Arnold Schilder: Banking in the new economy: a supervisory perspective

Speech by Mr A. Schilder, Executive Director of De Nederlandsche Bank N.V., at the Take Off Conference 'Information Battle: Consequences of the New Economy on Economic and Business Life', University of Maastricht, 14 February 2001.

* * *

Introduction

The new economy affects the almost two-hundred-year-old Nederlandsche Bank in many ways. Today, I will focus on the implications of the new economy for banks and for banking supervision. The subject therefore is: e-banking supervision.

Electronic banking

First, what is e-banking? E-banking is the provision of banking services by means of electronic data transfer between participants. The information is transferred via a network, which may be a computer network such as the Internet, or a telecommunications network. Rabobank's Random Access Banking is an example of e-banking. By that, customers can make payments, deposit savings, and make investments over the Internet or by telephone. In addition, when people shop in a Dutch cybermall, such as Davista (www.davista.nl), Random Access Banking mostly offers the possibility to pay using Rabo Direct. This last application could be described as using your PIN code over the Internet. Another recent example of e-banking is Wellowell, owned by ING. This is an on-line marketplace. Customers can compare insurance offers and banking products from various providers here, and close the deal there and then. Examples are a car insurance or a savings account. In this way, ING offers its own products, as well as those of its competitors.

What does the advent of electronic media mean for banks? I would like to mention three consequences. One is that the Internet makes the market more transparent. Consumers can compare products and services from different providers more easily, and shop around for the best offers. This is particularly the case for standard products like consumer credit, where price is the key factor determining the customers' selection. In addition, the costs of switching suppliers are lower in the case of electronic banking. Combined with the increased comparability of products, this could reduce customer loyalty. This in turn means fiercer competition for banks.

A second consequence of the new information and communication technologies is that the organisational structure of banks will be affected. Banks have a very integrated value chain, horizontally as well as vertically. This means that all elements of their service are provided by the same organisation. Examples are account management, product development and infrastructure. The Internet puts pressure on this integrated organisational structure. An important aspect of Internet technology is that its development requires very high initial investment, but that the marginal costs of use are low. This raises the possibility that new, specialised suppliers are able to carry out certain specific activities more efficiently than the banks themselves. On the one hand, this situation offers the banks the option to outsource some of their operations to others, thus achieving cost reductions. On the other hand, it could bring unwanted pressure on parts of the banks' value chain, and ultimately lead to deconstruction of the chain itself. A practical consequence of this trend is that banks are developing into network organisations by way of alliances and cooperation with both financial and non-financial institutions. For example the cooperation between ABN AMRO and KPN in relation to the launch of the 'Money Planet' Internet site.

A third consequence is that new suppliers can enter the market more easily. In the virtual world, barriers to entry are significantly lower. There is no longer a need for an extensive branch office network, for example. Lower entry barriers mean more suppliers in the market, which intensifies competition. These suppliers may take different forms. They may be existing banks originating from other countries. These banks can use the Internet to bring about a rapid internationalisation of their activities. Various institutions have already set up electronic subsidiaries, which offer banking services on an international scale under a new brand name or under the name of the parent bank. Examples

include the Bank of Scotland's electronic subsidiary Eubos, which offers mortgages on the Internet in this country, or ING Direct, ING's electronic offshoot, which is active in Canada and elsewhere.

New suppliers can also be pure electronic banks, or institutions from the non-banking sector. Pure electronic banks are not linked to an existing physical bank. Although they do not have the high fixed costs of a branch network, they do have to invest heavily in building up their reputation. It is interesting to note that the current market share held by such banks is still very small. The principal reasons for this are probably the lack of confidence resulting from the lack of a physical presence and the high cost of marketing the brand name. Newcomers from the non-banking sectors can be existing non-financial institutions that offer a limited range of financial services through electronic channels. Volkswagen in Germany is one example. They offer consumer credit. Also companies which specialize in payment systems are part of the non-banking category. Right now I am talking, they offer you the possibility to make payments over your mobile telephone. This sevice is already available in the United States. Other non-banking institutions include consumer comparison sites like Wellowell, portals and personal agents.

The implications of e-banking for supervision

So far I have described some consequences of electronic media for the banking system. But what are the implications for banking supervision? Let me discuss some recent activities undertaken by supervisors.

First, the Nederlandsche Bank supervises the banking system in accordance with the Dutch Credit Systems Supervision Act. The Policy Regulations for the Media (Beleidsregels Media) were formulated to indicate how this Act should be applied where financial services are offered via electronic media. Briefly put, these Regulations state that it makes no difference whether banking services are provided via traditional channels such as branch offices, or over the Internet. In both cases the institution concerned is required to hold a banking license. For example, an institution established in the Netherlands which provides banking services over the Internet comes under the supervision of DNB. However, a provider which is established abroad but via the Internet is active in the Dutch market is also subject to DNB supervision. Several indicators play a part in deciding whether activities are considered to be directed at the Dutch market, like the use of the Dutch language, contact points in the Netherlands, and the addressees of the media used. The existing regulatory legislation is therefore adequate for proper banking supervision, also with the advent of e-banking. E-banking has however made the regulator's task more complicated. How do we check that all providers that are active over the Internet in the Dutch market do indeed comply with regulatory legislation? This brings me to a recent DNB initiative.

Second, in combination with its fellow regulators the Dutch Insurance Board and the Securities Board of the Netherlands, the DNB has entered into a co-operative agreement with the Dutch National Police Agency (Korps Landelijke Politiediensten, or KLPD) and the Dutch Economic Investigation Service (Economische Controle Dienst, or ECD). We are working together on developing new tracking methods. The objective is that those whose actions on the Internet are in breach of the regulatory legislation can be traced.

A third initiative is the introduction of the internet officer. The digital detective, or cybercop, is already a familiar phenomenon in police circles. From the beginning, the use of cybercops has induced investigation authorities to develop techniques to discover the identity of those who are in breach of the law. The regulators want to use this technology in their supervision of the financial sector. The DNB now has one internet officer, which like the digital detectives is engaged in tracing financial offenders. So far, several indications of offences on the internet have been found. For example institutions that offer banking services over the internet without having a banking license. Also some so-called 'study investment associations' (studiebeleggingsclubs) were in breach of the regulatory legislation. These investment funds, founded by students, operated over the internet without a license of DNB.

A fourth initiative to protect consumers against unauthorised banking services is the introduction of so-called hyperlinks. This possibility is currently being investigated. Every financial services provider using e-commerce would be required to place a hyperlink on its website referring to the relevant regulator. By clicking on this hyperlink, consumers would access a list of providers licensed by the regulator, and could easily see whether a provider is on the list, and therefore is trustworthy. Another possibility being considered is a regulator's 'black list', which would be a special page on the

regulator's website listing financial services providers that are operating without a license and therefore not trustworthy.

So we work together with fellow regulators, the police and investigation services. However, the Bank has a separate unit concerned with the supervision of banks and information technology within its Supervision department. The fact is that e-banking involves several specific operational risks. One operational risk mainly relates to the security of systems and transactions, including data confidentiality and authentication of the parties involved. Another operational risk refers to the continuous availability of the Internet as a medium for financial transactions. This availability is prone to serious hazards, such as computer viruses and hackers. Think for example of the Homebanking application of ABNAMRO, that was subject to an attack of hackers in September last year. Such an incident may damage the reputation of the internet as a means of payment. It is therefore very important for banks to ensure the safety of e-banking. The regulators at our IT- unit monitor whether this is sufficiently done. To that end, they have conversations with the banks to gain insight in the controls, the legal implications and particularly the security of e-banking. Furthermore, they retrieve documentation, such as the banks' risk analysis, an independent EDP audit report and the results of a penetration test. This test is a legal attempt to hack, conducted by an external organisation.

As well as the national initiatives I just mentioned, there are international activities under way in the e-banking area. A good example of this is the work of the Electronic Banking Group, or EBG, which is a working group of the so-called Basel Committee of Banking Supervision. This group is engaged in formulating international guidance and principles regarding e-banking. The EBG recently published its principles for risk management in electronic banking, which also include issues relating to consumer protection. One example is a principle that concerns appropriate disclosures for e-banking services. This principle states that banking organisations should provide on their websites some core information in order to assist customers in making informed choices. Examples of such disclosed information could include contact details for the supervisory authority responsible for the supervision of the bank's head office as well as details of access to national compensation or insurance schemes. The risk management principles for e-banking are currently presented to the banking sector for consultation. It is expected that the final version will be presented to the Basel Committee next month. Around April, the principles will be published at the website of the BIS (www.bis.org). Beside the publications at our own website (www.dnb.nl), such as this speech, you also find a link to the site of the BIS.

Besides the work of the Basel Committee that applies specifically to the banking sector, there is more general legislation in the form of EU directives. These affect e-banking as well. For example the Directive on electronic commerce, which requires providers of electronic services to make information on prices and conditions accessible for consumers. Another relevant directive for e-banking is that on the remote provision of financial services. This states for example that consumers have the right to recall an agreement if a supplier did not provide them with the terms of delivery, like prices, before entering into a transaction.

Conclusion

To summarize: e-banking is a phenomenon which affects both banks and regulators. I hope I have made clear that this subject has the regulators' full attention, both nationally and internationally. As well as participating in international discussions on e-banking, the Bank has undertaken various initiatives to include e-banking in its supervisory policy. This does not mean that we can afford to be complacent. Developments are proceeding rapidly, and the DNB is closely monitoring developments to ensure a timely response. In various ways we keep up our know-how on an continuous basis. By means of courses and self-study, for example. But also by benchmarking through third parties, as it is relevant to review one's own organization from time to time. Finally, a very important way for keeping up our know-how is by recruiting new staff. So if the supervision of e-banking has aroused your interest, DNB is probably something for you.