret, Security hole found in Eudora, ZDNet Service, 28/4/2000
[Kane2000b] Kane, Margaret, New flaw discovered in Microsoft Hotmail, ZDNet Service, 10/5/2000
[Kapp2000] Kappelman, Leon A., Backdoor in e-commerce software exposes credit cards, Year2000-discuss Service, 28/4/2000
[Kard2000] Kardaras, Dimitris, Business to Customers E-Commerce Implications in Banking in the UK and Greece, in: Abramowicz W. i Orlowska M.E. (editors), Business Information Systems 2000, Springer Verlag, 2000, s. 255
[Kipp2000] Kippenhahn, Rudolf, Tajemne przekazy - szyfry, Enigma i karty chipowe, Prószyński i S-ka, Warszawa, 2000
[Krat2000] Kratofil, Bruce, New Explorer and Netscape Browser Vulnerabilities, ZDNet Service, 21/4/2000
[Lemos2000] Lemos, Robert, Beware shopping cart's backdoor!, ZDNet, Service, 27/4/2000
[Łysak1999] Łysakowski, Paweł, Fundamenty rozwoju bankowości elektronicznej - prace Rady Bankowości Elektronicznej przy Związku Banków Polskich, in: Gospodarowicz,

Andrzej (ed.), Zastosowania rozwiązań informatycznych w bankowości, Wydawnictwo Akademii Ekonomicznej we Wrocławiu, 1999, s. 24

[MIT1997] Laubacher, Robert J., Malone, Thomas W. oraz MIT Scenario Working Group, Two Scenarios for 21st Century Organizations: Shifting Networks of Small Firms or All-Encompassing "Virtual Countries"?, Massachusetts Institute of Technology - Sloan School of Management, Working Paper 21C WP #001, Cambridge (USA), 1997

[Nob2000] Nobel, Carmen, Hype aside, WAP has worries, PC Week, 10/3/2000

[Pila97a] Pilawski, Bogdan, Dziś za wcześnie, jutro za późno... czyli handel i banki w sieci Internet, Marketing-Serwis Monthly, nr 3, March 1997, s. 6-12

[Pila97b] Pilawski, Bogdan, Ostrożnie - Internet!, Marketing-Serwis Monthly, nr 7, June 1997, s. 12-15

[Press2000] Pressman, Roger S., Can WebApps Be Engineered?, E-ssentials!, nr 18, May 2000

[Proct2000] Proctor, Paul E., The Practical Intrusion Detection Handbook, Prentice Hall, July 2000

[PrBank] Prawo Bankowe, Ustawa z dnia 29 sierpnia 1997, Dz.U. Nr 140, poz. 939

[Reut2000] Reuter, Microsoft planted secret password in software, ZDNet e-WEEK Service of 14/4/2000

[Ricc2000] Ricciuti, Mark, Taking sides on XML, Serwis CNET News, 26/5/2000

[Rohde2000] Rohde, Laura, BT Cellnet takes lock off WAP market, IDG Net Service, 22/6/2000

[Rogow1999] Rogowski, Grzegorz, Społeczeństwo informacyjne jako jedno z najważniejszych wyzwań dla zarządzania strategicznego bankiem w XXI wieku, in: Gospodarowicz, Andrzej (ed.), Zastosowania rozwiązań informatycznych w bankowości, Wydawnictwo Akademii Ekonomicznej we Wrocławiu, 1999, s. 86

[Sayer2000] Sayer, Peter, Telco Must Stop Selling WAP Phones - for Now, 23/5/2000, www.thestandard.net

[Spinks2000] Spinks, David, BTSecurity Breach, E-COM-SEC Discussion List, 2/5/2000

[Stank2000] Stankiewicz, Piotr, Szyfry, hasła i cyfrowe podpisy, “Rzeczpospolita” z 14/7/2000, “Moje pieniądze” Supplement

[Sull2000] Sullivan, Eamonn, Workers face more mature threat from bigger worms, PC Week, 11/5/2000, http://www.zdnet.com/pcweek

[Tasch2000] Taschek, John, The basic failure of XML is its premise, Serwis ZDNet, 23/4/2000

[WAP1998] Wireless Application Protocol Forum Ltd., Wireless Application Protocol - Architecture Specification, version of 30-Apr-1998

[Wong2000] Wong, Wylie, Industry consortium launches XML site, CNET News Service, 20/6/2000