

E-BANKING – IMPACT, RISKS, SECURITY

Tittrade Cristina

*Universitatea Româno Americană, B-dul Lacul Tei, nr 71, bl 18, sc B, et. 2, ap. 55, sector 2, Bucuresti,
Tel : 0762985187, e-mail: cristina_titrade@yahoo.com*

Ciolacu Beatrice

Universitatea Româno Americană, e-mail : beatrice_ciolacu@yahoo.com

Pavel Florentina

Universitatea Româno Americană, e-mail: pav_florentina@yahoo.com

The evolution of electronic banking (e-Banking) started with the use of automatic teller machines (ATMs) and has included telephone banking, direct bill payment, electronic fund transfer and online banking. According to some, the future direction of e-banking is the acceptance of mobile telephone (WAP-enabled) banking and interactive-TV banking. However, it has been forecast by many that online banking will continue to be the most popular method for future electronic financial transactions.

Electronic funds transfer (EFT), refers to the computer-based systems used to perform financial transaction electronically. The term is used for a number of different concepts including electronic payments and cardholder-initiated transactions, where a cardholder makes use of a payment card such as a credit card or debit card. Card-based EFT transactions are often covered by the ISO 8583 series of standards.

Keywords : e-banking, e-commerce, e-banks.

Introduction

In order for customers to use their banks online services they need to have a personal computer and Internet connection. Their personal computer becomes their virtual banker who will assist them in their banking errands. Examples of e-banking services that customers can get online are:

- Attaining information about accounts and loans,
- Conducting transfers amongst different accounts, even between external banks,
- Paying bills,
- Buying and selling stocks and bonds by depot,
- Buying and selling fund shares³⁹

These services that are offered by e-banking are changing and being improved because of the intense competition between the banks online. Banking industry must adapt to the electronics age, which in its turn is changing all the time.

EFT transactions require authorisation and a method to authenticate the card and the card holder. Whereas a merchant may manually verify the card holder's signature, EFT transactions require the card holder's PIN to be sent online in an encrypted form for validation by the card issuer. Other information may be included in the transaction, some of which is not visible to the card holder (for instance magnetic stripe data), and some of which may be requested from the card holder (for instance the card holder's address or the CVV2 security value printed on the card).

EFT transactions are activated during e-banking procedures. Various methods of e-banking include:

- Telephone banking
- Online banking
- Short Message Service (SMS) banking
- Mobile banking
- Interactive-TV banking .

Independent of location or time, you can execute your payments and stock market orders and you get detailed information on your accounts and custody accounts.

Impact of e-banking on traditional services

One of the issues currently being addressed is the impact of e-banking on traditional banking players. After all, if there are risks inherent in going into e-banking there are other risks in not doing so. It is too early to have a firm view on this yet. Even to practitioners the future of e-banking and its implications are unclear. It might be convenient nevertheless to outline briefly two views that are prevalent in the market.

The view that the Internet is a revolution that will sweep away the old order holds much sway. Arguments in favour are as follows:

- E-banking transactions are much cheaper than branch or even phone transactions. This could turn yesterday's competitive advantage - a large branch network, into a comparative disadvantage, allowing e-banks to undercut bricks-and-mortar banks. This is commonly known as the "beached dinosaur" theory.
- E-banks are easy to set up so lots of new entrants will arrive. 'Old-world' systems, cultures and structures will not encumber these new entrants. Instead, they will be adaptable and responsive. E-banking gives consumers much more choice. Consumers will be less inclined to remain loyal.
- E-banking will lead to an erosion of the 'endowment effect' currently enjoyed by the major UK banks. Deposits will go elsewhere with the consequence that these banks will have to fight to regain and retain their customer base. This will increase their cost of funds, possibly making their business less viable. Lost revenue may even result in these banks taking more risks to breach the gap.

Portal providers, are likely to attract the most significant share of banking profits. Indeed banks could become glorified marriage brokers. They would simply bring two parties together – eg buyer and seller, payer and payee.

The products will be provided by monolines, experts in their field. Traditional banks may simply be left with payment and settlement business – even this could be cast into doubt.

Traditional banks will find it difficult to evolve. Not only will they be unable to make acquisitions for cash as opposed to being able to offer shares, they will be unable to obtain additional capital from the stock market. This is in contrast to the situation for Internet firms for whom it seems relatively easy to attract investment.

There is of course another view which sees e-banking more as an evolution than a revolution.

E-banking is just banking offered via a new delivery channel. It simply gives consumers another service (just as ATMs did).

Like ATMs, e-banking will impact on the nature of branches but will not remove their value.

Traditional banks are starting to fight back.

The start-up costs of an e-bank are high. Establishing a trusted brand is very costly as it requires significant advertising expenditure in addition to the purchase of expensive technology (as security and privacy are key to gaining customer approval).

E-banks have already found that retail banking only becomes profitable once a large critical mass is achieved. Consequently many e-banks are limiting themselves to providing a tailored service to the better off.

Nobody really knows which of these versions will triumph. This is something that the market will determine. However, supervisors will need to pay close attention to the impact of e-banks on the traditional banks, for example by surveillance of:

- strategy
- customer levels
- earnings and costs
- advertising spending
- margins
- funding costs

- merger opportunities and threats.

Risks

Strategic Risk - A financial institution's board and management should understand the risks associated with e-banking services and evaluate the resulting risk management costs against the potential return on investment prior to offering e-banking services. Poor e-banking planning and investment decisions can increase a financial institution's strategic risk. On strategic risk E-banking is relatively new and, as a result, there can be a lack of understanding among senior management about its potential and implications. People with technological, but not banking, skills can end up driving the initiatives. E-initiatives can spring up in an incoherent and piecemeal manner in firms. They can be expensive and can fail to recoup their cost. Furthermore, they are often positioned as loss leaders (to capture market share), but may not attract the types of customers that banks want or expect and may have unexpected implications on existing business lines.

Banks should respond to these risks by having a clear strategy driven from the top and should ensure that this strategy takes account of the effects of e-banking, wherever relevant. Such a strategy should be clearly disseminated across the business, and supported by a clear business plan with an effective means of monitoring performance against it.

Business risks - Business risks are also significant. Given the newness of e-banking, nobody knows much about whether e-banking customers will have different characteristics from the traditional banking customers. They may well have different characteristics. This could render existing score card models inappropriate, this resulting in either higher rejection rates or inappropriate pricing to cover the risk. Banks may not be able to assess credit quality at a distance as effectively as they do in face to face circumstances. It could be more difficult to assess the nature and quality of collateral offered at a distance, especially if it is located in an area the bank is unfamiliar with (particularly if this is overseas). Furthermore as it is difficult to predict customer volumes and the stickiness of e-deposits (things which could lead either to rapid flows in or out of the bank) it could be very difficult to manage liquidity.

Of course, these are old risks with which banks and supervisors have considerable experience but they need to be watchful of old risks in new guises. In particular risk models and even processes designed for traditional banking may not be appropriate.

Transaction/operations risk - Transaction/Operations risk arises from fraud, processing errors, system disruptions, or other unanticipated events resulting in the institution's inability to deliver products or services. This risk exists in each product and service offered. The level of transaction risk is affected by the structure of the institution's processing environment, including the types of services offered and the complexity of the processes and supporting technology.

In most instances, e-banking activities will increase the complexity of the institution's activities and the quantity of its transaction/operations risk, especially if the institution is offering innovative services that have not been standardized. Since customers expect e-banking services to be available 24 hours a day, 7 days a week, financial institutions should ensure their e-banking infrastructures contain sufficient capacity and redundancy to ensure reliable service availability. Even institutions that do not consider e-banking a critical financial service due to the availability of alternate processing channels, should carefully consider customer expectations and the potential impact of service disruptions on customer satisfaction and loyalty.

The key to controlling transaction risk lies in adapting effective policies, procedures, and controls to meet the new risk exposures introduced by e-banking. Basic internal controls including segregation of duties, dual controls, and reconcilements remain important. Information security controls, in particular, become more significant requiring additional processes, tools, expertise, and testing. Institutions should determine the appropriate level of security controls based on their assessment of the sensitivity of the information to the customer and to the institution and on the institution's established risk tolerance level.

Credit risk - Generally, a financial institution's credit risk is not increased by the mere fact that a loan is originated through an e-banking channel. However, management should consider additional precautions when originating and approving loans electronically, including assuring management information systems effectively track the performance of portfolios originated through e-banking channels. The following aspects of on-line loan origination and approval tend to make risk management of the lending process more challenging. If not properly managed, these aspects can significantly increase credit risk.

- Verifying the customer's identity for on-line credit applications and executing an enforceable contract;
- Monitoring and controlling the growth, pricing, underwriting standards, and ongoing credit quality of loans originated through e-banking channels;
- Monitoring and oversight of third-parties doing business as agents or on behalf of the financial institution (for example, an Internet loan origination site or electronic payments processor);
- Valuing collateral and perfecting liens over a potentially wider geographic area;
- Collecting loans from individuals over a potentially wider geographic area;
- Monitoring any increased volume of, and possible concentration in, out-of-area lending.

Liquidity, interest rate, price/market risks - Funding and investment-related risks could increase with an institution's e-banking initiatives depending on the volatility and pricing of the acquired deposits. The Internet provides institutions with the ability to market their products and services globally. Internet-based advertising programs can effectively match yield-focused investors with potentially high-yielding deposits. But Internet-originated deposits have the potential to attract customers who focus exclusively on rates and may provide a funding source with risk characteristics similar to brokered deposits. An institution can control this potential volatility and expanded geographic reach through its deposit contract and account opening practices, which might involve face-to-face meetings or the exchange of paper correspondence. The institution should modify its policies as necessary to address the following e-banking funding issues:

- Potential increase in dependence on brokered funds or other highly rate-sensitive deposits;
- Potential acquisition of funds from markets where the institution is not licensed to engage in banking, particularly if the institution does not establish, disclose, and enforce geographic restrictions;
- Potential impact of loan or deposit growth from an expanded Internet market, including the impact of such growth on capital ratios;
- Potential increase in volatility of funds should e-banking security problems negatively impact customer confidence or the market's perception of the institution.

Reputational risks - This is considerably heightened for banks using the Internet. For example the Internet allows for the rapid dissemination of information which means that any incident, either good or bad, is common knowledge within a short space of time. The speed of the Internet considerably cuts the optimal response times for both banks and regulators to any incident.

Any problems encountered by one firm in this new environment may affect the business of another, as it may affect confidence in the Internet as a whole. There is therefore a risk that one rogue e-bank could cause significant problems for all banks providing services via the Internet. This is a new type of systemic risk and is causing concern to e-banking providers. Overall, the Internet puts an emphasis on reputational risks. Banks need to be sure that customers' rights and information needs are adequately safeguarded and provided for.

Security

Security is one of the most discussed issues around e-banking.

E-banking increases security risks, potentially exposing hitherto isolated systems to open and risky environments.

Security breaches essentially fall into three categories; breaches with serious criminal intent (fraud, theft of commercially sensitive or financial information), breaches by 'casual hackers' (defacement of web sites or 'denial of service' - causing web sites to crash), and flaws in systems design and/or set up leading to security breaches (genuine users seeing / being able to transact on other users' accounts). All of these threats have potentially serious financial, legal and reputational implications.

Many banks are finding that their systems are being probed for weaknesses hundreds of times a day but damage/losses arising from security breaches have so far tended to be minor. However some banks could develop more sensitive "burglar alarms", so that they are better aware of the nature and frequency of unsuccessful attempts to break into their system.

The most sensitive computer systems, such as those used for high value payments or those storing highly confidential information, tend to be the most comprehensively secured. One could therefore imply that the

greater the potential loss to a bank the less likely it is to occur, and in general this is the case. However, while banks tend to have reasonable perimeter security, there is sometimes insufficient segregation between internal systems and poor internal security. It may be that someone could breach the lighter security around a low value system.

It is easy to overemphasise the security risks in e-banking. It must be remembered that the Internet could remove some errors introduced by manual processing (by increasing the degree of straight through processing from the customer through banks' systems). This reduces risks to the integrity of transaction data (although the risk of customers incorrectly inputting data remains). As e-banking advances, focusing general attention on security risks, there could be large security gains.

Financial institutions need as a minimum to have:

- a strategic approach to information security, building best practice security controls into systems and networks as they are developed
- a proactive approach to information security, involving active testing of system security controls (e.g. penetration testing), rapid response to new threats and vulnerabilities and regular review of market place developments
- sufficient staff with information security expertise
- active use of system based security management and monitoring tools
- strong business information security controls.

These are the issues line supervisors will be raising with their banks as part of their on-going supervision.

Conclusion

In conclusion e-banking creates issues for banks and regulators alike. For their part, banks should:

- Have a clear and widely disseminated strategy that is driven from the top and takes into account the effects of e-banking, together with an effective process for measuring performance against it.
- Take into account the effect that e-provision will have upon their business risk exposures and manage these accordingly.
- Undertake market research, adopt systems with adequate capacity and scalability, undertake proportional advertising campaigns and ensure that they have adequate staff coverage and a suitable business continuity plan.
- Ensure they have adequate management information in a clear and comprehensible format.
- Take a strategic and proactive approach to information security, maintaining adequate staff expertise, building in best practice controls and testing and updating these as the market develops. Make active use of system based security management and monitoring tools.
- Ensure that crisis management processes are able to cope with Internet related incidents.

One of the benefits that banks experience when using e-banking is increased customer satisfaction. This due to that customers may access their accounts whenever, from anywhere, and they get involved more, this creating relationships with banks.

Banks should provide their customers with convenience, meaning offering service through several distribution channels (ATM, Internet, physical branches) and have more functions available online. Other benefits are expanded product offerings and extended geographic reach. This means that banks can offer a wider range and newer services online to even more customers than possible before.

The benefit which is driving most of the banks toward e-banking is the reduction of overall costs. With e-banking banks can reduce their overall costs in two ways: cost of processing transactions is minimized and the numbers of branches that are required to service an equivalent number of customers are reduced.

With all these benefits banks can obtain success on the financial market. But e-banking is a difficult business and banks face a lot of challenges.

Bibliography:

1. Business Objects Learning Solution to Power e-Business Intelligence, Editura Business Objects, 2001
2. AFZENI PAOLO, STEFANO CERI, „Database Systems”, Ed. McGraw-Hill, 1999.
3. AVERACE CHRISANTHI, TONY CARNFORD, „Developing Information Systems. Concepts, Issues and Practice”, Ed. Macmillan Press, 1993.
4. Adamson C. , Venerable M. Data Warehouse Design Solutions, Editura, Wiley, 1998
5. Berry J. A. M. , Linoff G. Data Mining Techniques: Marketing, Sales and Customer Support, Editura Wiley, 1997.