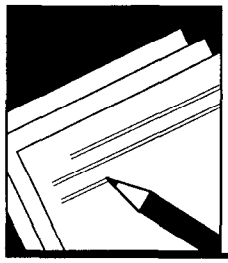
PDP/02/6



IMF Policy Discussion Paper

Issues in Electronic Banking: An Overview

Andrea Schaechter

INTERNATIONAL MONETARY FUND

 PDP/02/6

IMF Policy Discussion Paper

Monetary and Exchange Affairs Department

Issues in Electronic Banking: An Overview [1]

Prepared by Andrea Schaechter

Authorized for distribution by Piero Ugolini

March 2002

Abstract

Using electronic delivery channels for banking services and products has become increasingly popular in recent years. Electronic banking makes it possible to offer banking services around the world 24 hours a day. The dependence on technology for providing the services with the necessary security, and the cross-border nature of transactions, involve additional risks for banks and new challenges for banking regulators and supervisors. This paper provides an overview of some of the issues resulting from the development of electronic banking and how they are currently being addressed by regulatory and supervisory authorities.

JEL Classification Numbers: G21; G28

Keywords: electronic banking, banking regulation, banking supervision

Author's E-Mail Address: aschaechter@imf.org

---

[1] The author appreciates helpful suggestions and comments from Richard Abrams, Philip Bartholomew, Warren Coats, Jesper Dockir (Danish Financial Services Authority), Vassili Prokopenko, Marc Quintyn, Gareth Rees (United Kingdom Financial Services Authority), Mark Zelmer, and participants in an internal IMF seminar held on November 15, 2001.

I. INTRODUCTION

While electronic banking in the form of automatic teller machines and telephone banking has been around for a number of years, the popularity of accessing banking services through the Internet and mobile phones is rising. Increasingly, not only basic services are offered—such as balance inquiry, funds transfer and bill payments—but also loan and credit card applications, foreign exchange transactions, new accounts as well as brokerage, fiduciary, and insurance services. It goes without saying that e-banking provides vast opportunities for banks and their customers. Access to services and products is fast and available around the clock independent of the location of the customer. The electronic delivery channels increase transparency and can lead to higher competition among banks, and a most significant point—through lower costs,[2] penetrating new markets and expanding the geographical reach (International Monetary Fund, 2001). The digitalization of transactions can help reduce costs for banks and increase efficiency. While it can be expected that bank products become more standardized, there are also incentives to introduce new bank products.

Along with new business opportunities and benefits for customers from electronic banking, though, come various risks that must be addressed by bank management and the regulatory and supervisory authorities.[3] Due to drastically lower transaction costs and ease of activities, cross-border transactions should be increased beyond the existing phone banking activities and face-to-face operations with nonresidents. The key issue for banking supervisors

---

[2] Estimates indicate that a typical customer transaction costing about one U.S. dollar in a branch or through a phone call would cost just about two cents online (Claessens, Glaessner, and Klingebiel, 2000).

[3] The Bank for International Settlements through its Basel Committee for Banking Supervision (BCBS) has formed an "Electronic Banking Group" that aims at facilitating analysis and dialogue among supervisors to develop a prudential supervisory framework for e-banking activities, and has recently issued two volumes on these matters (See BIS, 2000 and 2001).

is how to ensure effective supervision of operations both in their own market (as host supervisor) when services are provided from abroad, and in foreign markets when the bank is licensed in the home jurisdiction. Both issues are not new, given the continuously rising importance of cross-border transactions, but can take on even more significance in the case of e-banking. A new, or considerably more pronounced aspect with which supervisors are faced, arises from the reliance on technology for the delivery channel of providing e-banking services and products. This paper provides an overview of the challenges faced by regulators and supervisors from e-banking and how they are currently being addressed by discussing the following issues: (i) authorization; (ii) cross-border supervisory issues; (iii) risk management; (iv) money laundering; and (v) consumer protection and education.

II. DEFINITIONS

Electronic banking can be defined as the use of electronic delivery channels for banking products and services, and is a subset of electronic finance.[4] The most important electronic delivery channels are the Internet, wireless communication networks, automatic teller machines (ATMs), and telephone banking. Internet banking is a subset of e-banking that is primarily carried out by means of the Internet. The term transactional e-banking is also used to distinguish the use of banking services from the mere provision of information.[5]

---

[4] See BCBS (2001): "... Electronic banking, or e-banking, includes the provision of retail and small value banking products and services through electronic banking channels as well as large value electronic payments and other wholesale banking services delivered electronically."

[5] Sometimes Internet banking is defined as a subset of PC banking, which also includes online banking. In contrast to Internet banking, online banking refers to bank transactions within closed networks (Deutsche Bundesbank, 2000).

Electronic banking services are offered in two main ways:[6] Either traditional brick and mortar banks combine traditional and electronic delivery channels (brick and click banks) or banks offer their products and services only—or predominantly—through electronic distribution channels without having a branch network (other than a physical presence as an administrative head office or nonbranch facilities such as kiosks or ATMs). These banks are called "virtual banks," "branchless," or "Internet-only" banks. Withdrawal and deposit of funds may be made through ATMs or other remote delivery channels owned by these virtual banks or other institutions. Setting up licensed virtual banks can, in principle, be done in three ways. First, they can be established as a new independent virtual bank obtaining a license from the banking regulator. Second, existing banks can create virtual banks as separately capitalized banks within a bank holding company structure. And third, a conventional bank can be recast into a virtual bank under its existing charter. An alternative approach is establishing a virtual bank through the creation of trade name virtual banks. These are established as independently operating divisions of existing banks without a separate charter.

Closely related to e-banking activities are products of electronic money. Definitions of e-money used by official bodies vary, mainly due to continuous technical innovations. The BIS (1998) defines e-money as "stored value or prepaid payment mechanisms for executing payments via point of sale terminals, direct transfers between two devices, or over open computer networks such as the Internet" (BIS, 1998).[7] E-money therefore differs from e-banking, since balances are not kept in financial accounts with financial institutions

---

[6] Most definitions and distinctions in the following two paragraphs are based on Furst, Lang, and Nolle (2000).

[7] In the 1998 report of the European Central Bank on electronic money, it is defined as an "electronic store of monetary value on a technical device that may be widely used for making payments to undertakings other than the issuer without necessarily involving bank accounts in the transaction, but acting as a prepaid bearer instrument."

(Bartholomew, Mason, and Shull, 1997). Issues for banking supervisor result from the different aspects on how banks can be involved in e-money activities. Banks can, for example, be the issuer or distributor of e-money. They can also be involved in maintaining records, processing, clearing, and settlement of e-money transactions. This paper does not address these risks and supervisory issues related to e-money, but focuses entirely on e-banking.

III. Some Data

Little detailed data on e-banking activities has been compiled and published. The main reason is the lack of reporting requirements that would explicitly distinguish e-banking activities from other delivery channels. Data published in the IMF *International Capital Markets* report (August, 2001) and Claessens, Glaessner, and Klingebiel (2001) indicate that the provision of internet banking is particularly high in Austria, Finland, Korea, Singapore, Spain, Sweden, and Switzerland, where more than 75 percent of all banks offer Internet banking (informational or transactional). Internet banking is particularly popular in the Scandinavian countries that have the highest customer user ratios with up to one-third of bank customers in Finland using Internet bank services. In most countries, Internet banking is provided through new business lines or branches of traditional brick and mortar banks rather than through separately licensed virtual banks.

The main characteristics of Internet banking activities in the United States are the following. They are based on responses to questionnaires compiled by OCC examiners for active national banks chartered in the fourth quarter of 2000, and the third quarters of 2000 and 1999. An overview of some of the results is presented in Furst, Lang, and Nolle (2000, 2001a, 2001b). At end-2000, Internet banking was concentrated in the largest banks. While 62 percent of all national banks had websites, only 37 percent offered transactional Internet banking. This

is a rapid increase from 20 percent in the third quarter of 1999.[8] The banks that offer transactional Internet banking accounted for over 90 percent of national banking system assets. Moreover, 18 percent of national banks had concrete plans to offer Internet banking by end-2001. Larger banks tended to offer a wider array of e-banking services, including loan applications and brokerage services. While most consumers in the United States have their accounts with banks that offer Internet banking services, consumer use has remained limited to about 4 percent.[9]

The number of virtual banks remains relatively low. As of July 2001, there were nine separately chartered virtual banks and about 20 trade name virtual banks operating in the United States (Furst, Lang, and Nolle, 2000; OCC http://www.occ.treas.gov/netbank/ibi.htm). Asia saw the launch of the first two virtual banks in 2000 and 2001.[10] The European Union has several virtual banks operating, either as separately licensed banks or as subsidiaries or branches of brick and mortar banks.[11]

---

[8] Of the 10,000 U.S. banks and thrifts, approximately one-third had websites in the third quarter of 1999, out of which 1,100 were transactional websites.

[9] The results of a similar survey for the 202 banks supervised by the Luxembourg supervisory authority [Commission de Surveillance du Secteur Financier (CSSF)] were published in its 2000 Annual Report. They indicate that 38 percent of all banks have websites, but only 7 percent of the banks offer transactional Internet banking. Thirteen percent of banks are planning to introduce this service.

[10] MEVAS bank is Hong Kong SAR's first virtual bank. Bank of Singapore operates finatiq.com for retail customers and finixis.com for business customers. These are however not separately chartered.

[11] Examples are Merita Bank (Finland), Santander Direct Bank (operating in Spain, Germany, and Brazil) and Advance Bank (Germany). Some of the subsidiaries licensed in Germany as banks are actually direct brokers, which under the German system are regarded as a special type of direct banks.

IV. Challenges for Banking Regulators and Supervisors

This section provides an overview on how electronic banking exacerbates some of the traditional bank risks, in particular operational, reputational, and legal risks, and the need for increased cross-border cooperation among bank supervisors.[12] It also summarizes how these issues are currently addressed by a number of regulators and supervisors.

A. Authorization

Issuing licenses for virtual banks is often based on the same or similar conditions for virtual and brick and mortar banks. Some banking supervisors and regulators have amended their laws or adopted new regulations to address the specific nature of electronic banking activities and associated risks.[13] Box 1 provides an example of guidelines for the authorization of virtual banks in Hong Kong SAR. Locally incorporated virtual banks must have a physical presence in Hong Kong, through the conversion of an existing locally incorporated authorized institution, which is at least 50 percent owned by a well-established bank or other supervised financial institution. An overseas-incorporated virtual bank that wishes to establish itself in Hong Kong in branch form must come from a country where there is an established regulatory framework for electronic banking. This last point indicates that the concerns of under what circumstances the activities of a virtual bank should require a license, how the supervisor can identify these circumstances, and how any circumvention can be prevented are more critical than the question of what are the licensing conditions. Since these questions are all related to the supervision of cross-border activities, they are addressed in the following section.

---

[12] These aspects are, for example, discussed in BIS (1996, 1998, 2000, 2001), Parker (2001), and Sergeant (2000).

[13] For an overview of international approaches see Reserve Bank of India (2001).

Box 1: Hong Kong Monetary Authority: Authorization of Virtual Banks

Summary of Guidelines Issued by the Hong Kong Monetary Authority on May 5, 2000

General principles

1. The HKMA will not object to the establishment of virtual banks in Hong Kong provided that they can satisfy the same prudential criteria that apply to conventional banks.
2. A virtual bank that wishes to carry on banking business in Hong Kong must maintain a physical presence here.
3. A virtual bank must maintain a level of security that is appropriate to the type of business that it intends to carry out.
4. A virtual bank must analyze the nature of the particular types of risk to which it is exposed and put in place appropriate policies, procedures and controls to deal with these risks.
5. A virtual bank must be able to present a business plan, which strikes an appropriate balance between the desire to build market share and the need to earn a reasonable return on assets and equity.
6. A virtual bank must set out clearly in the terms and conditions for its service what are the rights and obligations of its customers.
7. Virtual banks may outsource their computer operations to a third party service provider provided that the principles in the MA's guidelines on outsourcing are complied with.

Principles applicable to locally incorporated virtual banks

1. In line with existing authorization policies, a locally incorporated virtual bank cannot be newly established other than through the conversion of an existing locally incorporated authorized institution.
2. A locally incorporated virtual bank should be at least 50 percent owned by a well-established bank or other supervised financial institution in good standing in the financial community and with appropriate experience.

Principles applicable to overseas-incorporated virtual banks

1. An overseas-incorporated virtual bank that wishes to establish itself in Hong Kong in branch form must come from a country where there is an established regulatory framework for electronic banking.
2. An overseas-incorporated virtual bank must have total assets of more than USD16 billion.
3. An overseas-incorporated virtual bank will be subject to the "three-building"1/ condition in respect of its physical offices, but not in respect of its cyber network.

Source: Hong Kong Monetary Authority, 2000a (http://www.info.gov.hk/hkma/eng/guide/index.htm).

1/ According to the "Three-Building" Condition, overseas-incorporated banks licensed in or after 1978 and overseas-incorporated restricted licensed banks authorized in and after 1990 may maintain offices in not more than three buildings.

B. Cross-Border E-Banking Supervisory Issues

Various supervisory issues emerge from cross-border e-banking activities. Table 1 summarizes the different types of bank/customer relationships that all call for international cooperation in banking supervision. Cases A to D are scenarios that also apply to brick and mortar banks, but may be accentuated when these banks also offer cross-border e-banking

services. Cases E to H refer to cross-border activities of virtual banks that raise additional regulatory and supervisory questions.

Table 1. Types of Bank/Customer E-Banking Relationships

Licensed: / Type of bank:	Home		Abroad	
	Onshore	Offshore	Onshore	Offshore
Brick and click	A	B	C	D
Virtual	E	F	G	H

Recommendations on how to supervise cross-border banking activities of brick and mortar banks have been made by the Basel Committee on Banking Supervision (BCBS) through the Bank for International Settlements (BIS) in its 1996 paper on "The Supervision of Cross-Border Banking" and in the minimum standards set up in 1992.[14] In the case of home country institutions providing banking services to customers outside the country, the home country supervisor should be responsible for oversight of the banking organization on a consolidated basis. The host supervisor's oversight is limited to the bank's activities conducted in the local market. The BCBS also recommends that the home country supervisor should provide host supervisors with information on how they oversee the activities. In case the host supervisor has concerns about the effectiveness about the home supervisors oversight, bilateral cooperative arrangements should be undertaken.

Most supervisors require licensing from virtual banks in all countries in which they provide services. This is a way to bring activities of virtual banks under the supervision of each host country with the objective to protect local residents and the local banking system. This is particularly relevant, in cases where the supervision and cooperation with the home supervisor are not adequate. In essence, virtual banks might need to be required to establish a

[14] BIS (1996); and BIS (1992). For a few country examples on supervisory approaches to cross-border activities see also OECD (2000).

network of licensed virtual, or possibly brick and mortar, branches in each country in which they offer banking services and take deposits. This practice is required, for example, in most of the countries of the European Union and the United States. Should a virtual bank that is licensed outside these jurisdictions wish to offer e-banking services and take deposits in these countries, it must first establish a licensed branch.[15] This criterion is not only used for virtual banks, but also for foreign brick-and-mortar (click) banks that explicitly target a domestic customer base. Most commonly, however, offshore banks use this practice (see below).

Determining when a bank's virtual services trigger the need for a license in a particular country or territory can be more difficult in case of Internet services than for brick and mortar banks. For example, a virtual bank licensed in country X would not be considered as taking deposits in country Y if customers make their deposits by posting checks to an address in country X. The option to make deposits at ATMs in country Y, however, would most likely be considered as deposit taking in country Y.

Some indicators showing where and from where banking services are provided are mailing addresses, languages, and advertisements.[16] As mentioned in the previous paragraph, a mailing address can indicate where a bank is taking deposits and from where it operates. Another indicator can be the language in which customers are addressed on the web page. Mailing addresses and languages would be revealed on the banks' website, and also possibly in advertisements that are specifically targeted at nonresident customers. Supervisors need to address these issues and establish clear rules, since the borderlines between these cases are not clear-cut. The actual conduct of supervising virtual banks is the same as that of brick and

[15] The common market in the European Union allows banks licensed in one member state to set up branches in other member states without further licensing requirements.

[16] For example, Bank of France (2000) proposes a set of indicators intended to assess the real intention of a bank to provide banking services in a country.

mortar banks with on-site inspections taking place in the administrative head offices of the virtual banks, but additional supervisory attention is given to the risks that are exacerbated in e-banking (see Section C).

Since offshore banking has the potential of being less regulated than onshore banking (Erico and Musalem (1999) and IMF (2000a)), virtual offshore banking could increase the range of insufficiently regulated activities. If offshore banks target customers of the home supervisor, the home supervisor is faced with the challenge to decide when a service is no longer solely provided in the offshore center but in the home country.[17] Such services would then have to be prohibited or put under standard onshore regulation, since effective banking supervision would call for applying the same prudential regulations and supervisory procedures to onshore and offshore banking in the domestic market.

Providers outside banks increasingly provide and operate e-banking technology. The reliance on these providers not only adds another dimension of risk that needs to be considered by banks and supervisors, but can also necessitate further cross-border cooperation among supervisors if these providers are located outside the home country.

C. Risk Management

Operational, reputational, and legal risks are risk categories mostly affected by the specific nature of e-banking activities. The BCBS stresses that the management of these risks should become an integral part of the banking institution's overall risk management framework. In that respect, the BCBS recently published through the BIS (May 2001)

---

[17] Even if they only provide strictly offshore services, it should be made clear that licensed offshore banks are not supervised by the home country, and the home country offers no protection to depositors in such banks.

14 principles of risk management for e-banking that provide guidance to promote safe and sound e-banking activities (see Box 2).[18]

Box 2: Basel Committee for Banking Supervision: Risk Management Principles for Electronic Banking

(May 2001)

Board and Management Oversight

Principle 1: The Board of Directors and senior management should establish effective management oversight over the risks associated with e-banking activities, including the establishment of specific accountability, policies and controls to manage these risks.

Principle 2: The Board of Directors and senior management should review and approve the key aspects of the bank's security control process.

Principle 3: The Board of Directors and senior management should establish a comprehensive and ongoing due diligence and oversight process for managing the bank's outsourcing relationships and other third-party dependencies supporting e-banking.

Security Controls

Principle 4: Banks should take appropriate measures to authenticate the identity and authorization of customers with whom it conducts business over the Internet.

Principle 5: Banks should use transaction authentication methods that promote non-repudiation and establish accountability for e-banking transactions.

Principle 6: Banks should ensure that appropriate measures are in place to promote adequate segregation of duties within e-banking systems, databases and applications.

Principle 7: Banks should ensure that proper authorization controls and access privileges are in place for e-banking systems, databases and applications.

Principle 8: Banks should ensure that appropriate measures are in place to protect the data integrity of e-banking transactions, records and information.

Principle 9: Banks should ensure that clear audit trails exist for all e-banking transactions.

Principle 10: Banks should take appropriate measures to preserve the confidentiality of key e-banking information. Measures taken to preserve confidentiality should be commensurate with the sensitivity of the information being transmitted and/or stored in databases.

(continued)

[18] While these principles are presented under three main headings ("Board and Management Oversight," "Security Controls," "Legal and Reputational Risk Management"), this paper discusses issues by risk category.

Legal and Reputational Risk Management

Principle 11: Banks should ensure that adequate information is provided on their websites to allow potential customers to make an informed conclusion about the bank's identity and regulatory status of the bank prior to entering into e-banking transactions.

Principle 12: Banks should take appropriate measures to ensure adherence to customer privacy requirements applicable to the jurisdictions to which the bank is providing e-banking products and services.

Principle 13: Banks should have effective capacity, business continuity and contingency planning processes to help ensure the availability of e-banking systems and services.

Principle 14: Banks should develop appropriate incident response plans to manage, contain and minimize problems arising from unexpected events, including internal and external attacks, that may hamper the provision of e-banking systems and services.

Operational risk

The central use of new technology to provide e-banking services has important implications on banks' operational risk. This new technology may require changes in procedures supervisors use to ensure that banks properly manage their e-banking risks in the areas of security, data confidentiality, data and system integrity, system availability, and outsourcing. These risk factors are also closely linked to reputational and legal risks for banks, since, for example, breaches of securities can have damaging effects on the reputation of a bank, while also having legal consequences. For virtual banks, which conduct their entire business through electronic distribution channels, these risks are paramount.[19] In many countries in which e-banking activities have gained importance, bank supervisors have put in place internal guidance notes for examiners and, in a number of cases, released risk management guidelines for banks.[20] Some of the main aspects considered to significantly

[19] Nonetheless, also traditional brick and mortar banks rely to a large extend on technological systems and can face large operational risks.

[20] See for example Bank of France (2000), Belgian Banking and Finance Commission (2000), United States, Federal Deposit Insurance Corporation (1998), Hong Kong Monetary Authority (1998, 2000b, 2000c), Monetary Authority of Singapore (2001), and United States, Office of the Comptroller of the Currency (1999, 2001).

contribute to operational risk from e-banking are summarized below (for more details see also BIS 1998 and 2001).

Security is considered the central operational risk of e-banking. Threats can come from inside and outside the system. They include unauthorized access to the system through, for example, "back doors," "brute force," "hijacking," "sniffing," or "spoofing" to retrieve and use confidential consumer information, add customer assets, subtract customer liabilities, or interrupt operations.[21] Similarly, "denial of service" attacks and injecting a virus can disrupt services and affect integrity of information.

Security practices involve combinations of hardware and software tools, administrative procedures and personnel management function to maintain secure systems and operations (Monetary Authority of Singapore 2001). Human resource management must ensure that personnel involved in maintaining and operating the websites and systems is adequately trained in security practices. Basic internal security principles include: the "never alone principle," "segregation of duties," and the "access control principle" (Monetary Authority of Singapore, 2001). Some of the principal security practices consist of properly configured firewalls, strong encryption technology and authentication techniques, sound password

[21] Some of the security threats include: "back doors" which are pieces of program code written into applications or operating systems to grant programmers access to programs without the need to go through the normal security controls; "brute force" attack, which is a technique to capture encrypted messages and then use software to break the code and gain access to messages, user IDs, or passwords; "hijacking," an attack in which a connection is stolen after a victim has authenticated himself or herself to the system; "sniffing," which involves the use of a software program that is illicitly inserted somewhere on a network to capture user passwords as they pass through the system; and "spoofing," which refers to an attempt to gain access to a system by posing as an authorized user. The Hong Kong Monetary Authority (2000c) provides an overview of these and other common types of online attacks and examples of possible preventive measures. See also United States, Office of the Comptroller of the Currency (1999) and BIS (2000) for these definitions.

policies, procedures to accept traffic only from authorized sources, adequate backup and recovery arrangements, and updated virus scanning tools. These practices should regularly be tested and reviewed by outside experts to analyze the network vulnerabilities and recovery preparedness.

Security measures must ensure the confidentiality of data, as well as the integrity of the system and data. The first refers to ensuring that data is not being accessed or transmitted by unauthorized sources. The latter refers to the accuracy, reliability and completeness of information processed stored or transmitted between banks, their customers, and external service providers. Internal controls and audits, and supervisory examination, are crucial to detect and correct any security risks. A shortage of skills and expertise in this area could easily become a potential risk.

In addition to security, system availability is an essential criteria to limit operational and reputational risk for banks. To take full advantage of the potential benefits of e-banking services, systems should be available on a 24-hour basis. In addition, reliable performance, fast response time, and swift recovery capability are crucial. Capacity planning is also important to address increasing transaction volumes and new technological developments. This includes considerations about the budgetary impact of new investments, the availability to attract staff with the required technological expertise, and potential dependence on external service providers.

Increasing reliance on outsourcing can add substantially to banks' operational risk. Outsourcing not only introduces an additional security threat, it can also have a major impact on the data and system integrity and availability. Conducting appropriate due diligence, ensuring the adequacy of contracts governing e-banking, developing appropriate contingency plans, and monitoring the ongoing viability of third party services—particularly when these are new firms with no track record—must become part of banks' risk management (BIS 2001).

On the other hand, outsourcing also can be cheaper and more efficient if the service provider has more expertise in the task than the bank in question. This could result in less operational risk and cheaper service for the bank and ultimately consumers.

Reputational Risk

Reputational risk is considerably increased through e-banking. If a bank fails to deliver secure, accurate and timely services on a consistent basis, its reputation is at risk. In addition to system availability and integrity, breaches in data confidentiality and any other glitches to the security of operations can damage a bank's reputation (BIS, 1998, 2000; OCC, 1999).

For banks that rely entirely or predominantly on electronic delivery channels, reputational risk can be higher than for traditional brick-and-mortar banks. Problems that are encountered in one e-bank can potentially affect other e-banking service providers if customers loose confidence in electronic delivery channels as a whole or view bank failures as being related to supervisory deficiencies in the system. Bilateral cooperation between the home and host country supervisors is crucial to minimize the risk of a country's reputation being affected by a (virtual) bank failing as a result of activities in an inadequately supervised host country. Increased reputational risk from e-banking also accentuates the need to have crisis management plans and procedures at hand in case of loss of confidence in e-banking. Problems experienced in e-banking can also have negative effects on the reputation of related activities and firms. For the banking system as a whole, however, there seems to be no systemic risk from e-banking as long as the share of virtual banks continues to be rather low.

Legal Risk

Legal risks can also arise from e-banking. Virtual banks can potentially expand the geographical scope of their services faster than traditional banks. In some cases, however, the banks might not be fully prepared and lack sufficient resources to become entirely familiar

with the local laws and regulations before they begin to offer services in a new jurisdiction, either as a licensed branch or without license if this is not required. In the latter case, legal risk can be heightened should the lack of contact between the virtual bank and the host country supervisor result in the virtual bank being uninformed and unaware of regulatory changes. Violations of customer protection laws, including data collection and privacy, and regulations for soliciting could be important issues.[22]

There are two other important sources of legal risk. First, there can be uncertainty about which legislation applies to e-banking transactions—the legislation of the jurisdiction in which the (virtual) bank is licensed or in which the services are offered. Both legislations might conflict with each other. And second, as a consequence of this, also enforcement can be difficult. Moreover, enforcement of certain emerging areas of law is uncertain, for example, laws related to electronic contracts and digital signatures (BIS, 2000).

Other Risks

The use of electronic delivery channels for banking activities also has implications for other traditional banking risks such as strategic and business risk, credit risk, liquidity risk, market risk, and foreign exchange risk.

Offering e-banking services is a decision that involves **strategic and business risk.** The highly sophisticated technology involved in e-banking, the rapid technological developments, the lack of importance of borders for banking activities and competition, and the newness of e-banking are elements that distinguish the risk nature of e-banking from other strategic decisions. Predictions regarding business opportunities are still highly uncertain given

[22] For an example of good practices for legal risk management see the Bank of France's white paper (2000) entitled "Internet. The Prudential Consequences." (http://www.banque-france.fr/gb/infobafi/main.htm).

the newness of e-banking. Competition is global and customers can easily, and might be more ready to, switch to a different bank should they not be fully satisfied with the services provided. To build a customer base, virtual banks tend to price very competitively, an issue that warrants supervisors' attention. Investment in technology can involve significant start-up costs and in this case, timing is critical since a bank wants to acquire up-to-date and widely used technology. Adequate expertise and resources to identify, monitor, and control e-banking also must be available. Technology and e-banking services have to become a coherent part of the bank's business and strategy. Supervisors must ensure that management of banks are aware of the risks involved in e-banking and carefully assess their strategic options so that the added uncertainties may be compensated by additional returns.

Expanding the geographic range of customers through e-banking and the lack of face-to-face customer relations can affect **credit risk**. E-banking allows banks to reach customers around the world, but it also can make the credit risk analysis process more difficult if specific information about countries and their business environment are less well known and understood. The lack of personal relations between bank personnel and customers can have particularly important implications for credit risk analysis.[23] However, a broader geographic range of customers may also result in better diversification of loan portfolio, which would reduce credit risk contained in each institution.

E-banking can also have an impact on **liquidity risk**. Higher volatility can be caused by customers who maintain accounts solely on the basis of rates—a tendency that can already be observed as clients become better educated and more rate sensitive. Increased monitoring by supervisors may be warranted. Greater liquidity may be required for virtual banks than for

[23] In general, banks offering Internet services in regions or countries with which they are not familiar, face greater risks, whether they be political, social, economic, or legal.

traditional banks, should the liquidity risk be perceived as considerably higher than for traditional banks. Supervisors also need to ensure that banks have sufficient collateral that could be used to obtain temporary liquidity support.

In principle, the central bank's lender-of-last-resort role should apply in the same manner to virtual banks as to brick and mortar banks. Temporary central bank loans should only be provided against collateral to solvent but illiquid virtual banks that are licensed in the home country. Lending to a virtual bank that is at risk of insolvency should only be considered for systemically important banks, and then subject to enhanced supervision and restriction. Preferably, though, fiscal resources should be used to dealing with insolvent systemically important banks.

The impact of e-banking on **market risk** is ambiguous. On the one hand, increasing securities issuance and trading over the internet could potentially increase the volatility in prices, causing banks that create or expand deposit brokering, loan sales, or securitization program as a result of internet banking activities to be at greater risk. On the other hand, rising trading volumes in securities would also raise their liquidity. Supervisors need to assess the effects on individual banks and how these banks manage the resulting risks (BIS, 2000).

E-banking should not have any impact on **foreign exchange risks**. Even though some banks might be in a position to accept more deposits in foreign currency and/or grant foreign currency loans to an increasingly international customer base, it is the ability to hedge any positions that determines the foreign exchange risk, regardless of the positions' origin. However, hedging foreign exchange risks for less traded currencies might be at substantial costs and need to be considered in the bank's cost analysis.

D. Money Laundering

E-banking, in particular Internet banking, can potentially be misused for money laundering. The report of the Financial Action Task Force (FATF) 1999–2000 summarizes the main implications of Internet banking for money laundering. The lack of face-to-face contact with customers is the major concern. It represents the obvious trade-off between the benefits of electronic banking on the one hand and concerns about potential misuse on the other hand. This danger is, however, not unique to internet banking, but also present for every brick and mortar bank that offers completely dematerialized and automated transfers, deposits, and withdrawals of cash without any contact with bank staff. Once an account has been opened, it is impossible for banks to identify whether a transaction is being carried out by the nominal account holder and from where the transaction is taking place.

Several countries have issued regulations or guidelines on customer identification to combat money laundering in the absence of face-to face contact. While in a number of countries, regulations already in place for postal or telephone banking have been applied in the same way for Internet banking (e.g., the United States and the United Kingdom), some countries have issued additional recommendations. In the United Kingdom, guidance issued to financial sector firms on non face-to-face verification of identity and address, requires them to use a combination of checks, for example, the Register of Electors; making a credit reference agency search; requesting sight of a current signed passport, driving license, a recent bill or local authority tax bill; bank or building statement. It is also possible for firms to rely upon certified copies of documents. In cases where physical recognition seems to be impossible to implement, the Bank of France (2000) makes recommendations for additional verification steps including asking for additional documents as proof of customer's identity to open customer accounts in France. These could, for example, include photocopies of both sides of an identity card or passport, two original pay slips, the original of the latest gas and electricity

bill, a bank identification form or a cancelled cheque. In its memo on prudential requirements for Internet financial services, Belgium's Banking and Finance Commission (2000) notes that additional attention is required for client identification without face-to-face contact. In Spain, on-line banking services are restricted to customers who have already been identified in a traditional relationship with their bank.

Monitoring on-line transactions requires great vigilance. The measures suggested are similar to those used to combat money laundering through conventional banking activities, but require more attention since they can take place around the clock. Particularly, fully automated transactions make it extremely difficult to detect money-laundering activities in a timely enough manner that their execution can still be suspended. Banks should draw up an account activity profile for each customer to spot abnormalities in transactions. Criteria for suspicious transactions include, for example, transfers made from or to specific areas, especially the non-cooperative countries and territories identified by the FATF. However, e-banking facilitates disconnecting transactions from specific locations. Other criteria to detect money laundering are unusually large amounts or series of transactions, which seem to be broken down into smaller payments that do not exceed a reporting threshold.

The FATF (2000) notes that another concern of money laundering through e-banking relates to the regulatory or investigative jurisdiction that might be involved in detecting and ultimately pursuing money laundering violations. The global nature of e-banking makes it even more important to coordinate legislation and regulation internationally to avoid the creation of safe havens for criminal activities. The FATF therefore recommends working toward uniformity of standards among jurisdictions.

E. Consumer Education and Protection

Customer education on security risks and precautions can play an important role for consumer protection and for limiting reputational risk. Security risks can be heightened when a consumer does not understand the necessary security precautions and misuses them inadvertently. Banks should therefore provide prominent and easy-to-understand advice to customers on the importance of security precautions and concerning personal privacy policies. This guidance should be understood before any e-banking services are activated.

For supervisors, assisting in the educational process and requiring banks to raise consumer awareness can become a key means to help protect consumers. A number of supervisory authorities view education as part of their mandate to consumer protection and have increased their efforts in that respect.[24] The U.S. FDIC, for example, provides a link on its website that allows customers to identify online banks with legitimate charters and FDIC insurance (http://www.fdic.gov/bank/individual/online/index.html). It also issues tips on internet banking, offers consumer help lines, and issues official memoranda as special alerts warning of specific entities that may be conducting unauthorized banking operations in the United States and Canada (http://www.fdic.gov/bank/individual/online/fils.html).

V. Summary and Conclusions

While electronic banking can provide a number of benefits for customers and new business opportunities for banks, it also poses new challenges for banking regulators and supervisors:

---

[24] See for example statements by Davies (2000).

- The cross-border nature of activities calls for intensified cross-border cooperation between supervisors.

- Traditional banking risks are exacerbated, in particular operational, reputational, and legal risks as a result of the technology dependence and the global forum for activities. Supervisors therefore need to ensure that risk management practices for electronic banking become an integral part of banks' risk management policies.

- Amplified risks in electronic banking also result from: (i) the dependence on a relatively small number of highly specialized providers of technology; and (ii) the potential of contagion if customers lose confidence in these technologies and the security of e-banking operations.

- Electronic banking also has the potential to create new opportunities for criminal activities and facilitate others, such as money laundering. In that context, strictly applying policies such as "know-your-customer policies" and vigilantly monitoring e-banking transactions become increasingly important. Moreover, customer education on security risks can play an important role for consumer protection and, at the same time, limit reputational risk.

References

Bank for International Settlements Basel Committee on Banking Supervision, 1992, *Minimum Standards for the Supervision of International Banking Groups and their Cross-Border Establishments* (Basel), http://www.bis.org/publ/bcbsc004.htm#v3d4.

———, 1996, *The Supervision of Cross-Border Banking*, October (Basel), http://www.bis.org/publ/bcbs27.htm.

———,1998, *Risk Management for Electronic Banking and Electronic Money Activities*, March (Basel), http://www.bis.org/publ/bcbs35.htm.

———, 2000, "Electronic Banking Group Initiatives and White Papers," October (Basel), http://www.bis.org/publ/bcbs76.htm.

———, 2001, "Risk Management Principles For Electronic Banking," May (Basel), http://www.bis.org/publ/bcbs82.htm.

Bank of France, 2000, "Internet. The Prudential Consequences," White Paper of the Banque de France and the General Secretariat of the Commission Bancaire (Paris), http://www.banque-france.fr/gb/infobafi/main.htm.

Bartholomew, Phillip, Joseph R. Mason, and Bernhard Shull, 1997, "Monetary Aspects of Electronic Money," paper presented at the Annual Meetings of the Western Economic Association in Seattle (July 11).

Belgium Banking and Finance Commission, 2000, "Financial Services Via The Internet: Prudential Requirements," May 5 (Brussels), http://www.cbf.be/mov.htm.

Claessens, Stijn, Thomas Glaessner, and Daniela Klingebiel, 2000, "Electronic Finance: Reshaping the Financial Landscape Around the World," The World Bank, Financial Sector Discussion Paper No. 4 (September).

———, 2001, "E-Finance in Emerging Markets: Is Leapfrogging Possible?" The World Bank, Financial Sector Discussion Paper No. 7, June (Washington).

Commission de Surveillance du Secteur Financier (Luxembourg), 2001, Annual Report 2000.

Davies, Howard, 2000, "The Transformation of Financial Services Regulation: Facing up to Markets Without Borders," Financial Service Authority, United Kingdom, Speech held at the 2000 Global Internet Summit, George Mason University, March 13 (Washington), http://www.fsa.gov.uk/pubs/speeches/sp42.html.

Deutsche Bundesbank, 2000, "Electronic Banking from a Prudential Supervisory Perspective," Monthly Report, December (Frankfurt), http://www.bundesbank.de/index_html_en.htm.

Erico, Luca and Alberto Musalem, 1999, "Offshore Banking: An Analysis of Micro- and Macroprudential Issues," IMF Working Paper 99/5 (Washington: International Monetary Fund).

European Central Bank, 1998, "Report on Electronic Money," (Frankfurt), http://www.ecb.int/pub/pub01.htm.

Financial Action Task Force on Money Laundering, 2000, "Report on Money Laundering Typologies 1999–2000," February (Basel) http://www.oecd.org/fatf/FATDocs_en.htm.

Financial Services Authority United Kingdom, 2001, "The FSA's Approach to the Regulation of E-Commerce," June (London) http://www.fsa.gov.uk/pubs/discussion/dp6.dpf.

Furst, Karen, William E. Lang, and Daniel E. Nolle, 2000, "Who Offers Internet Banking?" in *OCC Quarterly Journal*, Vol. 19, No. 2, June (Washington) pp. 29–48, http://www.occ.treas.gov/netbank/r&a.htm.

———, 2001a, "Internet Banking in the U.S.," in *Capco Journal of Financial Transformation*, September (http://www.occ.treas.gov/netbank/r&a.htm).

———, 2001b, "Internet Banking: Market Developments and Regulatory Issues," May, http://www.occ.treas.gov/netbank/r&a.htm.

Group of Ten, 1997, "Electronic Money. Consumer Protection, Law Enforcement, Supervisory and Cross Border Issues," Report on the Working Party on Electronic Money, Bank for International Settlement, Basel, (April).

Hong Kong Monetary Authority, 1998, "Outsourcing," Letter from December 8, http://www.info.gov.hk/hkma/eng/guide/circu_date/981208.htm.

———, 2000a, *Authorization of Virtual Banks. A Guideline Issued by the Monetary Authority Under Section 16(10) of the Banking Ordinance*, May 5, http://www.info.gov.hk/hkma/eng/guide/guide_no/20000505e_index.htm.

———, 2000b, *Management of Security Risks in Electronic Banking Services*, July 6 (Hong Kong), http://www.info.gov.hk/hkma/eng/guide/circu_date/200007061_index.htm.

———, 2000c, *Annex 1 to Management of Security Risks in Electronic Banking Services. Examples of Common Types of Online Attacks and Possible Preventive and Detective Measures*, July 6 (Hong Kong), http://www.info.gov.hk/hkma/eng/guide/circu_date/200007061_index.htm.

International Monetary Fund, 2000a, "Offshore Financial Centers. The Role of the IMF," June 23 (Washington: International Monetary Fund), http://www.imf.org/external/np/mae/oshore/2000/eng/role.htm.

———, 2000b, "Offshore Financial Centers," IMF Background Paper (Washington: International Monetary Fund), June 23, 2000 (http://www.imf.org/external/np/mae/oshore/2000/eng/back.htm).

———, 2001, *International Capital Markets. Developments, Prospects, and Key Policy Issues*, (Washington: International Monetary Fund).

Monetary Authority of Singapore, 2001, "Internet Banking, Technology Risk Management Guidelines," (February), http://www.mas.gov.sg/singfinsec/index.html.

Organisation for Economic Co-operation and Development, 2000, "Cross Border Trade in Financial Services: Economics and Regulation," Steering Group Under the Committee on Financial Markets, in: OECD Financial Market Trends, No. 75, pp. 23–60, March (Paris), http://www.oecd.org/daf/financial-affairs/markets/.

Parker, Peter, 2001, "E-Commerce and Regulation: The Perspectives of the Financial Service Authority (FSA)," Financial Service Authority, United Kingdom, speech held on March 2001.

Reserve Bank of India, 2001, Report on Internet Banking, June 22, http://www.rbi.org.in/index.dll/21?sectionhomepage?s1secid=9999&s2secid=9999.

Sergeant, Carol, 2000, "E-Banking: Risks and Responses," Financial Service Authority, United Kingdom, speech held on March 29, 2000, http://www.fsa.gov.uk/pubs/speeches/sp46.html.

United States, Federal Deposit Insurance Corporation, 1998, *Electronic Banking. Safety and Soundness Examination Procedures*, June (Washington), http://www.fdic.gov/regulations/information/electronic/elecbank.pdf.

United States, Office of the Comptroller of the Currency, 1999, *Internet Banking. Comptroller's Handbook*, October (Washington), http://www.occ.treas.gov/netbank/ebguide.htm.

———, 2001, *Comptroller's Corporate Manual. The Internet and the National Bank Charter*, January (Washington), http://www.occ.treas.gov/netbank/ebguide.htm.