CBFA

BANKING, FINANCE AND INSURANCE COMMISSION

Circular CBFA_2009_17 of 07/04/2009

Financial services via the Internet: Prudential requirements

Scope:

Credit institutions, insurance companies, investment firms and management companies of undertakings for collective investment and Belgian branches of these institutions which are governed by the law of a state that is not a member of the European Economic Area (EEA). The circular is also to be brought to the attention of institutions established in Belgium that are governed by the law of an EEA Member State.

Summary/Objective:

The first part of this circular addresses the basic principles that serve as a frame of reference for the CBFA in assessing the appropriateness of the organization put in place by financial institutions that offer services via the Internet. In particular, it will examine the risks as well as the requirements with regard to organization and internal control. Compliance with the rules of conduct will then be discussed, as will the potential impact of cross-border transactions via the Internet.
In the second part, provided in annex, attention will be paid specifically to sound practices regarding the management of Internet security risks.

Dear Sir or Madam,

1. Rationale

Credit institutions, insurance companies, investment firms and management companies of undertakings for collective investment, hereafter referred to collectively as "financial institutions", must have an organization appropriate to their activities[1].

Many such financial institutions offer financial services via the Internet, allowing their clients to request information, carry out transactions and communicate with their institution.

This circular contains a number of recommendations and explains the most important provisions in the existing regulatory and prudential framework that apply specifically to the provision of financial services via the Internet.

These recommendations are based partly on a number of international standards[2] on risk management that can be a useful frame of reference for Belgian practice.

In an annex to this document, we set out sound practices specifically for managing security risks relating to financial services via the Internet.

---

1 See Articles 20 and 20*bis* of the Law of 22 March 1993 (credit institutions), Article 14*bis* of the Law of 9 July 1975 (insurance companies), Articles 62 and 62*bis* of the Law of 6 April 1995 (investment firms). For management companies of undertakings for collective investment, see Article 153 of the Law of 20 July 2004 on certain forms of collective management of investment portfolios.

2 Electronic Banking Group of the Basel Committee on Banking Supervision, "Risk Management Principles for Electronic Banking" (July 2003) and "Management and Supervision of Cross-Border Electronic Banking Activities" (July 2003).

The CBF's Circular D1 2000/2 of 5 May 2000 on financial services via the Internet addressed to credit institutions and investment firms is hereby abrogated.

2. Scope

A. Ratione personae

The sound management practices in question apply to credit institutions, insurance companies, investment firms and management companies of undertakings for collective investment governed by Belgian law.

They also apply to Belgian branches of credit institutions, insurance companies, investment firms and management companies of undertakings for collective investment that are governed by the law of a state that is not a member of the EEA.

Notwithstanding the competence of the home supervisors as regards the supervision of the organization and internal control of a financial institution, it seems useful to bring the recommendations contained in this circular to the attention of branches of financial institutions governed by the law of other EEA Member States. They can be used as a guide to the CBFA's supervision of these branches.

B. Ratione materiae

The prudential requirements pertain to both information and advice offered via the Internet and the Internet services offered by financial institutions allowing their clients to consult and/or manage their data and to carry out transactions.

Financial institutions generally use various types of websites for this purpose. Thus, in addition to purely informational websites describing the financial institution and its range of services and products, and interactive websites with educational and simulation functions, there are also transactional websites that make it possible to carry out financial transactions such as transferring funds, making payments, accessing credit, taking out insurance policies, managing information or buying or selling investment instruments.

A characteristic of financial Internet services is that communication between clients and their financial institution, whether for accessing information, consulting the client's financial situation or carrying out transactions, take place via the Internet. The Internet services used in the process are for the most part, and increasingly, automated from beginning to end ("straight through processing") without human intervention; this makes it essential that the necessary internal (client identification, account status, possession of the securities sold, limits, etc.) and external (compliance of the transaction with the market rules or payment infrastructure concerned) controls be built into the Internet services. This necessity is further reinforced by the increasing tendency for transactions such as stock exchange and payment transactions to take place in real time, meaning that the time available to carry out these controls is extremely limited.

Because of the attendant risks, transactional services via the Internet demand the utmost attention from a prudential perspective.

3. Prudential requirements

A. Starting points and risks attendant on offering financial services via the Internet

Financial institutions that offer or conduct financial services via the Internet must - as when using any other distribution channel - comply with all legal and regulatory provisions that apply to such transactions.

Furthermore, these institutions must put in place an appropriate structure and organization as well as control and security measures governing electronic information processing, and adequate internal control procedures in order appropriately to cover the specific risks attendant on using the Internet.

These risks – the materialization of which can have a significant impact on an institution's financial position and reputation – concern, among other things:

a) ***legal risks***: in order to use the Internet for service provision, an institution must examine a series of (in some cases new) legal situations in Belgium or abroad that require a suitable framework; however, the legal or regulatory framework is in some cases entirely new, uncertain, incomplete or even non-existent;

b) ***operational risks:*** the use of the Internet for service provision presupposes the existence of IT and security systems and procedures that make it possible for the institution's staff to monitor client transactions or services by third party providers; the staff in question must be appropriately trained for the purpose;

c) ***reputational risks:*** institutions can suffer harm to their reputation if their services via the Internet are inadequate, insecure or unreliable, if they fail to meet the expectations of their users and their audience, or if they neglect or contravene the relevant Belgian and/or foreign legal and regulatory provisions.

B. Requirements with regard to an institution's organization and internal control

1. General

Before offering information or services via the Internet, a financial institution is required to take stock of the attendant risks and appropriately adapt – and, where necessary, test – its organization and internal controls. In so doing, account should be taken of the types of services offered and of their complexity and scope.

In what follows, the prudential requirements in this regard are explained. These pertain, among other things, to the institution's general policy as well as to specific aspects of the organization relating to the Internet services offered, including the legal and operational framework of the activity, its security, the potential role of authorized agents, the identification and authentication of clients, outsourcing and audit trails.

2. Policy aspects

The institution's senior management – where applicable, the management committee – is required to define its policy and strategy for the provision of services via the Internet as well as for the organization and monitoring of the transactions concerned. The policy must be submitted to the governing body for approval. Such a policy could include the following points:

a) defining a general, financial and commercial policy;

b) determining the marketing objectives and content of the website;

c) determining the technical objectives and options with regard to security, as set out in the enclosed annex;

d) defining the institution's risk management policy and the implications for the various levels of control of the institution (internal control, internal and external audit, …);

e) setting out the internal reporting requirements, taking into account the risks and any detected threats and security incidents;

f) examination and management of the legal implications and risks;

g) determining the resources and procedures for data storage;

h) aligning the internal control system with the organization of the Internet services.

The internal audit function should include, and evaluate, the implementation and functioning of the Internet policy in its audit planning and activities. Appropriate audit programmes and techniques should be used for the purpose.

The activity is to be included in the management's annual report evaluating the internal control system[3]**.**

3. Contractual relationships

Financial institutions that allow their clients to consult and manage their data and carry out transactions via the Internet should enter into a prior agreement with their clients to this effect. A specific agreement is not necessary in the case of a purely informative website, where no personalised data can be consulted.

In addition to describing the nature and scope of the services provided, such an agreement should also cover the conditions and modalities that are specific to the use of the Internet. Thus, among other things, it should include a precise description and demarcation of the responsibilities of each party in using the technologies provided or recommended by the institution for the purpose of identifying and authenticating the client and validating the transactions.

Compliance with the legislation on the prevention of money-laundering also requires that an institution be able to suspend the execution of a client's transactions for the purpose of a regulatory check and/or to refuse to execute them.

Furthermore, if external suppliers are used for the provision, development, management or support of websites or Internet services, institutions should make sure they enter into a suitable contract; the same is true for any counterparties and for the markets, regulated or otherwise, involved in the provision of Internet services.

4. Security

Financial institutions which provide services via the Internet face various security risks.

The annex provides an overview of sound management practices which the CBFA expects financial institutions to follow when updating their security plans. These sound management practices distinguish between points and recommendations related to the security of:

- on the one hand, an institution's own IT infrastructure (internal computer infrastructure, firewalls, email and web servers, etc.) against threats associated with the Internet, and
- on the other hand, financial transactions, consultations and management activities via the Internet.

These sound management practices are relevant for both large and small institutions, although the characteristics of the Internet services offered and the threats faced may vary from one institution to another. Financial institutions are expected to comply with these sound practices or explain any deviations to the CBFA ("comply or explain").

[3] See Circular CBFA_2008_12 of 9 May 2008 concerning the senior management's report on the evaluation of the internal control system and the statement by senior management concerning periodic prudential reporting.

Financial institutions are asked:
- to conduct a delta analysis between their (internal) organisation of Internet activities and the guidelines provided in annex to this circular;
- to draw up a plan regarding the necessary actions and means.

The most important conclusions of this delta analysis, as well as the plan, must be submitted to the CBFA at the latest **by 31 August 2009**. These should also provide an adequate explanation and justification ("comply or explain") for any deviations from the sound management principles contained in the annex to this circular which the institution deems acceptable.

In the case of financial institutions that belong to a group, the group dimension may play an important role in determining the specifics of the security policy in respect of Internet services. In such cases, the institution must demonstrate that the group-level organization does not infringe on the soundness of its security policy and measures.

The CBFA expects to be informed at once of any security incidents in which third parties succeeded in circumventing, via the Internet, the security of the institution's Internet services or of its IT infrastructure.

5. Operational aspects - Availability, continuity and correct execution of transactions

A high level of availability is an important and publicly visible measure of the quality and reliability of the websites and Internet services offered. Each institution should determine the desired availability objectives and should ensure that the necessary organizational and technical measures are taken. To this end, institutions should adopt appropriate incident management in order to be able to restore their websites or Internet services in case of a malfunction within the (time and quality) objectives that have been set.

Depending on the nature and importance of the websites and Internet services offered and the continuity objectives sought, the institution should have appropriate emergency plans and provisions in order to be able to withstand large-scale disruptions to the Internet service. The principles set out in Circulars PPB 2005/2 and PPB/D.256 of 10 March 2005 on "Sound management practices in respect of business continuity planning for financial institutions" continue to be fully applicable.

When drawing up these emergency plans and in particular during the risk assessment and business impact analysis, attention should be paid to the "(D)DOS" attacks[4] which, though still limited, are nonetheless rapidly increasing; these attacks seek to cause serious - and in some cases lengthy - disruption to the availability of the websites and Internet services provided.

The financial institution is required to ensure an adequate follow-up of the transactions passed on to it via the Internet, by putting in place procedures to provide for their correct processing and to manage the inherent risks appropriately. The institution must see to it that the staff who (may) deal with the Internet applications are suitably trained.

6. Involvement of external service providers

Where certain activities relating to the offer of websites and/or financial services via the Internet are outsourced, or where external service providers are used for the necessary support, the financial institution should obtain the necessary guarantees that the said service provider has the capacity and competence necessary to carry out the outsourced tasks in a reliable and professional manner and thereby to ensure the continuity of the service.

Where the institution outsources the management of websites and/or Internet services to a third party, senior management - the management committee, where applicable - should also ensure that the external service provider has the necessary independent security tests carried out (see Annex, points

[4] (D)DOS attacks, i.e. "(Distributed) Denial of Service" attacks, are intended to make the Internet sites of individuals or companies unavailable by saturating the sites over a period of time with enormous quantities of (sometimes specially designed) Internet messages.

2.2.9 and 3.2.7), that the institution is informed of the results of these tests and that the service provider periodically and as often as necessary evaluates the security of the Internet services offered in the light of developments with regard to security threats. If the service provider does not perform all the aforementioned security tasks, then the institution itself must take charge of carrying them out; the respective responsibilities of the parties concerned must be clearly laid out in the contract with the external service provider. Moreover, the financial institution's contract with the service provider must stipulate that the institution has the right on its own initiative to have a security audit carried out.

The principles set out in Circulars PPB 2004/5 of 22 June 2004 and PPB 2006/1 of 6 February 2006 on "Sound management practices for outsourcing" continue to be fully applicable.

7. Remote identification of clients

Via the Internet, financial institutions can reach people who, for reasons of geographical distance, cannot easily be identified through face-to-face contact.

As regards the identification of clients at a distance, financial institutions must comply with the provisions of the Law of 11 January 1993, in particular Article 6*bis*, as well as of the CBFA Regulation of 27 July 2004, approved by the Royal Decree of 8 October 2004, and in particular Articles 8, § 2, 34 and 37, which stipulate that the institution is required to have a monitoring system by which atypical transactions can be traced.

This regulation is explained in various CBFA circulars on the obligations of customer due diligence and on preventing the use of the financial system for money-laundering and the financing of terrorism[5].

C. Requirements as regards compliance with the rules of conduct

The remote relationship that can be a regular feature of online service provision, both in the creation of the business relationship and afterwards when carrying out transactions, excludes a number of traditional "human" contacts and interactions that might otherwise serve to exchange information between the intermediary and the investor.

It is therefore important that the institution recognize, when it enters into a business relationship, that providing distance services (whether the full range of services or specific parts thereof) does not exempt them from carrying out the necessary exchange of information and providing advice to the client.

Credit institutions, investment firms and UCITS management companies should refer in particular to the following provisions:
- the Law of 14 July 1991 on trade practices and the information and protection of consumers, and in particular the section of this Law on distance service agreements;
- the provisions of Articles 27, 28 and 28*bis* of the Law of 2 August 2002;
- the Royal Decree of 3 June 2007 concerning the rules and procedures for transposing the Markets in Financial Instruments Directive.

When providing investment services via the Internet that relate to non-complex financial instruments, there may be cases in which the service provided is limited to the execution of orders or to the receipt and transmission of orders (*execution only*). In such cases, the institution can, pursuant to Article 27, § 6, of the Law of 2 August 2002, forego obtaining information about the client's knowledge and experience.

It is important that the institutions always verify whether the conditions are met which allow them to offer their services under this regime. This means, among other things, that no initiative is to be taken to encourage the client to take up the institution's offer of certain transactions.

Moreover, this regime does not release financial institutions from their general obligation to act honestly, fairly and professionally in the best interests of their clients[6] and in particular as regards the obligation to

[5] See, among others, Circular PPB 2004/8 of 22 November 204 as amended by Circular PPB 20O5/5 of 12 July 2005.

[6] Article 27, § 1, of the Law of 2 August 2002 on the supervision of the financial sector and on financial services.

take measures to avoid conflicts of interest[7], as well as its obligation to obtain the best possible result when executing orders[8].

When executing orders or receiving and transmitting orders relating to complex financial instruments, the financial institution must have first obtained information from its client regarding the latter's knowledge and experience. If the service or the product is not suited to the client in question, the institution should have the necessary system in place to warn the client of this.

Some financial institutions offer their clients the option of receiving investment advice via the Internet.
In that case, the institution will have to observe the duty of care referred to in Article 27, § 4, of the Law of 2 August 2002. Before any investment advice services can be offered, the institution must make the necessary IT arrangements to ensure that for each client, only such transactions may be carried out as are deemed appropriate to his knowledge and experience, financial situation and investment objectives.

Insurance companies should refer in particular to:
- the Law of 14 June 1991 on trade practices and the information and protection of consumers, and in particular the section of this Law on distance service agreements;
- the Royal Decree of 22 February 1991 containing general regulations relating to the supervision of insurance companies and in particular Article 15;
- the Law of 27 March 1995 concerning insurance and reinsurance mediation and the distribution of insurance and in particular Article 12*bis* to 12*quinquies*;
- the Royal Decree of 14 November 2003 on life insurance activities and in particular Articles 8 and 72.

Where necessary, we refer as well to the Code of Good Conduct for advertising and providing information about individual life insurance products, drawn up by the professional associations after consultation with the CBFA.

Finally, we refer as well to the individual info sheets on life insurance and other insurance products which the professional associations in the sector drew up in implementation of Article 12*bis*, § 3, of the Law of 27 March 1995.

D. Cross-border nature of the services offered or provided

A website by definition has an international reach, and therefore a significant proportion of the offers and provision of services via a website can be of a cross-border nature.

In the case of cross-border provision of services within the EEA, the institution is required first of all to comply with its notification requirements in accordance with its legal status.[9] So far, the CBFA's view on the notification requirement has been that the provision of a service is presumed to have a cross-border nature, not only if the characteristic performance of the service (i.e. the essence of the service for which payment is due) takes place on the territory of another Member State, but also if the undertaking advertises its services to investors in that other Member State, whether by moving there, by means of distance selling technologies or through advertisements other than publicity.

The question arises as to the rules that apply to cross-border service provision. As things stand now, a distinction should be made according to the sorts of services offered via Internet.

---

7 Article 20*bis*, § 2, of the Law of 22 March 1993 on the legal status and supervision of credit institutions, and Article 62*bis* of the Law of 6 April 1995 on the legal status of and supervision of investment firms.

8 Article 28 of the Law of 2 August 2002 on the supervision of the financial sector and on financial services.

9
- for credit institutions, see Article 38 of the Law of 22 March 1993 on the legal status and supervision of credit institutions;
- for investment firms, see Article 87 of the Law of 6 April 1995 on the legal status of and supervision of investment firms, and the standard letter of 15 October 2007 to investment firms and credit institutions governed by Belgian law;
- for management companies of undertakings for collective investment, please see Article 180 of the Law of 22 July 2006 on certain forms of collective management of investment portfolios;
- for insurance companies, see Article 57 of the Law of 9 July 1975 concerning the supervision of insurance companies.

For insurance intermediation as well as for financial or banking services other than investment services, the intermediary must comply with the rules protecting the general good, including the rules of conduct, of the country on whose territory he offers or provides his services (the host country).

As regards investment services, credit institutions and investment firms must comply with both the organizational rules and the rules of conduct of the country of origin (the home country). The host country cannot impose its own rules regarding investment services. However, other rules of the host country, such as the law on the prevention of money-laundering or any language legislation, do apply. The same principles are applied, in the draft UCITS IV Directive[10] to management companies of undertakings for collective investment.

With respect to the use of a website, more specifically, several foreign supervisors have taken the view that where an offer from abroad of services or of instruments via the Internet is directed or available to investors in their territory, that offer is considered to be made in their territory. When assessing these criteria, each case is generally examined separately in order to determine, among other things, whether the nationals of the country in question are being specifically targeted (language use, prices quoted in that country's currency, mention of local contact addresses) or whether in reality transactions or services are carried out via the website, and whether investors are solicited by email or other forms of communication technology.

The institution must, therefore, carefully outline its business objectives and ensure that if it solicits clients on the territory of another State via its website, it complies, where applicable, with the rules of the State in question. In order to make sure that its actions are not misunderstood in countries that are not being targeted, an institution can take one or more of the following measures:

a) mention on the website that it is intended for investors within a clearly defined geographical area in which the firm is active and complies with local regulations (mention notifications, warnings and disclaimers); in order to determine the location of the investor and to check whether he falls within the target group, the institution can use post, telephone or special localisation techniques;

b) ensure that the content of the website or other promotional materials (e.g. in the media or the press) is not in contravention of the rules in force in the aforementioned geographical target area (e.g. if the website is not addressed to British clients, no local addresses or prices in GBP should be mentioned);

c) provide for access control through password protection for all or part of the website, to which only persons belonging to the target group will receive passwords;

d) contact local supervisors in order to make sure that the website does not contravene local regulations.

Yours sincerely,

Jean-Paul Servais
Chairman

Annex: CBFA-2009-17-1 / Sound practices for managing Internet security risks.

[10] Article 18(3) of the draft Directive.