

Legal Issues in Mobile Banking

WEBER, Rolf, DARBELLAY, Aline

Reference


WEBER, Rolf, DARBELLAY, Aline. Legal Issues in Mobile Banking. *Journal of banking regulation*, 2010, vol. 11, no. 2, p. 129-145

DOI : 10.1057/jbr.2009.16

Available at:

<http://archive-ouverte.unige.ch/unige:100135>

Disclaimer: layout of this document may differ from the published version.



Legal issues in mobile banking

Rolf H. Weber

is Ordinary Professor of Civil, Commercial and European Law at the University of Zurich and Visiting Professor at the University of Hong Kong. He is at the head of the project 'Law, Regulation and Finance', which is one specific topic of the research programme 'Finance and Financial Market' at the University of Zurich. He is Director of the European Law Institute and the Center for Information and Communication Law at the University of Zurich. In addition, he is engaged as an attorney-at-law and as a Member of the Editorial Board of several Swiss and international legal periodicals.

Aline Darbellay

is a research assistant at the University of Zurich. She has been active in the topic 'Law, Regulation and Finance' of the research programme 'Finance and Financial Market'. She is currently working on projects in financial market regulation. She holds a Master's of Law from the University of Lausanne.

ABSTRACT The use of mobile phones in order to effectuate banking transactions is bound to increase in a significant way in the near future. This growth in mobile financial services not only depends on technological advances, but also on consumer confidence in the provided services. Mobile financial services can be divided into mobile banking and mobile payment; therefore, legal certainty must be established as to what supervisory regime applies to the various activities involving banks and non-banks. Mobile banking activities fall within the scope of the banking business, and oversight is provided by the competent financial market authority for prudential supervision, if the definition of banking activities encompasses all relevant mobile banking activities. Furthermore, legal aspects also play a role in the evolution of mobile banking as far as the need to enhance customer trust in the offered services is concerned. Major issues arise in relation to data security and consumer protection. Moreover, the outsourcing of certain key activities to mobile operators deserves further attention, as mobile operators can, under specific circumstances, become deeply involved in mobile banking.

Journal of Banking Regulation (2010) **11**, 129–145. doi:10.1057/jbr.2009.16

Keywords: mobile financial services; mobile banking; prudential supervision; customer trust; data security; consumer protection

INTRODUCTION

Customer mobility has become enhanced in modern financial markets as bank customers wish to trade independently of their location. Insofar as electronic banking has already enabled bank customers to trade any time, mobile banking has additionally allowed them to trade anywhere, thereby implying even more flexibility to the benefit of innovative customers (p. 26).¹ A new development has therefore been the growing investor interest in mobile telephony as a means of trading and obtaining information regarding specific securities.² The use of mobile phones is indeed burgeoning in the field of financial services.

Great business opportunities result from the diffusion of mobile phones. The broader usage of mobile telephony has encouraged banks as well as non-banks to develop new payment services for their customers.³ The banking industry is not primarily driven by the opportunity for new gains resulting from the mobile financial services, but rather by the projection of an image as an innovative bank. In the industrialised economies, the additive model implies that banking appears as an additional channel for already banked customers. Mobile banking is now accelerating across Europe, as most major banks are using this communications form to make all their services available through multiple

channels, thereby attracting new customers.⁴ Further, the transformative model aims at offering unbanked persons access to banking services. The financial product linked to the use of mobile telephony is thus targeted at unbanked customers, who are largely low-income persons (p. 3).⁵ This model especially corresponds to the needs of developing countries, in which mobile telephony has spread much faster than the use of computers. For instance, in Africa, four in ten people now have a mobile phone.⁶ Therefore, mobile banking may even enhance the adoption of banking services by people in remote areas.

After a troublesome start, mobile banking is on the way to growth as technology has matured and favourable conditions have been assembled. Especially in industrialised countries, the trend to be observed consists in the convergence of wireless communications and the Internet (p. 92).⁷ For instance, standards such as the wireless application protocol (WAP) and iMode are considered key building blocks towards enabling the delivery of Internet services via mobile phones (p. 94).⁷ The commercialisation of 3G phones also fosters the advancement of mobile financial services.⁸ These technological developments offer new perspectives for the growth of mobile commerce. In the developing world, mobile financial services are often provided through short message services (SMS). Text-based services have the potential to unlock a range of social and economic benefits to users even based on the most basic mobile phones.⁹ Therefore, mobile phones are now seen as a vital tool of development.¹⁰ In the future it is not the innovativeness of technology, but the innovativeness of users and uses that will drive mobile commerce growth to a new level.¹¹

The success of mobile banking depends to a large extent on the user-friendliness of the offered services. The idea of providing financial services through mobile phones attracts customers owing to its convenience. Moreover, the services can be widely used only if they imply a reduction in costs as compared to traditional banking tools. Further, if data transmission using WAP technology was too slow in the past, the technology has recently become appropriate for customers since the transmission speed increased.² In sum, customers are keen on adopting the mobile services as soon as three key requirements are met: simplicity, cheapness and rapidity (p. 61).¹² Apart from these, security is also essential in order to promote customer trust in the provided services. To some extent, the security requirement can come into conflict with the simplicity, cheapness and rapidity of the services; however, customer adoption does not go without guaranteeing customer confidence. Customers are particularly concerned about data security in the banking field.

The growth of mobile banking also depends on the suitability of the legal framework for mobile banking. Regulators must comply with the various requirements of the industries and users and create an attractive environment in order to satisfy customers' needs. The distinctive feature of mobile banking is the fact that another medium is used than in traditional banking.¹³ There is general agreement among banks and bank supervisors that mobile banking activities should be approached similarly to traditional banking practices (p. 2).¹⁴ The financial market regulator provides an oversight of all banking activities, mobile banking services included. However, there are specific risks related to mobile banking and merely its unique characteristics give rise to further concerns. First and foremost, legal aspects have a role to play, as the relationship between the bank and its customers appears to be very loose in mobile banking. Legislators must focus on the dangers inherent in mobile banking. The question arises as to whether the bank's fiduciary duties, such as the duties of loyalty, advice and diligence, can be applied. Further, consumer protection deserves attention in terms of transparency requirements. Finally, mobile operators perform a crucial function in the mobile commerce value chain. They may be directly or indirectly involved in mobile banking services, for instance through billing. This trend makes it important to analyse the position of mobile operators in the mobile banking field.

OVERVIEW OF THE MOBILE FINANCIAL SERVICES

Finance-related services being offered by employing mobile telecommunication technologies are generally referred to as mobile financial services (p. 69).¹ It is very important to define the various types of mobile financial services in order to ascertain which regulatory and supervisory regimes apply to them. Mobile financial services include mobile payment and mobile banking. The limit can be drawn between the different domains while determining whether a banking activity or a sheer mobile payment is concerned.

First, mobile payment has already become widely expanded in industrialised as well as developing countries. Mobile payment usually implies financial services providers fulfilling an intermediary function between buyers and sellers in order to facilitate the purchase of goods or services with the help of mobile devices. The particularity of the issues related to payment services leads to the necessity of implementing a supervisory regime specifically applicable to payment institutions, which is less stringent as compared to the regime applicable to banks (para. 7 of the preamble).¹⁵ Second, mobile banking is growing slowly and is much more regulated than mobile payment. Mobile banking services are always associated with a banking activity. The competent authority of financial market supervision is responsible for the prudential supervision of mobile banking activities. Third, the issuance of electronic money also deserves to be treated separately, as it does not automatically correspond to a banking activity. Electronic money institutions may be subject to a specific regulation and supervision if they are not a credit institution receiving funds from the public (para. 5, 6 and 7 of the preamble).¹⁶

In the developing world, the substantial growth in mobile phone penetration implies that there are much more mobile phones and sellers of mobile airtime than cash machines and bank branches.⁹ Therefore, a high potential of developing financial markets through the use of mobile devices is to be expected. Mobile financial services have essentially developed outside the regulated banking area, as non-banks are much more involved than banks in the offering of services and because of the fact that customers bring low amounts of money into the scheme. The enormous social and economic benefits resulting from mobile banking might induce regulators to allow mobile banking to grow besides the regulated banking segment, that is without formal regulatory approval. Consequently, this fact facilitates the creation of innovative mobile-money schemes and contributes to the creation of more efficient financial markets even in remote areas. After noticing the success of these mobile-money schemes, banks realised that teaming up with a mobile operator to launch a mobile-money service would allow them to reach many more customers; then the banks' involvement in mobile-money schemes has in turn reassured banking regulators.⁹ This results in a mixed regulatory approach which recognises the distinctive features of mobile-money schemes. For instance, the customer identification process is more formal than for buying a Subscriber Identity Module (SIM) card, but less rigorous than for opening a bank account.⁹ Technically, a great part of these mobile-money schemes belongs to mobile payment. Yet they tend to be confounded with mobile banking, mainly because they reach unbanked customers, thereby being considered as a means of making banking services available to a broader range of people.

Mobile payment

Mobile payment refers to the range of mobile commerce services involving payment transactions initiated or confirmed by using a mobile phone. The use of mobile telephony is particularly promising in the field of micro-payments. Small purchases of goods or services tend to be increasingly operated via the mobile phone. Credit card processing is not a viable option for too little payments because of the minimum credit card transaction costs; to the contrary, mobile payment systems have inherent advantages achieving low transaction costs.¹⁷

The distinction between mobile banking and mobile payment is very important because of the fact that different regulatory and supervisory systems apply to the corresponding activities. The

regulatory and supervisory oversight of mobile payment gives rise to a less stringent regime than the prudential supervision of mobile banking services, as the risks in banking are substantially higher.

In the field of mobile payment, two alternatives exist: On the one hand, mobile operators can provide value-added services apart from their core telecommunications services. Value-added services may be offered by a content provider and are at any case billed by the mobile operator. Telecommunications services and value-added services are supervised under the same roof, though more stringent duties apply to value-added services. The regulatory systems require the registration of telecommunications service providers. In the European Union, the competent authorities are the National Telecommunications Com-missions.¹⁸ In Switzerland, the notification to the Federal Office of Communications is necessary before providing telecommunications and value-added services.¹⁹ On the other hand, a specific regime applies to payment institutions in the European Union. They have to apply for an authorisation from the banking supervisor as a payment institution before providing payment services, such as mobile payment services (art. 5).¹⁵ The activities of the mobile operator include the payment transactions for the provided goods or services. The European legal framework applies in cases in which the operator acts only as an intermediary who simply arranges for payment to be made to a third-party supplier (para. 6 and art. 3 let. I).¹⁵

In practice, the use of mobile telephony to effectuate mobile payments is already wide-spread because of the simplicity of the service. There are two basic forms of payment mechanisms: First, the easiest practice of implementing the data transfer consists in including mobile payments directly in the phone bill, that is, the customer pays for the goods or services later together with the mobile phone bill. Mobile operators are well equipped at handling small payments and at billing.²⁰ In these cases, the mobile operator acts only as an intermediary who simply arranges for payment to be made to a third-party supplier (para. 6 of the preamble).¹⁵ National jurisdictions allow these payments via the phone bill up to a limited amount. Second, mobile payment can be conducted over customers' prepaid accounts. If a prepaid account is used, electronic money may be issued in parallel. The demarcation line cannot be easily drawn between prepaid accounts and deposit accounts. Both may be considered as payment accounts and criteria must be established in order to determine whether a banking activity is involved or not. Managing a deposit account is a banking service whereas the bank typically pays interest to depositors. Providers of mobile prepaid accounts do not pay interests. Further, the bank engages in banking activities with the funding providing from the deposits. Providers of mobile prepaid accounts must keep the entrusted money aside for the sole purpose of executing customers' transactions and limit their activities to fulfilling this purpose.

In the developing world, mobile-money schemes are very innovative. Mobile payment especially benefits from a favourable environment in the developing countries having less experience with traditional banking services. In such countries, mobile payment is likely to be the path to the adoption of mobile financial services while lower adoption of mobile banking is expected (p. 16).²¹ Mobile financial services can indeed have enormous social and economic benefits. Traditionally, people who want to send money need to travel to deliver the cash in person or ask an intermediary, such as a bus driver, to deliver the money. Mobile payment can make it easier, quicker, cheaper and safer to transfer money while allowing customers to pay money into the system by handing cash to an agent, usually a mobile operator's airtime seller, who credits the money to the customers' mobile-money account.⁹ Customers can transfer money with the help of a SMS containing a special code which can be taken to an agent to withdraw cash.⁹ Therefore, non-banks are deeply involved in offering mobile financial services. Launched in 2007 by Safaricom, Kenya's largest mobile operator, M-Pesa has in 2009 nearly 7 millions users, which is not bad for a country of 38 millions people, 18.3 millions of whom have mobile phones.⁹ M-PESA is primarily used to transfer money, is also used to pay for everything from school fees to taxis, and is eventually used as a form of savings account, even though it does not pay interest.⁹ Poor people generally save in order to deal with unexpected events by buying livestock, which can get

sick or die, or buying gold, which can be stolen, or investing in community-based schemes, which may be fraudulent.⁹ Therefore, mobile financial services offer a more reliable alternative. Especially, this use of M-PESA gives rise to concerns about qualifying the target service as a mobile banking service rather than a mere mobile payment service. Therefore, it is necessary to draw a demarcation line between mobile payment and mobile banking in order to know when banking regulations should apply to the offered services.²²

Mobile banking

Mobile banking includes the whole range of services in which a banking activity is involved.²³ Mobile banking services are regulated similarly to traditional banking practices in the sense that the same regulatory and supervisory treatment applies to them. Regulations empower national authorities to supervise the financial markets. Providers of mobile banking services are considered as credit institutions required to obtain authorisation before commencing their activities (art. 6).²⁴ Therefore, mobile banking falls under financial market regulations.

Broadly speaking, various types of financial services can be offered in mobile banking. The mobile banking segment encompasses mobile accounting, mobile brokerage and mobile financial information. Relating to the technological tools, credit institutions providing mobile banking services rely on one or a combination of the following three strategies: text messaging, browser-based programmes or downloadable mobile banking applications (p. 6).²¹

Mobile accounting

Mobile accounting includes transaction-based banking services revolving around a standard bank account (p. 57).¹² The deposit and credit businesses are at the core of the banking activities. The deposit business of a credit institution implies the acceptance of funds from the public. The credit business implies the granting of loans and the acceptance of credits. These banking activities can be accomplished through the use of mobile devices as a tool to facilitate transactions.

Various banking activities fall under mobile accounting. Bank customers principally take advantage of mobile accounting in order to monitor their transactions. Among others, bank customers may be able to use their mobile phone to make money remittances, giving payment instructions, executing payment transactions, or cancelling orders. Text messaging can serve the purpose of initiating and confirming mobile payments. For instance, Postfinance in Switzerland enables its customers to transfer money to another postal account by text message, in the amount of up to 100 Swiss francs per day and recipient.²⁵ Another service consists in the confirmation of direct payments via the phone's microbrowser. Mobile accounting also enables bank customers to transfer funds from one sub-account to another, for instance from savings account to securities account and vice versa (p. 75).¹ Further, the line between mobile banking and mobile payment is especially difficult to draw when bill payments are comprised. The distinctive feature is that mobile banking covers transactions revolving around a bank account while mobile payment is executed through the phone bill or a prepaid account. Banks are involved in mobile banking, as its strength lies in managing account-based payments or macropayments, and in mediation of payments.²⁰ Mobile operators tend to be the key actors in mobile payment.

In the developing world, the widespread adoption of mobile payment can be seen as a transition towards the adoption of banking services. As many poor people do not have a bank account, these new customers are inclined to rapidly use mobile financial services as a way of saving money. Mobile banking is therefore gaining momentum in developing countries. Moreover, banks increasingly team up with mobile operators in order to reach more potential customers.⁹ For instance, MTN, the South Africa-based multinational telecommunications company, launched a mobile-money service in Uganda in March 2009, in partnership with Stanbic Bank, also based in South Africa.⁹ Money can be easily

transferred through text messages and money can be stored on mobile devices. As increasing amounts are at stake, regulators should be aware of the fact that they have a role to play in establishing appropriate frameworks which deal with relevant issues such as depositor protection. The idea is to recognise mobile-money schemes as mobile payment services up to a certain amount by limiting balances and transfers; as far as larger sums are concerned, the offered services should be considered as mobile banking and a more stringent regulatory treatment should apply as compared to the less formal regulatory treatment applied to mobile payment.

Mobile brokerage

Mobile brokerage refers to intermediary services such as selling and purchasing stocks, bonds, funds, derivatives and foreign exchange instruments; mobile brokerage allows the placing and the cancellation of orders to sell and purchase securities or other financial instruments (p. 77).¹ In this area, credit institutions act on their own name for the account of others. They provide banking services primarily related to trading in the stock markets. Mobile services can also help to operate and administer a securities account.

Trading is made available through mobile devices. This is especially suitable for modern bank customers, as mobile trading matches their lifestyles. For instance, the Saxo Bank, which has its headquarters in Denmark, focuses on its image as an innovative bank while advertising its SaxoMobileTrader to its customers.²⁶ The SaxoMobileTrader is a flexible trading platform enabling clients to trade in currency markets, stock markets and derivatives markets. The key aspect lies in delivering professional trading tools to private investors. By this means, the bank wishes to satisfy its customers as well as attract new customers.

In the developing world, focus is not put on Web browser applications but rather on SMS. For instance, Google Trader is a marketplace application which allows customers to buy and sell goods and services on their mobile phone using SMS.⁹ To a certain extent, Google acts like a non-depository financial intermediary while performing the brokerage function of bringing buyers and sellers together in order to allocate resources more efficiently. Google Trader costs twice as much as a standard SMS and is an especially valuable service for matching buyers and sellers of agricultural products and commodities; sellers send a message giving information on where they are and what they have to offer, which will be available to potential buyers within 30 km for 7 days.⁹ Further examples are TradeNet in Ghana and CellBazaar in Bangladesh.⁹ These innovations contribute to make financial markets more efficient.

Mobile financial information

Only mobile financial information provided by credit institutions and other financial services institutions fall within the scope of mobile banking. They are meant to provide the customers with anytime, anywhere access to information and may either concern the bank and securities accounts of the customer or it may be regarding market developments with relevance for that individual customer (p. 79).¹ Mobile accounting and mobile brokerage cannot be developed successfully without guaranteeing access to the related information. Therefore, relevant information for decision making should be made available through the mobile phone. This, in turn, allows customers to make informed judgments.

Information related to the bank account can be delivered via mobile devices. Mobile phone users see when payments have been credited and have the possibility to check their balances at anytime and anywhere. Moreover, there are alert services which warn customers as soon as they approach their account limit, or when large amounts are debited. For instance in the United Kingdom, First Direct sends to the customers mini statements as text messages and alerts them to keep the accounts up-to-date with their funds.²⁷ Further, the mobile phone is a convenient tool to help

customers to locate branches or Automated Teller Machines. Finally, mobile financial information can be used to make investment decisions, bank customers receiving manifold information, such as share prices or stock prices.

In the developing countries, focus is put on agricultural information; valuable agricultural information includes market prices, weather data and farming tips.⁹ Customers are ready to pay fees to receive these services. For instance, Nokia, the world's largest handset-maker, launched its own information service, Nokia Life Tools, in India.⁹ These services help farmers and make markets more efficient.

Electronic money issuance

Electronic money is considered as an electronic surrogate for coins and banknotes, which is stored on an electronic device and which is generally intended for the purpose of effecting electronic payments of limited amounts (para. 3 of the preamble and art. 1 para. 3 lit. b).^{16,28,29} It is worth mentioning that the issuer of electronic money is not allowed to create money. Electronic money can therefore only be issued on receipt of funds not less in value than the monetary value issued. Thus electronic money must always be prepaid. The monetary value corresponds to a claim on the issuer. To make transactions possible, electronic money must also be accepted by the counterparty as a means of payment. Technically, mobile electronic money is transferred via the wireless network. Electronic money institutions are the key actors taking real money in order to issue electronic money. They first receive real money from the customer and then exchange the money for points loaded on the prepaid account of the customers, who will be able to use their points to make payments through their mobile phone.

The regulatory and supervisory regime depends on the activity performed by the issuer of electronic money. If the entity issuing electronic money is a credit institution accepting deposits from its customers, the regulatory and supervisory function will be conducted by the financial market authority. If no banking activity is involved but only a mere payment system, no banking licence will be required to issue electronic money. In particular, the receipt of funds does principally not constitute a deposit if the funds received are immediately exchanged for electronic money (art. 2 para. 3).¹⁶ The investment activities of sheer electro-nic money institution cannot be similar to those of credit institutions. This fact pleads for the introduction of a separate prudential supervisory regime which should be less cumbersome and more targeted than the supervisory regime applying to credit institutions (para. 7 of the preamble).¹⁶ In the European Union, there is thus a specific regulation applied to electronic money institutions which are no credit institutions. Electro-nic money institutions are regulated less than banks. However, business activities of electro-nic money institutions must be restricted more than those of credit institutions. The limitations on their investments are aimed at ensuring that their financial liabilities related to outstanding electronic money are backed at all times by sufficiently liquid low risk assets (para. 12 of the preamble).^{16,30}

In the European Union, there are still electronic money institutions which can escape from the regulatory treatment. A waiver indeed exists when only limited amounts are concerned (art. 8).¹⁶ The European regulator proceeds on the assumption that the supervisory regime would be too burdensome on very small electronic money institutions. In Switzerland, there are no specific rules regarding the issuance of electronic money.²⁹ Switzerland often adopts the European provisions on an autonomous basis, however, the Swiss legislator decided not to transform the Electronic Money Directive.

PRUDENTIAL SUPERVISION OF MOBILE BANKING SERVICES

International regulatory frameworks have not established a specific supervisory regime for mobile banking services. As far as a banking activity is concerned, the general rules for credit institutions and banks also apply to mobile banking services providers. National regulators proceed on

the assumption that banking services are concerned and that the particularity of mobile banking merely relates to the fact that banking services can be delivered electronically through mobile devices.³¹ Therefore, designing the regulatory and supervisory regime depends less on the use of mobile telephony to undertake banking transactions than on the targeted banking activity, such as deposit taking or brokerage. This regulatory model suits especially well for banks integrating mobile banking services in their range of activities. Nevertheless, regulators and supervisors should be aware of several distinctive features in mobile banking. Emphasis is put on keeping technological innovations under supervisory oversight in the sense that mobile banking has to remain in the regulated area. Regulators need to take into account the elevated risks relating to innovations coming from outside the banking system. Furthermore, the localisation of customers gives rise to specific concerns related to data security and consumer protection.

Involvement of financial market authorities

The prudential supervision of the banking business means that financial market authorities provide oversight of the regulated area. First and foremost, supervisory authorities grant the right to carry on the business of a credit institution. Before engaging in banking activities, credit institutions must apply for permission to carry on the regulated activities. Credit institutions receive deposits or other repayable funds from the public and grant credits for their own accounts (art. 4 para. 1).²⁴ National authorities are empowered by regulation to supervise credit institutions.

Depending on regulation, the supervisory oversight amounts to integrated financial market authorities or an array of decentralised authorities. If there is a consolidated financial oversight, the financial market authority supervises banking, securities and related financial markets including issues related to money laundering. Indeed enhanced money laundering risks arise from having new channels for depositing and transferring funds. This fact is relevant for mobile banking. Insofar, the issues related to mobile banking services are entirely under the roof of a single authority in jurisdictions having adopted the system of an integrated financial market authority.

The European Community legislation states that Member States must require credit institutions to obtain authorisation before commencing their activities (art. 6).²⁴ The choice of the supervisory system and the requirements for the authorisation fall within the scope of the Member States. For instance in the United Kingdom, the consolidated supervisor is the Financial Services Authority (FSA).³² In Germany, the integrated financial market authority is the Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin).³³ In France, the Commission Bancaire (CB) is the supervisor of the banking industry and the Autorité des Marchés financiers (AMF) the supervisor of the securities sector;³⁴ these two authorities have several cross-sector supervisory powers and partly share the responsibility for the banking and securities segments. In Switzerland, the various sectoral authorities are under the roof the Financial Market Supervisory Authority (FINMA); the FINMA is in charge of giving the authorisation to the supervised entities needing the authorisation under the specific financial market laws.³⁵⁻³⁷

The existence of many supervisory authorities poses problems as regards cross-border banking services. These concerns are especially relevant in the field of mobile banking, thereby tackling new challenges for the financial market authorities. Indeed, the customers can undertake transactions from anywhere and their funds can basically be directed anywhere. These facts make the localisation of mobile banking transactions complicated. Further, the development of new tools such as mobile banking services may help to achieve an increased globalisation in rendering the financial services, which also corresponds to an objective of international trade agreements.³⁸ Globalised finance may foster the expansion of international trade, thereby supporting trade liberalisation. In the European Union, concerns have been raised about the role of finance in the creation of an internal market. Customer confidence in the use of new techniques for the distance marketing of financial services is

considered as a key aspect to allow distance selling.³⁹ Convergence is therefore crucial to the success of the mobile banking business and must be supported by appropriate government policies.⁴⁰

The best response in terms of supervision seems to arise from home country control (p. 82).⁴¹ The financial market authority competent to approve credit institutions shall also supervise their cross-border activities. As it is extremely difficult for them to provide a complete oversight of credit institutions' activities, they also need to cooperate with other financial market authorities, for instance while facilitating the exchange of information. The risk of coordination failure must be minimised in order to avoid inconsistent or contradictory regulatory approaches. Further, a certain harmonisation of the regulatory provisions would foster cross-border banking services, to the benefit of globalised financial services. For instance, regulators should develop common principles regarding mobile banking transactions. This may help to reduce impediments to the development of an efficient market for the electronic delivery of banking services (p. 1).¹⁴

Scope of mobile banking activities

The competent financial market authority is entitled to specify the scope of banking business executed by a financial institution. Only authorised persons are allowed to carry out a regulated activity as far as they get an authorisation (art. 19 para. 1).³² As they fall under the regulated area, these authorised persons must then comply with provisions made by the competent financial market authorities.

The greatest concern of financial market authorities is to make sure that every banking activity is encompassed in financial market regulations and does not stay apart from the supervisory frameworks. For this purpose, emphasis must be put (i) on determining what constitutes a banking activity; and (ii) on defining banks. Banks are primarily active in the financial sector. If a company's balance sheet looks similar to a bank's balance sheet, the target institution should be regulated like a bank. Further, there are specific banking activities that only regulated banks are allowed to perform. The core principle is that only banks are authorised to publicly take deposits and grant credits. Accordingly, depositor protection is an important aspect of banking regulation.

Above all, banking activities include the taking of deposits and the granting of credits.^{34,42,43} An adequate definition of banking activity makes sure that relevant activities do not grow outside the regulated segment. This concern deserves particular attention in mobile banking, as – as mentioned – a subtle demarcation line must be drawn between mobile banking and mobile payment. To some extent, the two systems of making mobile payments can come close to a banking activity. First, when a mobile operator charges customers through the phone bill in the process of collecting a payment for a provider of goods or services, the mobile operator acts as a mere intermediary. The mobile operator takes a certain risk and has to worry about the creditworthiness of the customer. In such cases, the mobile operator is remunerated while sharing a part of the gain with the content provider. The mobile operator makes a transaction possible between the customer and the provider of goods or services while acting as an intermediary. If this activity attains considerable proportions and ends up being considered as banking activity, regulators should intervene and make clear that the targeted mobile regulators must get a banking licence. Practically, this requirement could be concretised with the help of upper limits as regards mobile payments; above a certain amount, the activity would be considered as a banking activity.

Second, when prepaid accounts are created in order to facilitate mobile payments, the proceeding typically implies the issuance of electronic money. This activity is normally not considered as a banking activity. Nevertheless, the entity gathering the money of customers may obtain a great amount of funds at its disposal. If this activity is growing, it could come close to the deposit taking activity of banks. Consequently, the establishment of clear criteria determines whether the offered services constitute banking activities or not. For instance, deposit taking typically involves interest

rates, but not always. The classification of the provided services as a banking activity or not depends to a major extent on how the entity manages the risks related to the money received in exchange for electronic money. There are limits on the activities of electronic money institutions which are no credit institutions. If they want to invest the money that they obtain in the same way like banks, they would have to get a banking licence. Apart from that, the issuance of electronic money is in principle not considered as a banking activity in Switzerland.⁴⁴⁻⁴⁶ The financial market authority could decide to change the practice in cases in which electronic money institutions grow to a considerable extent and develop similar practices to banks. Broadly speaking, regulators could fix limits above which the provided service would be considered as a banking activity; it seems to be adequate that financial market regulations apply as soon as considerable amounts of money are at stake. Otherwise, financial market participants could exploit the regulatory gap in order to bypass financial market regulations.

In the developing world, the establishment of clear criteria and rules defining the different types of mobile financial activities is especially important because of the fact that the demarcation line between mobile banking and mobile payment is extremely blurred. Mobile-money schemes have developed outside the regulated banking sector. This trend is not problematic as long as mobile-money schemes limit balances and transfers and as long as mobile-money services do not pay interest when used like savings accounts.⁹ However, the activities of mobile operators resemble banking activities as soon as the balance sheet of a mobile operator looks similar to a bank's balance sheet. An addition of small amounts can eventually imply that large sums are collected by a non-bank. The fact that people use mobile-money schemes like savings accounts implies risks which should be taken into account by regulators. Collectors of money through mobile devices should be supervised like financial institutions if their customers are considered as depositors. For instance, it would make sense that the rules related to depositor protection apply to them. Regulators cannot content themselves with only looking at the limits of balances and transfers imposed on single customers, but must also look at the nature of mobile operators' balance sheet. Otherwise, non-banks could exploit the regulatory breach in order to be increasingly involved in banking activities. Further, banks could even associate with mobile operators as a means to circumvent the stringent banking regulations. Therefore, clear rules must be established in order to avoid that financial institutions bypass regulations. Even though the creation of mobile-money schemes is extremely promising and beneficial to the developing world, limits must be drawn in order to keep the growth of the mobile sector under an appropriate regulatory oversight.

CUSTOMER TRUST IN MOBILE BANKING

Financial services providers take advantage of establishing a favourable environment in view of the mobile banking adoption. Growing trust is the key issue in this regard. The experience of bank customers in the hands of a few reckless providers may cause them to distrust all similar offerings in the market; providers may therefore enjoy positive externalities from creating appropriate levels of consumer protection which help create trust, leading to more rapid adoption (p. 29).⁵ Therefore, the market as a whole benefits from the establishment of high standards enhancing customer trust. In the context of the liberalisation of financial services, national states are entitled to take the necessary measures to protect bank customers as long as they are not used as a means of avoiding states' commitments resulting from international agreements (para. 2 let. a).³⁸ For this purpose, national states may establish regulatory and legal frameworks to ensure customer confidence in mobile banking services.

Data security

The duty of banks relating to data security and data protection includes two aspects: On the one hand, banks are not allowed to disclose personal data to third parties. On the other hand, data security implies that banks must prevent unauthorised persons from betraying their customers while misusing

their personal data. The banks have to protect their customers against the threat of malware on mobile devices. These duties apply to mobile banking similarly as to traditional banking. Data security contributes to the protection of bank customers. The general rules on data protection apply to financial services providers even when a mobile phone is used to undertake banking transactions.⁴⁷⁻⁵⁰

The adoption of mobile banking services primarily depends on customer trust. The security issue is crucial to the success of the provided services. For instance, users want assurance that their sensitive wireless communications and transactions are not intercepted; before fully accepting the wireless financial applications, they require financial data to be made secure.⁵¹ Security comprises customer identification and authorisation through all the stages of wireless transmission. For security purposes, customer authentication means that the banks need to know whether the customer is authorised to undertake the targeted transaction.⁵² As an example, it can be foreseen that after the transaction has been undertaken by bank customers, the Mobile Transaction Number process would involve transaction confirmation through the mobile phone (p. 219).⁵³ Thereby, transactions-related data are sent to customers via their mobile phone; this check enhances security and customer confidence in the offered services.

If bank customers undertake transactions over wireless networks, the problems relating to online banking apply in the same way in mobile banking. When customers use their mobile phone to undertake transactions through the Internet, the typical malware scenarios known in online banking can occur. Phishing and Pharming are the most common cases of fraud. They occur when customers are deceived through the means of a falsified website which looks similar to the online banking portal (p. 218).⁵³ Customers are generally able to conduct financial transactions on a secure website. Technically, they need a Personal Identification Number (PIN) and a Transaction Number (TAN). Fraud occurs if a falsified website invites the bank customers to give their PIN and TAN and the swindler can use these confidential data later in order to operate an unauthorised banking transaction. In order to avoid these types of fraud, the bank customers must make sure that they write the correct domain name of their bank website and that they do not click on any link in order to access their online banking portal. Customer due diligence may help avoid fraud cases. For this purpose, the bank has the duty to inform its customers on the risks associated with online banking.

In mobile banking, specific concerns have been raised if transactions are undertaken over the mobile network. The attackers of information have partly adapted their methods for the mobile telecommunication sector.⁵⁴ Together with interceptions or mobile viruses, already in circulation, dangers of the identity stealing type can appear by mobile phone phishing, phreacking and hacking.⁵⁴ While the use of mobile banking services has been spreading, the interest of fraudsters in developing new techniques is increasing, thereby leading to new dangers for mobile customers. To a certain extent, mobile operators can play a role in avoiding that unauthorised persons can betray customers during the transmission of data over the mobile network. Mobile operators must take technical and organisational measures to protect personal data against accidental or unlawful destruction, unauthorised disclosure or access because of the fact that the processing involves data transmission over the mobile network. Accordingly, mobile personal devices are well positioned to provide a technical solution for reducing fraud. A certain degree of security is already part of the identification mechanisms of existing mobile phones as a way to prevent call theft; moreover, it is relatively easy and inexpensive for device manufacturers to incorporate additional mechanisms to ensure secure transaction authorisation.⁵⁵

Consequently, electronic banking increases banks' dependence on information technology, thereby increasing the technical complexity of many operational and security issues and furthering a trend towards more partnerships, alliances and outsourcing arrangements with third parties, many of whom are unregulated (p. 5).⁵⁶ This development has been leading to the creation of new business models involving banks and non-bank entities, such as Internet service providers, telecommunication

companies and other technology firms (p. 5).⁵⁶ In particular, as an open network accessible from anywhere in the world by unknown parties, with routing of messages through unknown locations and via fast evolving wireless devices, the Internet significantly magnifies the importance of security controls, customer authentication techniques and customer privacy standards (p. 5).⁵⁶

Customer identification

It is essential in banking to assure that a particular communication, transaction, or access request is legitimate. For this purpose, banks should use reliable methods for verifying the identity and authorisation of new customers as well as authenticating the identity and authorisation of established customers seeking to initiate electronic transactions (p. 13).⁵⁶ In this regard, digital signatures play a crucial role. The various methods used by banks include PIN numbers, passwords, smart cards, digital certificates as well as biometric identifiers (p. 29).⁵ The security mechanisms such as Public Key Infrastructure (PKI) contribute to the creation of a safety environment.⁵⁴ PKI are arrangements needed to manage digital certificates; they bind public keys with respective user identities.

In the future, biometric technology will play an increasing role in data security and customer authentication related to the execution of financial services. Promising tools are the use of fingerprints and voice recognition. Fingerprints can be an easy way to identify bank customers. In Africa and India, pilot projects aim at introducing fingerprints in mobile banking with the objective of supporting poor and uneducated people.⁵⁷ In developing countries, substantial funds still remain outside the banking system. Attempts to develop mobile banking services correspond to the transformative model, as targeted customers are unbanked people. The technology has already been developed sufficiently. Mobile phones could be easily equipped with fingerprint readers. However, the use of fingerprints as digital signatures has not yet spread in mobile banking. This could be a possible trend in the future, not only in developing countries but also in industrialised countries.

Apart from that, the Know Your Customer (KYC) rule applies across all types of bank accounts (p. 32).⁵ This rule also applies in mobile banking in order to avoid too loose contractual relationships between banks and their customers. As a part of identifying its customers, the bank has to know their profile.

Consumer protection

Consumer protection goes beyond the requirements resulting from data security and customer identification. Generally, the bank owes a fiduciary duty to its customers. The bank shall comply with its duties in order to gain customer trust. In mobile banking, the close bank-customer relationship does not exist any longer. Therefore, the question arises as to whether the bank's fiduciary duties can be materialised in mobile banking. For instance, the duties of loyalty, information, advice and diligence cannot be fulfilled exactly in the same way like in traditional banking. Owing to the fact that these duties must be present in all types of banking services, a satisfying way has to be found in order to incorporate them in mobile banking.

The rationale for developing consumer protection standards depends on various aspects. On the one side, customer identification is imposed on banks for a public purpose, namely to combat money laundering. The requirement that the customer must go personally to the bank office while opening a new account relates more to public security than to consumer protection. Therefore, the purely electronic opening of a bank account through mobile devices cannot materialise in practice.⁵⁸ On the other side, consumer protection is also in the interest of banks. If the bank acquires customer confidence, customers adopt the mobile banking services more easily.

Specific concerns have been raised in the virtual world in terms of ensuring consumer protection. In particular, mobile accounting or mobile brokerage cannot be conceived without mobile financial information. The use of mobile telephony makes information easily available from anywhere

and at anytime. If banks develop their system of providing financial information through mobile devices in a sufficient way, the provided services can have a high value and replace the close bank-customer relationship to some extent. The advantage of financial information through mobile devices consists in the fact that customers are kept up-to-date with the status of their funds. They can, for instance, receive alerts as soon as they approach their account limit, which is a very valuable information. Through mobile phones, banks can reach their customers efficiently. Moreover, mobile phones may help customers locate the next branch office easily, making it easier for customers to access their bank if needed. Therefore, mobile phones can become a helpful instrument enabling customers to make informed judgments.

Last but not least, the banking industry recognises the need for transparency to promote confidence and acceptance of electronic commerce, such as mobile banking (p. 14).¹⁴ Transparency is highly valued by customers, as they wish to obtain access to relevant market information in the easiest and the most comprehensible way possible (p. 87).⁴¹ Mobile banking offers banks broader perspectives as regards the means to disclose appropriate information to customers. Therefore, the new information channel provided by the use of mobile devices in banking may even help banks to reduce some information asymmetries between them and their customers. With mobile devices, bank customers can be reached with relevant information rapidly and independently of their location; the additional means of communication available help to cover the customers' need for specific information and to enhance the transparency of the bank's practices.

MOBILE OPERATORS' POSITION IN MOBILE BANKING

Mobile operators can play different roles in the mobile commerce value chain. They may appear as collectors and payment agents of cash not only for themselves but also for third parties. As far as mobile banking is concerned, various models are possible depending on how intensively the mobile operator interferes in the banking process. With respect to a pure bank-driven model, mobile operators only take care of the mobile network. They stay outside the banking business involving bank accounts. At any rate, through generating more traffic on the network, mobile banking may make mobile operators more profitable (p. 34).⁵ If mobile operators effectuate mobile payments through the phone bills or a prepaid account, they may come closer to the banking business. If mobile operators pool individual deposits into one aggregated account at a bank, the boundaries between financial and non-financial institutions may become blurred. Thereby, emphasis must be put on the risks taken by mobile operators in order to evaluate their role in the banking process. Even if they do not directly exert a banking activity, the risk profile of the business of mobile operators may change as they become increasingly involved in making banking services available. Lastly, mobile operators may technically act like short-term deposit banks if they perform payment processing functions traditionally carried out by banks between their customers and third parties. In such cases, mobile operators should be required to obtain a banking licence before engaging in banking activities.

Regardless of the chosen model, mobile operators take increasingly part in mobile financial services. They play a crucial role in the expansion of the business. From a regulatory and supervisory point of view, this fact implies that telecommunication regulators will inevitably have to coordinate and share information with bank regulators (p. 34).⁵ From a banking perspective, the arrangements between banks and mobile operators lead to an outsourcing of the front end of the deposit taking business. In some regimes, the deposit taking function is viewed as being so core to banking business that deposit taking outside secure bank premises is prohibited; even in regimes where there are no explicit prohibitions, regulators may be very cautious in respect of outsourcing the collection of deposits to agents because of the risk of fraud and loss of reputation of the banking sector (pp. 31–32).⁵ Furthermore, the specific aspects relating to consumer protection play a role in cases in which mobile operators try to serve as financial institutions by granting credit for micropayments.²⁰ If mobile

operators are allowed to provide mobile phone holders with a loan, legal provisions have to apply in order to comply with customers' needs. Notably, legal frameworks must protect consumers against unfair or misleading practices.⁵⁹⁻⁶¹ Credit agreements concerning mobile payment may fall within the scope of the EC Directive if they involve an amount over 200 Euros, if they do not have to be repaid within 1 month and if they are not granted free of interest (art. 2 let. c, e and f).⁵⁹

CONCLUDING REMARKS

In sum, the use of an innovative technology can be considered as a great opportunity in the banking business. The use of mobile devices to effectuate banking operations has an especially encouraging future in the developing world as a means to reduce poverty. The expansion of mobile banking services deserves to be supported by a favourable regulatory and supervisory system. As the mobile world is fast evolving, there is no point in completely restricting technological innovations. Nevertheless, regulators shall anticipate the dangers arising out of mobile banking and focus on maintaining the growth of the sector in the regulated area. Regulators must care about not allowing unregulated entities to circumvent their regulations.

In order to develop mobile banking in the future, much concern has been raised about creating an environment fostering customer trust in the banking services. Without customer trust, mobile banking cannot grow successfully. There is a need to promote customer confidence in the electronic payment instruments. Mobile banking is a promising tool in the future. If the technology has already been sufficiently developed, the next step consists in enhancing customer trust in the offered services. Regulatory and legal frameworks may be able to respond to this objective.

In particular, it is in the interest of mobile banking that the demarcation line is properly drawn between mobile banking and mobile payment. Mobile banking services fall under a more stringent regulatory treatment and confidence in mobile banking may increase if bank customers understand the distinction. Furthermore, the regime applied to mobile payment should not be too loose either. Typically, customers first execute mobile payments and they would not adopt mobile banking afterwards if they are not satisfied with mobile payments. Mobile banking may thus enjoy positive externalities from the success of mobile payments in the light of the customers' expectations.

REFERENCES AND NOTES

- 1 Tiwari, R. and Buse, S. (2007) *The Mobile Commerce Prospects: A Strategic Analysis of Opportunities in the Banking Sector*. Hamburg, Germany: Hamburg University Press.
- 2 International Organization of Securities Commissions (IOSCO). (2001) Report on Securities Activity on the Internet II. June, p. 9.
- 3 Committee on Payment and Settlement Systems of the Bank for International Settlements (BIS). (2004) Survey of developments in electronic money and internet and mobile payments. March, p. 3.
- 4 Riivari, J. (2005) Mobile banking: A powerful new marketing and CRM tool for financial services companies all over Europe. *Journal of Financial Services Marketing* 10(1): 11–20, 14.
- 5 Porteous, D. (2006) The Enabling Environment for Mobile Banking in Africa. Report Commissioned by Department for International Development (DFID).
- 6 *Economist*. (2009) The power of mobile money. 24 September, p. 13.
- 7 Barnes, S.J. (2002) The mobile commerce value chain: Analysis and future developments. *International Journal of Information Management* 22: 91–108.
- 8 The Third Generation phone (3G phone) is a family of standards for wireless communications defined by the International Telecommunication Union (ITU). See <http://www.itu.int/home/imt.html>, accessed 26 October 2009.

- 9 *Economist*. (2009) Beyond voice, new uses for mobile phones could launch another wave of development. *Mobile Marvels, A Special Report on Telecoms in Emerging Markets*, 26 September, pp. 12–15.
- 10 *Economist*. (2009) Finishing the job, mobile-phone access will soon be universal. The next task is to do the same for the internet. In: *Mobile marvels. A special report on telecoms in emerging markets*, 26 September, pp. 15–16.
- 11 Jarvenpaa, S.L., Lang, K.R., Takeda, Y. and Tuunainen, V.K. (2003) Mobile commerce at crossroads. *Communications of the ACM* 46(12): 41–44, 44.
- 12 Georgi, F. and Pinkl, J. (2005) Mobile banking in Deutschland: Der zweite Anlauf. *Die Bank, Zeitschrift für Bankpolitik und Praxis*, March: 57–61.
- 13 See generally Zimmermann, S. (2008) E-commerce, Verbraucherschutz und die Entwicklung Intelligenter Agenten. In: J. Costede and S. Spindler (eds.) *Schriften zum Wirtschafts- und Medienrecht, Steuerrecht und Zivilprozessrecht*, Band 35. Frankfurt am Main, Germany: Peter Lang, p. 11.
- 14 Basel Committee on Banking Supervision (BCBS). 2000) EBG Initiatives and White Papers. Electronic Banking Group Initiatives and White Papers, October.
- 15 Directive 2007/64/EC on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, OJ L 319/1.
- 16 Directive 2000/46/EC on the taking up, pursuit of and prudential supervision of the business of electronic money institutions, OJ L 275/39.
- 17 Hinds, D. (2004) Micropayments: A technology with a promising but uncertain future. In: N. Mallat, M. Rossi and V.K. Tuunainen (eds.) *Mobile Banking Services. Communications of the ACM* 47(5): 42–46, 44.
- 18 For instance, in the United Kingdom the relevant authority is the Office of Communications. See the Communications Act 2003, c. 21.
- 19 Art. 4 of the Swiss Federal Act of 30 April 1997 on Telecommunications (Telecommunications Act), SR 784.10. No authorisation like in mobile banking is required but a mere registration. Nevertheless, art. 6 of the law states legal requirements for telecommunication services providers.
- 20 Mallat, N., Rossi, M. and Tuunainen, V.K. (2004) Mobile banking services. *Communications of the ACM* 47(5): 42–46, 45.
- 21 Cheney, J.S. (June 2008) An Examination of Mobile Banking and Mobile Payments: Building Adoption as Experience Goods? Discussion Paper, Payment Cards Center, Federal Reserve Bank of Philadelphia.
- 22 See below, Scope of mobile banking activities.
- 23 See further Weber, R.H. (2001) *E-Commerce und Recht, Rechtliche Rahmenbedingungen elektronischer Geschäftsformen*. Zurich, Switzerland: Schulthess, pp. 597–598.
- 24 Directive 2006/48/EC relating to the taking up and pursuit of the business of credit institutions, OJ L 177/1.
- 25 <https://www.postfinance.ch/pf/content/en/seg/priv/prod/pay/national/mobile>, accessed 26 October 2009.
- 26 <http://www.saxobank.com/en/trading-platforms/pages/mobile-phone.aspx>, accessed 26 October 2009.
- 27 <http://www1.banking.firstdirect.com/1/2/ourservices/mobile-banking>, accessed 26 October 2009.
- 28 See Weber, R.H. (1999) Elektronisches Geld, Erscheinungsformen und rechtlicher Problemaufriss. In: D. Zobl, M. Giovanoli and G. Hertig (eds.) *Schweizer Schriften zum Bankrecht*. Zurich, Switzerland: Schulthess, p. 47.

- 29 See Weber, R.H. (2001) E-money and regulation in Switzerland and in the EU. *Finance & Technologie* 77: 40–41, 40.
- 30 See para. 4.2.3, 4.3.2–4.3.7 and 6.9.1 of the FSA Handbook, Electronic Money (ELM).
- 31 See Bacchetta, M. Low, P. Mattoo, A. Schuknecht, L. and Wehrens, H.W.M. (1998) *Electronic Commerce and the Role of the WTO*, In: Special Studies 2. Geneva, Switzerland: WTO Publications, p. 52.
- 32 See Financial Services and Markets Act 2000 (FSMA 2000), c. 8.
- 33 The Federal Financial Supervisory Authority BaFin is established by the Gesetz über die Bundesanstalt für Finanzdienstleistungsaufsicht (FinDAG).
- 34 In France, see the Monetary and Financial Code (Code monétaire et financier, CMF). The AMF was established by art. L621-1 and the CB by art. L613-1. As regards the definition of banking activities, art. L311-1 states that banking operations include the taking of deposits and the granting of credits.
- 35 Art. 3 let. a of the Swiss Federal Act of 22 June 2007 on Financial Market Supervision (FINMA Act), SR 956.1.
- 36 See Art. 3 para. 1 of the Swiss Federal Act of 8 November 1934 on Banks and Savings Banks (Banking Act), SR 952.0.
- 37 See art. 10 of the Swiss Federal Act of 24 March 1995 on Stock Exchanges and Securities Trading (Stock Exchange Act, SESTA), SR 954.1.
- 38 See Annex 1B, Annex on Financial Services of the General Agreement on Trade in Services (GATS).
- 39 Para. 5 of the preamble of the Directive 2002/65/EC concerning the distance marketing of consumer financial services and amending Council Directive 90/619/EEC and Directives 97/7/EC and 98/27/EC, OJ L 271/16.
- 40 See further, A Global Action Plan for Electronic Business, Prepared by Business with Recommendations for Governments (2002) 3rd edn., July, p. 19.
- 41 Gkoutzinis, A. (2003) Cross-border electronic banking activities in the single European market and the normative value of home country supervision. *Journal of Banking Regulation* 5(1): 78–103.
- 42 In the United Kingdom, see para. 4 and 22 of Schedule 2 of the Banking Act 2009, c. 1.
- 43 In Germany, see art. 1 of the German Banking Act (Kreditwesengesetz, KWG).
- 44 Federal Banking Commission (FBC) Annual Report 1998 (German version), pp. 55–56.
- 45 FBC Annual Report 1999 (German version), p. 101.
- 46 Flühmann, D. (2009) Aktuelle aufsichtsrechtliche Fragestellungen des electronic banking. In: U. Bertschinger (ed.) *St. Galler Schriften zum Finanzmarktrecht*, Band 4. Zurich, Switzerland: Dike Verlag AG, p. 9.
- 47 In the European Union, see Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive), OJ L 281/31. This Directive is implemented by Member States.
- 48 See in the United Kingdom, the Data Protection Act 1998, c. 29.
- 49 See in Germany the Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG).
- 50 In Switzerland, see the Swiss Federal Act of 19 June 1992 on Data Protection (Federal Data Protection Act, DPA), SR 235.1. No generally applicable data security standard has been adopted by the Swiss legislator, as Swiss law fosters more detailed and customised data security standards developed by private institutions.
- 51 Tarasewich, P., Nickerson, R.C. and Warkentin, M. (2002) Issues in mobile e-commerce. *Communications of the Association for Information Systems* 8: 41–64, 49–50, 52.
- 52 Weber, R.H. and Willi, A. (2006) *IT-Sicherheit und Recht, Grundlagen eines integrativen Gestaltungskonzepts*, In: ZIK. Band 33. Zurich, Switzerland: Schulthess, pp. 13–14.
- 53 Kahler, T. and Werner, S. (2007) *Electronic Banking und Datenschutz*. Berlin, Germany: Springer.

- 54 Rusu, D. and Dospinescu, O. (2004) Mobile banking services in Romania, <http://www.ssrn.com>, accessed 26 October 2009, p. 9.
- 55 Herzberg, A. (May 2003) Payments and banking with mobile personal devices. *Communications of the ACM* 46(5): 53–58, 54.
- 56 BCBS. (2003) Risk management principles for electronic banking. July, p. 5.
- 57 Kahn, J. (2008) Banking, with fingerprints and house calls. *The Boston Globe*, 20 January.
- 58 See FBC Annual Report 2000 (German version), p. 19. 59 Directive 2008/48/EC on credit agreements for consumers and repealing Council Directive 87/102/EEC (Consumer Credit Directive) OJ L 133/66.
- 60 In the United Kingdom, see the Consumer Credit Act 2006 (CCA), c. 14.
- 61 In Switzerland, see the Swiss Federal Act of 23 March 2001 on consumer credit (Consumer Credit Act, Konsumkreditgesetz, KKG), SR 221.214.1.