Harry Leinonen – Veikko Saarinen

Payment system risks in Finland and the need for regulation and supervision

SUOMEN PANKKI
Bank of Finland

BANK OF FINLAND STUDIES A:101 • 1998

ISBN 951-686-577-1
ISSN 1238-1683

Oy Trio-Offset Ab
Helsinki 1998

Abstract

Regulation and control of payment system risks can be justified by the fact that, since payment systems are an integral part of the financial sector infrastructure, disturbances therein can spread widely through the society. The payment system risks that need to be controlled are classified here in the following basic categories: credit risks; liquidity risks; environment risks; clearing and settlement risks; and operating risks. Payment systems subject to supervision are categorized by the payment media used, so that the risk profiles within in each category are as uniform as possible. The report also discussed means of reducing payment system risks.

The report scrutinizes in particular the risks inherent in Finnish payment and settlement systems. In Finland overall payment system regulations and norms are based on legislation governing credit institutions, the Bank of Finland and the Financial Supervision Authority as well as on self-regulation. The Bank and the Financial Supervision Authority are jointly responsible for the supervision of Finnish payment systems. The Bank is responsible for controlling systemic risk and for overseeing payment systems as a whole, and the Financial Supervision Authority supervises and monitors individual credit institutions in respect of payment system risks. Because risks are constantly changing, regulation and supervision of payment systems need to be continually updated. As the new operating environment including the European Central Bank and the ESCB unfolds, new features will mark the supervision of payment systems and in general we will see more intense international cooperation in the area of payment systems.

Key words: payment systems, payment transactions, regulation, supervision, risks.

Tiivistelmä

Maksujärjestelmäriskien sääntelyä voidaan perustella sillä, että maksujärjestelmissä esiintyvät häiriöt voivat näiden järjestelmien merkittävän aseman vuoksi levitä laajalle yhteiskuntaan. Valvottavat riskit on tässä raportissa jaettu luotto-, likviditeetti-, ympäristö-, clearing- ja settlement- sekä toiminnallisiin riskeihin. Valvottavat maksujärjestelmät on esitetyssä riskikehikossa jaoteltu riskiprofiileittain mahdollisimman yhtenäisiin luokkiin. Raportissa esitetään keinoja maksujärjestelmäriskien vähentämiseksi.

Raportissa tarkastellaan erityisesti suomalaisissa maksu- ja selvitysjärjestelmissä esiintyviä riskejä. Maksujärjestelmien yleinen sääntely ja normisto ovat Suomessa perustuneet luottolaitoslainsäädäntöön, lakeihin Suomen Pankista ja Rahoitustarkastuksesta sekä itsesääntelyyn. Maksujärjestelmien viranomaisvalvonnasta vastaavat Suomessa Suomen Pankki ja Rahoitustarkastus yhdessä. Edellinen vastaa systeemiriskistä ja valvoo maksujärjestelmiä kokonaisuutena, jälkimmäinen vastaa yksittäisten luottolaitosten maksujärjestelmäriskeistä ja niiden valvonnasta. Koska riskit muuttuvat kaiken aikaa, maksujärjestelmien valvonnan kehittämisen tulee olla jatkuvaa. EKP ja EKPJ tuovat uusia piirteitä maksujärjestelmien valvontaan, ja yleensäkin kansainvälinen yhteistyö maksujärjestelmissä on lisääntymässä.

Asiasanat: maksujärjestelmät, maksuliike, sääntely, valvonta, riskit

Preface

Payment systems are an essential part of the infrastructure of a monetary economy. The efficiency that derives from specialization in economic activity cannot be fully exploited without reliable payment systems. In a modern society, households, enterprises, investors in the securities market, foreign exchange dealers etc are highly dependent on payment systems, which have become a part of everyday life. They are hardly noticed – until a disturbance occurs.

Disturbances may have far-reaching consequences. In this sense payment systems can be compared to road traffic. An accident or a disturbance can quickly jam an important route, thereby causing damage and difficulties, also to third parties. Central banks pay close attention particularly to such systemic effects. It is generally agreed that central banks play an important role in ensuring the continuous functionality of payment systems. This stems from their central role in interbank payment systems as well as their objective of promoting monetary stability. In the Statute of the European System of Central Banks, this task is described as 'promoting the smooth operation of payment systems'. The Act on the Bank of Finland states that, along with its other tasks, the Bank is to 'participate in maintaining the reliability and efficiency of the payment system and overall financial system'.

Even though central banks have traditionally had such responsibility – in fact, the origin of central banking derived to a large extent from the need to enhance the functionality of payment systems – the importance of it has been underscored in recent years. This is due to rapid growth in foreign payment transfers, which has increased the risk and contagion of disturbances. The increasing integration of economies and payment systems in connection with the Economic and Monetary Union has spurred central banks' own and cooperative efforts in this field. This study is based on objectives and guidelines defined as a result of international cooperation and on the statutory tasks of the Bank of Finland. It has been carried out in cooperation with the Financial Supervision Authority, which is administratively connected with the Bank. We have also tried to make use of studies conducted in other central banks, especially Banca d'Italia.

This study describes payment system risks and possibilities of reducing them and outlines a framework for monitoring payment systems. The supervisory framework and procedures will need to be

developed further on the basis of monitoring experience and particularly the preparatory work being done under the auspices of EMI/ECB. The study also provides information to supervised entities as to the objectives and content of supervision, ie the thinking behind supervision.

Payment system risks and the need for supervision were studied in 1996–1997 by a working group headed by Harry Leinonen of the Bank of Finland. The other participants members were Risto Herrala and Ilkka Vasara from the Bank of Finland and Harri Hirvi, Risto Nieminen, Veikko Saarinen and Ari Voipio from the Financial Supervision Authority. The working group's efforts were guided by a steering group, chaired by Ralf Pauli from the Bank of Finland and including Heikki Koskenkylä from the Bank and Kaiju Kallio and Veli-Pekka Valori from the Financial Supervision Authority. This publication is largely based on the group's findings.

Helsinki, 2 March 1998

Ralf Pauli
Adviser to the Board

Executive summary

In recent years, considerable attention has been devoted to the risks inherent in payment systems, in both large and small countries (eg G-10, G-20 and EU countries). This has been due inter alia to a substantial increase in the size of the risk exposures related to payments and their settlement, deficiencies in the risk management and supervision or oversight of payment systems, lags in legislation and other regulation, the increasing difficulty of controlling payment systems owing to their automation and integration, and the danger that systemic risk could spread more rapidly in the case of a disturbance.

The need for the regulation and supervision of payment systems has generally been justified by the fact that while payment and settlement systems are an integral part of the financial sector infrastructure, they also form a channel through which various disturbances may spread widely in the society. From the standpoint of safeguarding the functionality of the society, it has been felt that the most important objective of payment systems supervision/oversight is to promote systems stability and security. Other reasons for having supervision of payment systems include externalities, asymmetric information among system participants and the prevention of misuse and crime.

Regulation of payment systems may be carried out by the authorities, the banking industry, the markets or the service providers themselves. Regulation can be implemented properly only after the risks in question have been identified and the need to regulate them has been assessed. Regulation and supervision should be continually developed by utilizing the latest data on risks and supervisory findings, in order to keep the supervisory function up to date in an environment where risks are constantly changing. Regulation and supervision must be cost-effective and so far as possible based on self-regulation (provided the incentive is there).

The risks to be monitored should be clearly defined and the probabilities and consequences of their realization should be estimated. In this report, payment system risks have been classified into the following basic categories: credit risks; liquidity risks; environment risks; operating risks; clearing and settlement risks; and systemic risk, which is the product of the other risks. The definition of risks has been done from the standpoint of the payment system, because this is useful for supervisory and analytical purposes. The

report does not estimate the probabilities of risk realization because of a lack of the required historical data. Such data should be collected in Finland and abroad so as to enable us to improve our forecasting, description and quantification of risks.

In the above-mentioned risk classification scheme, payment systems subject to supervision are categorized on the basis of the payment media used, so that the risk profiles within in each category are as uniform as possible. The categories are cash and small-value noncash payment instruments, small-value credit transfers, documentary payments, large-value cheques and large-value credit transfers. The borderline between a small-value (retail) payment and a large-value payment is fuzzy, but in most cases it is FIM 50 000 – 100 000. Special credit risks are associated with payments that exceed FIM 10 million or FIM 100 million. The report contains a table with cross-comparisons of all the different risk and payment system categories and rough estimates (indicated by letter symbols) of the risks associated with each payment system category. In general, it may be noted that the most visible risks are those associated with criminality, information systems and management. Risks that materialize more seldom are environment risks, clearing and settlement risks and systemic risk. The most harmful risks are those inherent in large-value payment systems and systemic risk.

Effective control and supervision of payment system risks requires effective means of reducing (controlling) risk. The principal risk control means for credit risks and liquidity risks are gross settlement, credit limits, collateral requirements, irrevocable netting of payments and payment finality rules. The main means of controlling operations risks are good payments intermediation and data processing procedures, sufficient controls and guidance, backup operating facilities and a written security policy. The most important means of controlling risks associated with the operating environment are monitoring and impacting legislative changes; accurate and timely detection of problems; and preparation for technical changes and crisis situations. Systemic risk may be prevented by effective monitoring of the basic risks; payment system structures that prevent the spread of systemic risk; and effective central bank liquidity policy.

In Finland payment system regulation is based on credit institution legislation, laws governing the Bank of Finland and the Financial Supervision Authority, and self-regulation. Until now, there have been no special laws or regulations governing payment systems, but legislation on netting has been enacted recently and legislation is

being drafted on credit transfers and settlement finality. The EU, EMI, BIS, various standardization bodies etc have issued guidelines and minimum standards in order to promote the reliability and security of payment transactions. On the basis of these standards, the Bank of Finland, the banks and the Financial Supervision Authority have further developed the structures, risk management and supervision of domestic payment systems. The aim is to ensure that Finnish payment systems and their supervision comply with international recommendations and the requirements of Stage three of EMU, by the end of 1998.

The Bank of Finland and the Financial Supervision Authority are jointly responsible for the supervision of payment systems in Finland. The Bank of Finland is responsible for monitoring systemic risk and overseeing payment systems as a whole, whereas the Financial Supervision Authority is responsible for monitoring the payment system risks of individual credit institutions. In this report, this division of duties has been analysed in more detail by breaking down the duties into regulation, supervision/oversight, information and development.

Because risks are constantly changing, regulation and supervision of payment systems must be developed on an ongoing basis. The main areas that currently appear to require further development are the collection of data on risks; establishment of a risk database; increasing the effectiveness of regulation by breaking it down into regulation by the industry, market regulation and self-regulation; and by more effectively utilizing the possibilities offered by the corresponding categories of supervision.

It is of crucial importance to follow international developments in the field of payment system regulation and supervision and the discussion on these matters within the European System of Central Banks (ESCB) and the Bank for International Settlements. The European Central Bank and the ESCB will introduce new features to the supervision of payment systems, and international cooperation in the field of payment systems in general is intensifying (cf TARGET, RTGS, EBA-clearing and development of securities settlement systems).

Contents

1 Introduction

The purpose of this report is to present a summary of the concepts of payment system risks, both micro and macro, and to examine these from the viewpoint of payment systems in Finland. The aim is to study various payment system risks and determine the possibilities for reducing and controlling them. A risk classification scheme is developed and used as an analytical and monitoring tool in respect of payment and settlement system risks.

Payment system monitoring is examined from the authorities' viewpoint, but self-regulation is not entirely excluded. The latter is examined only briefly in terms of broad principles, as a deeper treatment of the subject would require a more comprehensive study than that presented here.

We begin with a description of the international development of payment systems and the general principles and challenges pertaining to system monitoring and regulation. Payment system risks, their classification and evaluation, as well as the development of a comprehensive risk framework form the core of this study. The part devoted to the organization of supervision deals with cooperation between authorities, eg the Bank of Finland and the Financial Supervision Authority (FSA), and the division of responsibility. The final chapter presents a summary of the main areas of regulation, supervision and developmental need as well as a look at what lies ahead in terms of international cooperation.

The report focuses on the new aspects in the development and monitoring of payment and settlement systems that present challenges to both central banks and banking supervisors and that demand a new kind of cooperation in the development of monitoring and the defence against systemic risk.

2 International developments

The development of payment systems and reduction of related risks have involved broad international cooperation, which has become even closer in the 1990s. The need for cooperation has been underlined by the nearly explosive growth in payment transfers, especially international transfers, during the past twenty years, as a result of dismantlement of foreign exchange control, globalization of financial markets and technical innovations. These changes have presented notable challenges to banks, in respect of practices and procedures in the provision of payment services, as well as to banking supervisors.

2.1 International cooperation in payment systems

Cooperation between central banks in the development of payment systems goes back to 1980, when the Bank for International Settlements (BIS) founded its Group of Experts on Payment Systems. However, it was not until 1989 that the G-10 countries published their first report on payment systems, which dealt with the risk implications of netting (Report on Netting Schemes). The so-called Lamfalussy report (Report on Interbank Netting Schemes), published in the following year, contains the well-known Lamfalussy minimum standards for multilateral netting systems and recommends certain general principles for monitoring them.

In 1992 the BIS Group of Experts became the Committee on Payments and Settlement Systems (CPSS) of the G-10 countries' central banks. The CPSS has prepared numerous highly regarded reports on reducing payment and settlement system risks, in cooperation with the G-10 countries. A report on enhancing securities settlements (Delivery versus Payment in Securities Settlement Systems) was published in 1992, and a report on international securities settlements (Cross-Border Securities Settlements) in 1995. In 1993 the Committee published a report on reducing risks in cross-border and multicurrency transactions by using central banks' payment and settlement services. A report titled 'Settlement Risk in

Foreign Exchange Transactions' was published in 1996; as a result, the central banks imposed a two-year time limit on banks during which they are to reduce these risks. Some private organizations, eg the largest banks in the G-20 and G-30 countries, IOSCO, FIBV and ISSA have also made recommendations for reducing foreign exchange, securities and derivatives settlement risks.

2.2 Payment systems cooperation in the EU

Payment systems cooperation between central banks began in 1991, when an ad hoc working group on payment systems was set up under the governors of EU central banks. After the EMI was established, this working group was named the Working Group on EU Payment Systems (WPGS). The WPGS has addressed four central aspects of the completion of the single market and preparation for Stage Three of EMU: monitoring of the ECU clearing system, harmonization of the main features of EU-country payment systems, central bank cooperation in the oversight of cross-border payments and planning of the payment system, as required by the single monetary policy.

The EU adopted the real-time gross settlement (RTGS) principle as a model for risk reduction in European payment systems, and each EU country is required to implement an RTGS system by the end of 1997. Linking together the national RTGS systems via central banks (Interlinking connection network) was seen as a way of creating a secure EU-wide real-time gross settlement system (TARGET) for settling payments related to the single monetary policy.

2.3 General principles for payment system supervision in the EU

The EU and the EMI in 1993–1994 drafted common procedures for use by central banks and bank supervisors in respect of payment systems supervision, related cooperation, and information exchange. The authority for overseeing payment systems is included in the Maastricht Treaty and the ECB Rules. Under Article 105 of the Treaty, one of the basic tasks of the ECB is to promote the smooth operation of payment systems. Article 22 of the ECB Statutes states that the ECB and national central banks may provide facilities, and the ECB may make regulations, to ensure efficient and sound clearing and payment systems within the Community and with other countries.

Supervision of EU payment systems is a cooperative task of the ECB, national central banks and bank supervisors. The central banks are responsible for the broad oversight of the systems and the bank supervisors for supervision of participating institutions. The EMI has prepared guidelines containing general principles for supervision and exchange of information between authorities.

The EMI was given the specific task of broad oversight of the EBA Clearing System, which it has done since January 1994. This system handles the settlement of ECU-denominated payments. The EMI has worked to ensure that the ECU Banking Association (EBA), which manages the system, enhances system risk management at least enough to meet the Lamfalussy minimum standards. It has been agreed that multilateral-multicurrency netting centres will be overseen by a single central bank (just as the Bank of England is responsible for the broad oversight of the London-based ECHO), which will coordinate the oversight activities of the central banks whose currencies are netted in the system.

To ensure the stability of electronic money systems, the EMI working group on electronic money is updating the 1994 recommendation. In order to get regulation quickly in place, the EU Commission in 1997 drafted a directive on electronic money issuance and a recommendation for minimum requirements for electronic payment instruments aimed at improving consumer protection. A directive on regulating cross-border credit transfers was issued in 1997, which is to be incorporated in member states' national legislation by 14 August 1999. The directive applies to transfers up to the equivalent of ECU 50 000.

2.4 Statutory duties of central banks in respect of payment systems

In connection with reform of banking and finance legislation, a number of countries have included payment system oversight and maintenance of stability as one of the main duties of the central bank, because of the systemic risk involved. Traditionally, almost all central banks have offered secure payment services to banks by operating large-value interbank funds transfer systems. In Finland this practice has been written into the new Act on the Bank of Finland, which will enter into force on 1 January 1998: 'The Bank of Finland shall also ... participate in maintaining the reliability and efficiency of the payment system and overall financial system and participate in their development'. For interbank payment transfers and settlements of various netting systems, the Bank operates a real-time gross settlement system (BoF-RTGS), in which payments are settled with central bank funds and have immediate finality.

In Sweden also, maintenance of the stability and efficiency of payment systems is among the statutory duties of the central bank. The bank operates the RIX system for large-value interbank funds transfers. The Swedish central bank focuses on three areas of payment system oversight: infrastructure, ie systems for payment and securities transactions; enterprises that play a central role in payment and settlement systems; and updating of regulations governing financing operations and payment systems.

Norway has drafted a legislative framework for all payment transfers, which would give the Norwegian central bank considerable responsibility for oversight and regulation of large-value fund transfers. The central bank would also be responsible for licensing large-value fund transfer systems. Small-value payments would fall under the purview of the banking supervision body. The draft legislation is to be introduced to the parliament in spring 1998. Also in Canada, it has been proposed that separate legislation concerning payment clearing and settlement should be passed in order to reduce systemic risk.

In Italy, Article 146 of the 1993 Banking Law assigns the Banca d'Italia the task of overseeing the payment system, giving it the power to 'issue regulations to ensure the efficiency and reliability of clearing and payment systems'. The Bank of England is a member of the umbrella organization of payment systems, APAC, and issues

settlement accounts to clearing banks participating in the large-value funds transfer system CHAPS.

The US Federal Reserve provides its own payment system for large-value funds transfers, Fedwire, and guarantees finality of the payments. Since mid-1996 the Federal Reserve has required that multilateral netting systems, such as CHIPS, fulfil the Lamfalussy minimum standards. In Australia it was proposed, in connection with the reformation of banking supervision, that a special Payment Systems Board, responsible for regulation and oversight of payment systems, be set up within the central bank. Under a new legislative proposal, the central bank of Japan will guarantee smooth settlement of payments between financial institutions and thus contribute to the maintenance of a stable financial system. The Japanese central bank is currently converting its payment system (BOJ-NET) into a real-time gross settlement system, and is requiring that participating netting systems (FEYCS) fulfil the Lamfalussy minimum standards.

2.5 Results of international cooperation in respect of payment systems

International cooperation in the area of payment and settlement system risks has resulted in numerous practical improvements in risk management, such as implementation of risk-reducing netting procedures, minimum standards and real-time gross settlement systems, as well as implementing recommendations concerning traditional payments, foreign exchange and securities transactions, and settlement of derivatives transactions. Various systems have been available for bilateral netting of currency transactions, such as FX-NET, ACCORD and VALUNET. Multilateral netting of currency transactions are handled by London-based ECHO (Exchange Clearing House), established in 1996, and by Multinet Bank in New York, established in 1997. Large private banks in G-20 countries have also began developing a payment versus payment (PVP) system for linking together foreign exchange transactions, and have proposed the establishment in London of a company offering continuous linked settlement (CLS) services. Such a company would provide a real-time system for settling foreign exchange transactions starting in 2000. According to advance information ECHO, Multinet and the CLS

initiative of the G-20 countries will combine their activities so as to eliminate redundancies.

The EMI and the EU countries have jointly prepared minimum standards for member states' payment systems (Minimum Common Features for Domestic Payment Systems), which must be met by the start of 1999. Securities settlement systems (SSS) in the EU countries that are to settle securities transactions associated with ESCB monetary policy operations must meet standards set by the EMI (Standards for the Use of EU Securities Settlement Systems in ESCB Credit Operations). The ECB will be responsible for broad oversight of the EBA Clearing System, and will coordinate oversight activities of the national central banks in the euro area. ECB/ESBC oversight of the payment system will constitute a new feature that will increase the effectiveness of cooperation between central banks and supervisors, increase the security of payment systems, and reduce the danger of systemic risk in Europe.

3 Regulation and supervision of payment systems

3.1 The challenges and objectives of supervision

Payment systems are an integral part of the infrastructure of the economy and especially of the financial sector. In a modern society, payment systems are highly integrated into various structures of the society, which means that a seemingly isolated disturbance or problem in such a system can spread widely across the society. The significant role of payment systems and the potential risks are well demonstrated by the fact that the annual total value of payment transfers in Europe exceeds 20 times the banks' aggregate balance sheet total and that the ratio has been increasing continuously. In order to ensure the functionality of the society, it has been considered that the prime objective of payment systems supervision is to promote systems stability and security by preventing the realization of broad systemic risk and preventing individual banks from encountering liquidity problems due to payment transfer problems. Moreover, with a stable payment system, individual customers can rely on the continuous availability of payment system services and can adopt new and more efficient payment methods.

Besides reducing or eliminating systemic risk, payment systems supervision is essential for the following reasons:

a) Externalities
   - Banks and the society have different objectives (maximizing profit or advantages vs improving security and smooth operation).
   - Owners and management can gain the full benefits of success, but have only limited liability for losses. The responsibility of banks' owners is limited to shareholding and the responsibility of the management to dismissal. Problems stemming from a failure or severe disturbance spread widely across the society.

b) Asymmetric information
   - Information that customers obtain on the banks is insufficient for deciding which bank is most reliable for effecting a payment order.

c) Prevention of misuse and crime
   - Prevention and uncovering of money laundering, embezzlements, computer crimes etc.

Besides the main objective of supervision – ensuring the stability and security of payment systems – maximum effectiveness of the systems is also important. In order to maintain competition, the eligibility criteria for system participation must be the same for all parties. In Finland competition is supervised by the FSA and the Office for Free Competition. Consumer protection and cooperation with the Consumer Ombudsman are closely linked to supervision of payments services offered to private customers. Cooperation between authorities is essential in payment systems supervision in order the ensure that all viewpoints are taken into consideration.

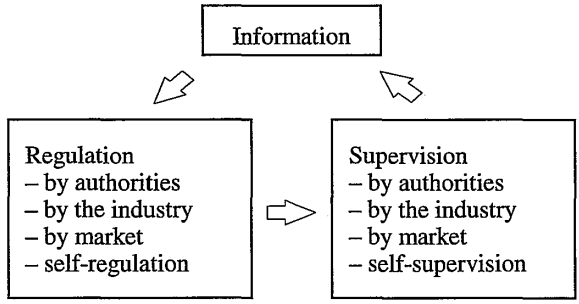
3.2 The link between regulation and supervision

Requirements for payment systems are set out in regulations, from which the regulatory body constructs a set of norms that it will expect a good or acceptable payment system to fulfil. The main problem in regulation is defining what is a good or acceptable payment system and updating the definition in a changing environment.

The objective of supervision is to ensure observance of the norms and criteria that derive from regulations. The major problems connected with supervision concern risk measurement; organization and scope of supervision; and sufficiently early detection of problems.

The availability of information is essential to both these tasks. The prerequisite for regulation is information on future procedures, risks and operating environments. Supervision requires information on the operations and risks involved in current systems.

Figure 1. **Link between regulation and supervision**



There is a fundamental link between regulation and supervision (figure 1). Regulation requires supervision and vice versa. Without effective supervision based on sufficient authority, regulation remains toothless. Without regulation, ie norms, supervision will lack goals for supervision and inspection.

Authorities have traditionally issued regulations, ie set norms, but this can also be done by the industry itself through cooperative organs (eg the Finnish Bankers' Association); by markets (eg stock exchanges); or by the supervised entities (banks) themselves. Devolution of regulation to the level of the industry, market or supervised entity requires the establishment of a general framework for delegated regulation. On the basis of such a framework, industry organizations can perform certain tasks associated with regulation or require self-regulation on the part of the banks. In this case, the authorities would merely oversee the self-regulation function and correct irregularities.

Payment system regulation is generally carried out by authorities. In Finland the related legislation is drafted by the justice and finance ministries. The competition and consumer protection authorities also issue guidelines and regulations based on their own perspectives. The Bank of Finland and the FSA are jointly responsible for supervision of financial markets and thus can issue guidelines and recommendations connected with payment systems; the FSA can also issue regulations. At the international level, there are a number of bodies closely linked with authorities that establish norms for payment systems, eg EMI, BIS, G-10 and the EU Commission.

Supervision, ie the enforcement of norms, can be carried out by the authorities, the industry, the markets or the supervised entities themselves. Devolution of supervision to these levels requires the

establishment of a general framework for delegated supervision. It falls to the authorities to ensure eg that banks' internal monitoring is appropriately organized and operating as intended.

Regulation and supervision of the industry as well as self-regulation and self-monitoring are viable alternatives to regulation and supervision by authorities. Since the banks and other providers of payment services are closest to the risks, they are also generally best able to assess them. On this basis, it is recommendable that the direct role of authorities in regulation and supervision be as limited as the stability goals will allow and that other parties have a larger practical role in regulation and supervision than at present. Direct regulation and supervision by authorities is needed mainly in situations where there is insufficient incentive for self-regulation and self-supervision or where other parties have insufficient information to carry on these activities. The authorities can to a certain extent contribute to the emergence of an environment conducive to self-regulation.

To improve operational efficiency, it is worthwhile for the authorities to establish a regulatory framework in which not only authorities but also other parties have incentives and interests in respect of regulation and supervision.

Authorities can expand self-regulation and self-supervision using eg the following means:

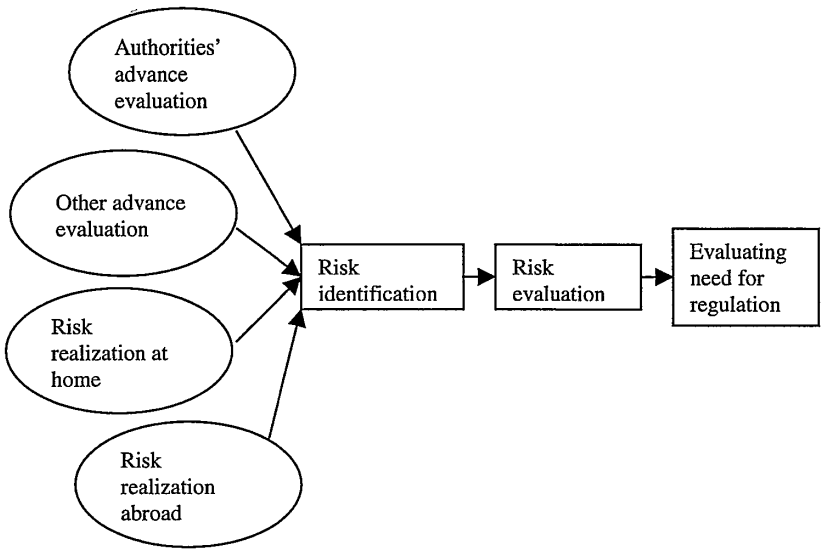
- extending the parties' responsibilities
- developing standards and norms that promote stability (eg safety norms)
- increasing the possibility of sanctions in self-supervision
- expanding public information activities.

3.3 The need for change in regulation and supervision

Changes in the operating environment have a continuous effect on the need to develop banking sector practices. Payment systems in particular change dramatically and rapidly. Changes affect banks' risks and total exposures. Regulation and supervision of payment systems in a changing environment need to be continuously developed in order to keep them up to date as the risks change.

Regulation (and hence supervision) usually develops according to the following process.

Figure 2. **Regulatory process**



The basic requirement for regulation is that a risk be identified and its size estimated. Then the need for regulation should be evaluated (figure 2). Some risks can be identified in advance by authorities and other entities such as banks. As the environment changes, the risks of new technologies can often be estimated on the basis of the risks of established technologies. However, new technologies may also involve surprising, unforeseeable risks. Such risks are identifiable only after they have been realized or problems arise. Both domestic and foreign experiences in risk realization may be useful in identifying risks.

Continuous operational supervision and risk realization produce information on new risks and needs for regulation and supervision – after the event. However, in an environment marked by significant change, regulation should be anticipatory, precisely targeted, and capable of reacting swiftly to new phenomena. To achieve this, emphasis must be placed on anticipation of risks and collection of data on realized payment system risks. The data should be stored eg in a risk database. Knowledge of risks encountered by other parties enables avoidance.

Anticipatory regulation and supervision require that authorities closely monitor payment systems development and invest in new technologies and analytical methodologies, at least to the extent of enabling relatively quick assessment of the need for change in official regulations.

3.4 The optimal amount of regulation and supervision

The overall objective of regulation and supervision is to reduce risk to an acceptable level. Banking and payment transfer activities are characterized by conscious risk taking in an effort to obtain a targeted level of return. Total elimination of risk is not a reasonable goal. Risk taking within set limits and the bearing of risk realizations are an essential part of the banking business. Thus one must accept the fact that also in respect of payment systems some of the risks involved may be realized despite regulation and supervision.

Theoretically, the optimal amount of regulation and supervision is attained when the marginal cost of increasing regulation-supervision equals the marginal benefit from the increase (figure 3). This can also be seen by examining the total costs, ie the theoretical objective is to minimize the total costs of regulation, supervision and realized risks. The biggest problem in defining the optimal situation is the choice of the period of examination and quantification of future risks. The objective of regulation-supervision is to influence the decisions and solutions of supervised entities, the risk-effects of which will not be seen for several years. Realized risks also have indirect effects that are difficult to assess.

It is difficult to apply this theoretical framework to practical implementation of supervision. In defining the scope of supervision, it is usually necessary to define the goal as attainment of an acceptable level of risk based on empirical experience and estimates of future developments. Delineation of the scope of regulation can be aided by the description and evaluation of risks. Self-regulation and self-supervision can be promoted by defining common targets for regulation and recognizing common needs for supervision.

When regulation and supervision of payment systems are based on empirical experience, one can expect to see a fluctuating pattern of regulation and supervision around the optimal level over time (figure 4). Reactions to changes often come too late. On the other hand, a crisis can easily lead to overreaction and hence to an excessive tightening of regulation and supervision.

Figure 3. **Optimal amount of regulation and supervision**

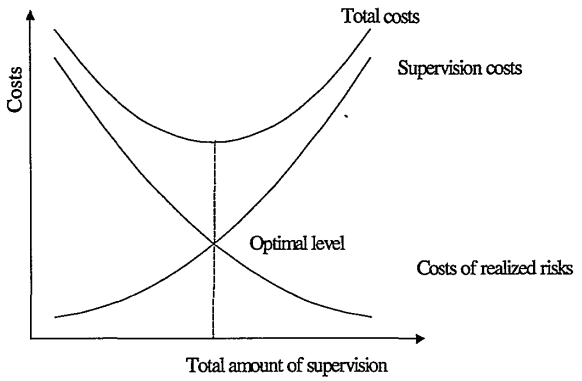
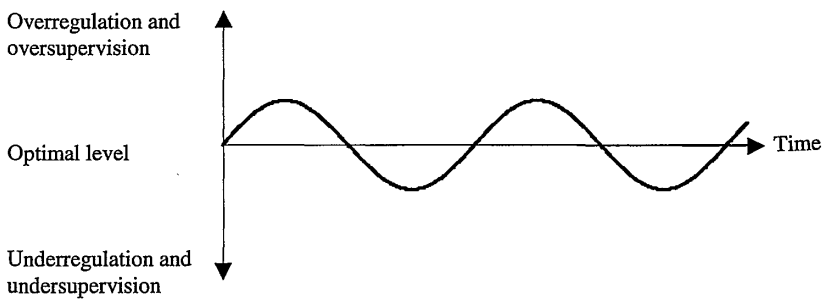


Figure 4. **Variation of regulation and supervision over time**



The need for regulation and supervision can be underlined via the appropriate incentives. By reducing information asymmetries, ie by disseminating more information, one can increase the understanding of the need for regulation and supervision. However, there is a danger that increased information will lead to a massive amount of reporting, unless the reporting is focused on the main risk factors or automated to cite anomalous behaviour. The supervised entities can be encouraged toward tighter internal control by increasing the banks' responsibility, especially the personal responsibility of management,

for self-regulation and self-supervision. In practice, this means enforcing sanctions for information concealment or bypassing or failing to execute accepted controls. This kind of incentive, based on increased responsibilities, is eg part of the New Zealand model. It is easily implemented by establishing clear rules for supervision and sanctions for infractions. It is difficult to create positive incentives because the externalities do not show up directly in banks' financial results.

In the practical implementation of regulation and supervision, it is necessary to rely on overall assessment of the balance between cost and benefit. The direct costs of supervision can be influenced significantly by paying attention to supervisory methods and the division of duties among those involved. In order to increase cost-effectiveness, it is worthwhile for the authorities to transfer as much as possible of the practical work of implementation to other parties. However, this requires that the parties have the incentives for genuine supervision and that the broad stability objectives of oversight be attained.

Costs of supervision by the authorities should be made known, eg by covering them by direct charges, so that supervised entities can evaluate the related benefits and costs. In Finland the FSA levies supervision fees on supervised entities. The costs of the Bank of Finland's broad oversight operations are covered indirectly by the Bank's income.

3.5 The legislative basis for supervision

The current Act on the Bank of Finland, which entered into force at the start of 1998, states in section 2 that 'the Bank of Finland shall ... promote the stability of the financial system' and in section 3, paragraph 2 that it shall also 'participate in maintaining the reliability and efficiency of the payment system and overall financial system and participate in their development'.

Under section 6 of the Currency Act and section 3 of the Regulations for the Bank of Finland, the Bank has a statutory monopoly on the issuance of banknotes and legal tender (Currency Act, section 2).

The activities of the FSA are based on the Act on the Financial Supervision Authority (No. 503/1993), which defines the norms that form the foundation for actual supervision. The FSA supervises banks and other participants in the financial and capital markets with the aim of ensuring that these entities operate in accord with legislation; their own Articles of Association and bylaws; and good banking and market practices.

The role of the European Central Bank in the regulation and supervision of payment systems is based on the Maastricht Treaty and the ECB Rules, as mentioned in chapter 2 above.

4 Payment system risks

Payment system risks can arise in customer payment systems or in interbank payment systems, developed for the banks' own payments, where the banks execute primarily their own payment orders.

A payment system can itself generate risks eg through poor risk management or inadequate organization. It may also transmit risks originating on the outside from one bank or country to another, if an important system participant has liquidity problems that spread to other participants. In such a case, the payment system may act as a conduit for systemic risk at the national or even international level if disturbances or losses spread in a chain reaction through different systems thus causing a domino effect.

Payment system risks are characterized by their short duration and continuous recurrence compared eg to banks' credit risk associated with credit granting. Once a payment has been irrevocably transferred to the possession of the proper receiver, the payment transfer risk is extinguished. On the other hand, since payment orders are issued continuously day after day, there are always payments-related risk positions.

4.1 The challenges of risk definition and assessment

Risk definition and assessment entails three challenging tasks:

- to draw up a clear risk classification scheme
- to estimate the probabilities of risk realization
- to quantify the consequences beforehand.

Since payment system risks can be classified from various perspectives, it is difficult to avoid overlapping and borderline cases. The most demanding job is to specifically classify individual events as payment system risks. Most risks change over time and their effects shift from one area to another. An agreement on nonverification of covering funds is a good example of the difficulty of classification. On the basis of such an agreement, the customer can make payments from his account without verification of covering funds up to the

amount that is credited to that account during the same day. With respect to the possibility of an enterprise going bankrupt and a bank being left liable for an intraday overdraft, it is a question of whether the risk is a payment transfer risk or a credit risk (ie extended overdraft facility). The assessment is thus affected by the perspective. In section 4.2, we introduce the classification scheme used in this report. The emphasis is placed on the scheme's usefulness as a tool for analysis and supervision.

It is relatively simple to estimate the probability of risk realization for frequently occurring events (eg counterfeit payment instruments) on which there are sufficient statistical data. There is a danger, however, that unusual changes will go unnoticed (eg a massive counterfeiting wave). Unfortunately it is very difficult to estimate the probability of realization of risks for infrequent events, eg a wide-spread gas explosion in the vicinity of a computer centre, an earthquake, a nuclear catastrophe, bankruptcy of a large bank etc.

Measuring the consequences of risk always entails the danger of over- or under-estimation. They may be overestimated because one cannot foresee the possibilities of substituting for the interrupted activity. In a real emergency situation the society and concerned parties will adapt to the situation and seek alternative payment systems. For instance, when cash loses its credibility with the public in a difficult and exceptional situation, alternative payment means are often utilized, such as gold or other commodities or work exchanges. Consequences may be underestimated when all possible connections and consequences of risks are not seen, eg in an integrated system.

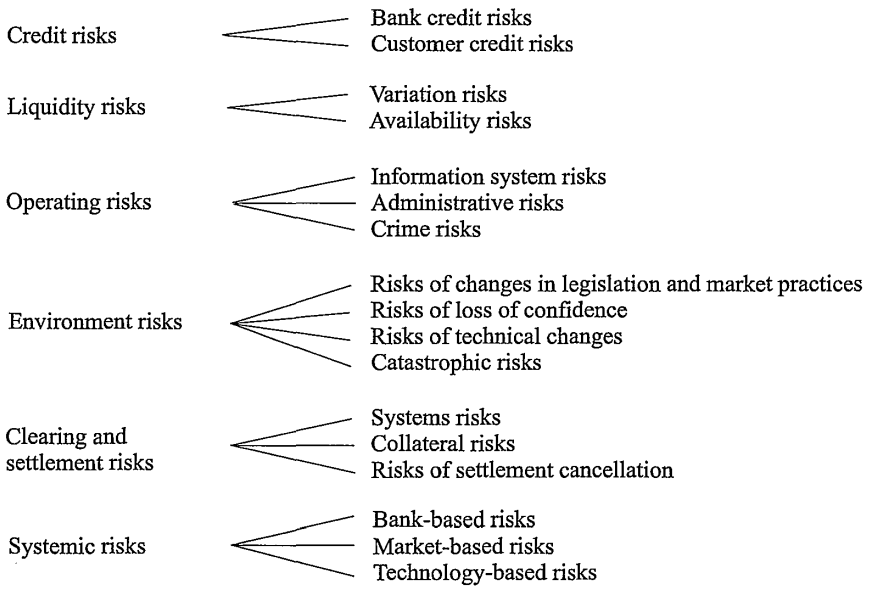
Measuring the magnitude of risks requires the resolution of these problems. If this can be achieved, as has been done in respect of payment card misuse, it makes sense to take risk-reducing measures for which savings exceed costs. In difficult-to-measure cases, decisions are based on subjective views of corporate management and authorities, which generally reflect decisionmakers' attitudes toward risk avoidance or risk management policy. Even though risk measurement always entails inaccuracy, outlining and analysing risks helps one to understand the nature of risks and to find means to reduce them.

4.2 Risk classification

Payment system risks can be classified in several different ways. It is difficult to develop a clear and hierarchically comprehensive structure for risk classification because the different types of risk are interconnected. For instance, a situation starting out as an IT-operations problem may lead to liquidity problems if the disturbance is prolonged. Risk realization generally leads to loan losses or liquidity problems and may ultimately lead to the realization of a systemic risk that threatens the whole payment system.

In order to classify payment system risks in a manner that is useful for supervision, this report starts the process with the basic risk categories and subcategories as presented in figure 5.

Figure 5. **Classification of payment system risks**



In scientific publications the classification of risks is usually less extensive. Here, we have aimed at detailed classification, taking into account different concrete risk types and different methods of protection. This classification can be expanded or contracted as needed. In the following, each risk category is explained in detail.

Credit risks

Credit risk refers to the risk of loss that arises when a bank transfers a payment to the final receiver before receiving covering funds.

A bank credit risk arises between two banks when the receiver's bank assumes irrevocable responsibility for the payment even though the subsequent transfer of covering funds, which is the responsibility of the sender's bank, is subject eg to the risk of bankruptcy of the latter bank. Bank credit risks are characteristic of interbank payments, where payment transfers result in open credit positions between banks.

A customer credit risk falls on the sender's bank when it transfers a payment despite a lack of covering funds in the sender's account. Competitive conditions often induce banks to assume customer credit risks, especially as regards large corporate customers.

Liquidity risks

Liquidity risk refers to risk of loss that arises when a bank's liquid assets or immediate access to credit are insufficient to cover its payment obligations.

Variation risk is due to wide variations in a bank's liquidity, which means that at times it is unable to foreword payments it has undertaken and must temporarily postpone the transaction.

Availability risk arises when a bank's impaired financial condition reduces the amount of liquidity that it can obtain from the market to the point where it has difficulty in making payments for which it is irrevocably committed. Poor liquidity may lead to repeated payment delays, compensation claims and, if prolonged, to loss of customers to rivals.

Operating risks

Operating risk refers to the risk of loss that arises when costly errors occur in payment transfer information systems, administration or organization or when these systems are misused or accessed by outsiders without authorization.

Information system risks are connected with IT systems and their manual support operations as well as to manual payment transfer processes. In the present stage of development, payment transfers are largely information transfers, as the volume of physical cash

payments and cash deliveries is continuously declining. The heavy dependence on IT systems also emphasizes these risks.

Administrative risks are generally connected with a bank's operating methods, division of responsibilities, functionality of internal risk management processes, employees' expertise, backup systems, problem-handing readiness etc. Increasingly more complex and continuously changing systems require far more expertise than before. Increased mobility of key employees and diminished numbers of backup people create risks of lack of expertise in managing special situations.

Crime risks change along with the development of the system. Criminals learn over time to exploit payment system weaknesses. As regards number of crimes, most realized risks relate to relatively small-value losses. Organized crime is growing, which may mean larger losses to banks. Increasing electronification means that criminals often need insider assistance from the bank's present or previous employees to bypass the systems' security features.

Environment risks

Environment risk refers to possible losses caused by rapidly changing operating environments. The ever-accelerating pace of change in society increases environment risk. The main environment risks are those caused by changes in legislation and market practices, risks connected with loss of confidence or technological changes and risks caused by catastrophes.

Changes in legislation and rules of the game have increased and may give rise to the emergence of new and unforeseen risks. Legislation varies from country to country and is constantly changing and becoming more subject to interpretation. New issues in consumer protection, product safety and liability may lead to unforeseen liabilities and damages and therefore to unexpected costs.

Risks connected with swings in confidence can in extreme cases cause customers to avoid a certain type of service or bank group. Loss of confidence may arise from an isolated and limited case that becomes highly contagious. Customer confidence is essential in making payments and using payment instruments (cf genuineness of banknotes).

Risks connected with technological changes have increased due to the ever-increasing pace of change. This may result in the rapid disappearance of certain types of services due to poor competitiveness. Dependence on technology can also lead to expensive and

unforeseen service maintenance needs. Technical protection of IT systems in many banks is based on passwords, encryption, control of user rights etc. The danger of hacking, ie unauthorized entry into information systems, is increasing. These criminals use more sophisticated tools and have more processing capacity at their disposal, which means that banks must continuously improve their systems. Increasing electronification also increases problems in identifying the genuineness of transactions, because a copied electronic transaction is absolutely identical to the original.

Certain catastrophic risks, connected eg with natural forces or societal changes, are rarely realized. The deep integration and centralization of payment systems, along with their dependence on high technology, mean increased vulnerability to large catastrophes.

Clearing and settlement risks

Clearing and settlement risk refers to possible losses arising in connection with clearing and fund transfers between banks. These risks are characteristic of interbank payment transfers.

Clearing and settlement systems risks are associated with IT and information transfer systems used by banks and central banks for clearing and fund transfers, and to their credibility, reliability and backup systems.

Clearing and settlement collateral risks are connected with the safety, adequacy and custodial care of collateral for clearing and fund transfers.

Settlement cancellation risks concern the certainty of the irrevocability and finality of clearing and fund transfers. These are based on the underlying domestic and foreign legislation, interbank agreements and possible special arrangements for disturbances. The main problems are the legal validity of netting in netting-based fund transfer systems and the timing of fund transfer finality as well as the applicable national legislation in the case of parties from different countries.

Systemic risk

Traditionally, systemic risk has been associated with a disturbance in the money market that begins with a bank run and spreads from bank to bank and may expand into a systemic crisis that threatens the operation of the whole financial system.

In the context of payment systems, systemic risk refers to risk of loss that arises when the whole payment system or a substantial part of it ceases to function and the operational capacity of the society's payment services is significantly weakened. As it spreads, this disturbance may expand to an overall systemic risk, which can jeopardize the operation of the whole financial system and the real economy.

Systemic risk may be caused by the failure of a critical part of a payment system, such as its information system, by insolvency of a significant participant bank or by a crash in a market in which settlement takes place. According to these criteria, systemic risks can be categorized by their origins as technology-, bank- or market-based risks. The increased volume and integration of systems, the centralization of payment transactions and international linkages have increased the danger of systemic risk. Systemic risk is also associated with the fact that one or more of the above basic risks can be realized on such a scale or spread so widely as to jeopardize the operation the whole system.

4.3 Classification of payment systems

Payment systems may be classified into different groups according to numerous criteria, such as method of use, transaction size, transfer speed etc. From the standpoint of supervision, an appropriate classification criterion is the size of the risk associated with different kinds of payment systems.

In the following, payment systems are categorized on the basis of the payment media used, so that risk profiles within each category will be as uniform as possible:

- cash payment instruments (cash and e-money without audit-trail and account keeping)
- debit payment instruments (debit cards, cheques, e-money)
- small-value credit transfers (ordinary credit transfers, express transfers, recurring payments, direct debiting with authorization verification)
- large-value cheques and bank drafts
- large-value credit transfers
- documentary payments (collections and documentary credit).

This report does not examine risks connected with cash payment instruments and documentary payments, even though they are included in the above classification scheme. Risks connected with use of cash are extensively covered in other publications, and the use of documentary payments is relatively small, and the specific issues concerning these are connected with document processing and identification as well as credit risks. E-money without account keeping is also left out, because it is being examined by other bodies (working groups of the EMI and Finland's Ministry of Finance).

The borderline between small- and large-value payments is in practice a shifting and often undefined one. There is no clearly defined markka value for a large-value cheque or credit transfer. The minimum in the case of a cheque used to be the FIM 1 000 guarantee limit, but this is no longer applied. The ceiling for a debit card transaction has been set at FIM 200 000. In banks' internal security instructions, a large-value transaction usually refers to one exceeding FIM 50 000–100 000. The directive on cross-border credit transfers sets the limit for retail payments at ECU 50 000. Special credit risks are associated with payments exceeding FIM 10 million – FIM 100 million.

Cooperation in the supervision of payment systems has focused on traditional payment systems. Risks connected with domestic vs foreign payment systems are examined here separately only if international systems (eg SWIFT) involve special risks. This study is limited to deposit banks; companies issuing payment cards, finance companies etc are excluded.

Payment system risks are described in detail in appendix 1 in accord with the above classification scheme for payment systems and payment system risks.

4.4 Payment system-specific risks and their overall evaluation

Risk classification scheme

A basic risk classification scheme for payment systems (table 1) can be set up by cross-tabulating basic payment system risks and payment systems as presented in figure 5 on page 35. Each row contains an individual risk type, ie credit risks, liquidity risks, operating risks,

environment risks, clearing and settlement risks and systemic risk; each column contains a payment system whose risk profile is as uniform as possible, ie debit payment instruments, small-value credit transfers, large-value cheques and large-value credit transfers.

This risk classification scheme and modifications thereof can serve as a supervisory tool in estimating probabilities and sizes of realizations of these risks in respect of a single bank, the whole banking sector, or different payment systems. Banks can also use the scheme in estimating risks inherent in their own payment systems. Based on its own experiences, a bank could enter into the table the frequency of each type of risk realization (eg once a year, once in 5 or 20 years) and the losses incurred. This would give a good picture of realized payment system risks. A bank could also estimate the maximum loss for each risk to obtain an estimate of its maximum total losses in connection with payment systems. The most difficult, but also most useful, estimation would be of the probable payment systems-related losses that the bank would incur over the next few years and eg the next 5–10 years.

To illustrate the use of the risk classification scheme, letter symbols are used to indicate the estimated significance of each risk by payment subsystem, its size by bank and also the size of the systemic risk associated with a disturbance.

System-specific risk relates to a sudden paralysis of a specific subsystem (eg use of payment cards) that has a significant effect on the stability and reliability of the subsystem.

The following letter symbols are used to indicate the significance of a system-specific risk:

jjj = the probability of risk realization is very low, but realization implies huge losses and will likely cause a subsystem crisis,

jj = the probability of risk realization is low but realization implies large losses and may cause a subsystem crisis,

j = the probability of risk realization is relatively low, but realization implies relatively large losses but is unlikely to cause a subsystem crisis.

The following letter symbols are used to indicate the significance of the bank-specific risk:

ppp = the probability of risk realization is very low, but realization implies huge losses and will likely cause a bank-specific crisis,

pp = the probability of risk realization is low, but realization implies large losses and may cause a bank-specific crisis,

p = the probability of risk realization is relatively low, but realization implies relatively large losses but is unlikely to cause a bank-specific crisis.

Correspondingly, the following letter symbols are used to indicate the significance of systemic risk:

sss = the probability of risk realization is very low, but realization implies huge losses and is likely to cause a serious systemic crisis,

ss = the probability of risk realization is low, but realization implies large losses and may cause a systemic crisis,

s = the probability of risk realization is relatively low, but realization implies relatively large loses but is unlikely to cause a systemic crisis.

Figure 6. **Probability of loss in payment transfers**

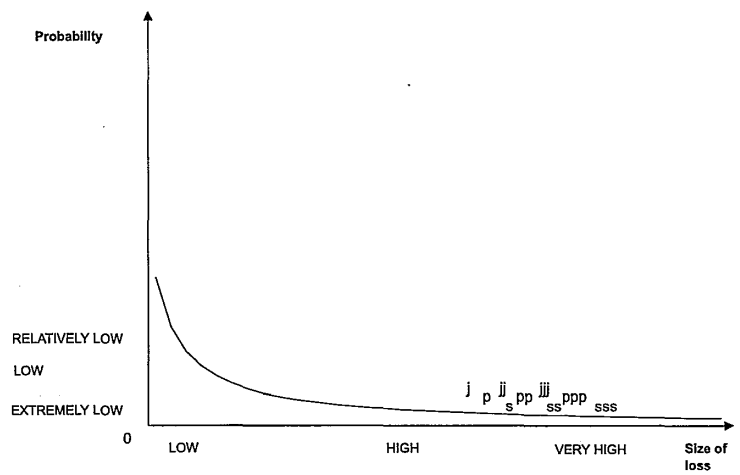


Figure 6 is a graph depicting the relationship between the probability of realization of a system-specific risk and size of the potential loss. It is characteristic of payment systems that losses occur infrequently (with low probability) but are huge in magnitude. Reliable operation of a payment system requires elimination of small and frequently realized risks. Therefore, the real problem concerns large-but-infrequently-realized risks. These often relate to fortuitous events that may occasionally affect a payment system, such as a fire, a sudden bankruptcy, a big accident etc.

The above risk estimates are intended as a discussion opener on the nature and size of payment system risks and are not intended for drawing detailed conclusions about the size of risks associated with current payment systems. An exhaustive examination of risks would require that these be examined on a system-specific and bank-specific basis and assessed in much greater detail than is attempted in this report.

Table 1. **Risk classification scheme for payment systems**

Payment system/risk type	Debit payment instruments	Small-value credit transfers	Large-value cheques	Large-value credit transfers
Credit risks				
Bank credit risk		p, s	pp, s	ppp, sss
Customer credit risk		p, s	pp, s	p, s
Liquidity risks		p, s	pp, s	ppp, ss
Operating risks				
Information system risks	j	j, p, s	p	pp, s
Administrative risks	j	p, s	p	pp, s
Crime risks	j	j, p	p	pp, s
Environment risks				
Risks of changes in legislation and market practices		p, s	p	pp, ss
Risks of loss of confidence	j	j, p, s	j, p	pp, ss
Risks of technical changes	j	j		jj, pp, ss
Catastrophic risks	j	j, p, s	j, p, s	pp, ss
Clearing and settlement risks				
Systems risks		pp, s	p, s	ppp, sss
Collateral risks		pp, s	p, s	ppp, sss
Settlement cancellation risks		pp, s	p, s	ppp, sss
Systemic risk	–	p, s	pp, s	ppp, ss

General assessment of risks

Risks connected with debit payment instruments are usually relatively small in value. Crime-related information system and administrative risks have been the most visible of these. No systems risks have appeared that would prevent the use of a certain debit payment instrument. An extensive wave of counterfeiting could cause a loss of public confidence in a specific debit payment instrument, but debit payment instruments do not entail systemic risk.

The risks associated with a single small-value credit transfer are small, but if bank credit risks cumulate over a large number of transactions, they may pose a real danger. In addition to the highly visible crime-related information system and administrative risks, there are risks that are realized only rarely, such as environment and clearing and settlement risks, which are connected with advance crediting of netted transactions to customers' accounts and the legal validity of netting in case of a disturbance. It is extremely rare that risks connected with small-value credit transfers expand to become systems risks or overall systemic risk.

Large-value cheques entail bank credit risk especially when the covering funds for a cheque are not verified and interbank risk positions are not controlled by limits or collateral. The most visible risks associated with large-value cheques have been crime-related and administrative risks. Other associated risks include clearing and settlement risks connected with advance crediting of netted transactions and the legal validity of netting. Large-value cheques are rarely associated with systemic risk in a disturbance situation.

Large-value credit transfers entail significant bank credit risks in disturbance situations when interbank risk positions are not controlled by limits or collateral. Despite backup arrangements, there are operating risks due eg to a high degree of automation. Other significant risks include environment risks and especially clearing and settlement risks. Systemic risk may also arise in the event of a disturbance.

Problems associated with the measuring and monitoring of risks

The basic problem in measuring payment system risks is the lack of systematically collected data for use in calculating probabilities of risk realization on the basis of past history. Moreover, some of the risks relate to events that occur so rarely that there are few (possibly zero) recorded observations.

One of the specific problems connected with the monitoring of payment system risks is that for most of the important risks the probability of realization is very low but the potential losses to banks or even to the society are huge. These risks are analogous to those associated with nuclear power stations and natural catastrophes. The most dangerous payment system risk is systemic risk, but other risks, especially those connected with large-value payment systems, may entail considerable potential losses.

Another special characteristic of payment systems, particularly in Finland, is the high degree of automation (over 70 per cent) and the new IT and communications technology involved. Misuse of IT and communications links may enable the swift diversion of large amounts of funds into criminal hands. Ensuring adequate security in payment systems that involve new means of transfer (eg Internet) and new means of payment (eg e-money) presents new types challenges to supervisory bodies and monitoring methods.

4.5 Means of reducing payment system risks

Effective control, reduction or elimination of payment system risks requires a variety of means of payment transfer, procedural rules, risk limits, instructions and recommendations. In the following, we examine the possibilities for reducing payment systems risks by main risk category. Banks that participate in payment systems can use these means at their own initiative, financial sector interest groups can recommend them to the members, or supervisory authorities can require compliance. Means of reducing risks are presented in detail in appendix 2.

Means of controlling credit risks

Bank credit risk can be eliminated by transferring covering funds for payments between banks before final crediting of customer accounts or via gross settlement (RTGS). The means of limiting the risk are bank-specific counterparty credit limits, collateral, legally irrevocable netting, and payment finality rules. In the extreme, risk control requires a real time monitoring system.

Customer credit risk can be reduced by analysing and classifying customer risks, setting limits and collateral requirements on a transaction/customer basis, assigning a responsible person for each customer and (preferably) real time monitoring of limits.

Means of controlling liquidity risks

Liquidity risks can be reduced by netting, well-planed timing of payments, and flexible use of limits and collateral. In order to plan for their intraday liquidity needs, banks need adequate forecasting systems and forecasted liquidity positions must cover payment obligations.

Means of controlling operating risks

Information system risks can be reduced by coordinating decisions concerning information systems, applying common standards, and systematically planning and maintaining the system so as to reduce errors and malfunctions. A solid information system architecture, skilled personnel, continuous training and written instructions will decrease the possibility of errors connected with complex systems and changes therein. Information system risks can also be reduced by effective internal monitoring, a fixed format for controlling change, security-enhancing systems, and effective backup systems.

The means of reducing administrative risks include observation of good payment transfer practices; clear division of duties and responsibilities also at the management level; effective use of internal modes of control and risk management; hiring and training a sufficient number of expert personnel and continuously updating their skills; conscientious maintenance and organized use of systems; sufficient backup personnel and systems; preparation of instructions for handling problems and disturbances; and seeing that agreements are in place to handle compensation claims due to errors and delays.

Crime risks can be reduced by preparing written security policies and procedural instructions concerning crime; integrating security planning into systems planning; sufficient controls; separating tasks that may entail danger if performed together; sufficient physical security and control of access to information systems; observance of safe practices; training personnel to recognize crime risks; and sharing experiences with other bodies on criminal methods and means of protection.

Means of controlling environment risks

Risks caused by changes in legislation and rules of the game are difficult to avoid, but they can be prepared for in advance. As regards the former, information can be obtained from various sources (domestic and foreign) on applicable legislation and planned amend-

ments, and active lobbying of legislators and authorities may also be a possibility. Similar methods can be used in respect of risks associated with changes in the rules of the game, although it may be possible to have a more direct influence on authorities via discussions, statements of opinion etc.

Risks connected with confidence loss can be avoided by regular advance information, well-organized management of information and crises; and rapid dissemination of accurate information whenever problems occur. Anticipating situations that could undermine confidence sometimes enables prevention.

Risks associated with technological change can be identified by monitoring developmental trends in the field. Since the major risks in this category relate to the possibility of breaking through existing security barriers, it is prudent to invest beforehand in new security systems and to employ parallel means of protection. Safeguarding the ability to adapt requires that systems have sufficient room for expansion.

Catastrophic risks can be reduced or alleviated by advance planning and building up and testing recovery capabilities. Various security arrangements and equipment, such as access control and fire extinguishing equipment, reduce the probability of a catastrophe. Decentralization of systems reduces vulnerability and enables partial operation during disturbances. Written instructions concerning the limiting of services or changeover to manual services will make it easier to manage crises.

Means of controlling clearing and settlement risks

The means of reducing clearing and settlement risks include effective and operational backup systems, adequate collateral arrangements and legislation guaranteeing the security of pledged collateral and settlement finality.

Means of controlling systemic risk

One method of controlling systemic risk is to create payment system structures and procedures that reduce the likelihood of both systemic risk realization and bank-to-bank or system-to-system contagion (eg RTGS, DVP and PVP). Another control method is for central banks or clearinghouses to put in place facilities for providing liquidity to market participants in case of a market crash or payments settlement in case of a technical malfunction. Operational backup systems are also important in preventing disturbances and contagion.

4.6 Current payment system regulation and supervision

Current regulation and supervision

In Finland payment systems regulation, supervision and procedures are based on legislation concerning credit institutions, the Bank of Finland and the FSA; cooperation between banks under the auspices of the Finnish Bankers' Association; and agreements between the central bank and the banks involved in the clearing and settlement system and between the banks. At present, there is no specific legislation on payment systems, and their use is largely governed by voluntary agreements and self-regulation. The netting of foreign exchange, securities and derivatives transactions became legally valid even in the event of bankruptcy under a law that entered into force on 1 July 1997. Legislation is currently being drafted on the foreign credit transfers and settlement finality.

The FSA influences payment systems via inspections; supervision based on continuous reporting; and guidelines and regulations. The Bank of Finland influences payment systems via international cooperation (EMI, ECB, BIS); issuance of recommendations; development of systems in cooperation with Finnish banks; and encouraging and supporting banks' own initiatives and projects. The central bank also has an impact on the terms of access and agreements pertaining to payment systems. The central bank decides which institutions gain access to its current account facility (BoF-RTGS) and the banks, through the Finnish Bankers' Association, decide on participants in their jointly maintained payment systems: the Finnish interbank payment system (PMJ), the clearing system for large-value express transfers and cheques (POPS) and the clearing system for cross-border Finnish markka payments (loro).

In connection with its operating activities, the central bank oversees the BoF-RTGS system and the participants via the rules that it sets and carries the responsibility for the stability of the system. The central bank's Internal Audit Department supervises the system, focusing especially on changes and special situations. The Bank of Finland's external auditors can also examine the Bank's payment systems. This approach will probably be used increasingly in the future, as the importance of RTGS payments increases. The FSA supervises funds transfers of supervised entities and the related payment and settlement systems. In the interests of developing

supervision and joint supervision, the Bank of Finland and the FSA established a joint working group on payment systems supervision cooperation (MAJAVA). A unit dealing with payments and IT systems has been set up within the FSA with the aim of improving the effectiveness of supervision.

International and domestic recommendations and standards

The EU, EMI, BIS, various international standardization bodies and others have issued norms as a means of improving the reliability and security of payment and settlement systems. These norms have been of various types, including minimum standards, directives, general principles, and standards. In Finland the Finnish Bankers' Association has developed security standards for electronic customer interfaces. The most important recommendations and standards are

- EMI minimum standards for member states' payment systems
- general principles for payment system supervision in EU countries (see chapter 2.3)
- principles for data exchange in EU countries' payment systems
- Lamfalussy minimum standards for multilateral netting systems
- EU minimum requirements for foreign retail payments (directive on cross-border credit transfers)
- rules on settlement finality and collateral and (in preparation) securities settlement systems
- EMI eligibility criteria for securities settlement systems
- security requirements for TARGET
- Finnish PATU standard for customer interfaces
- report of the ISO working group (TR) on information security for financial services (ISO/TR 13569 15 Nov 1996 Banking, securities and other financial services – information security guidelines).

Payment system projects and working groups in Finland

Since 1995 the Bank of Finland and the banks operating in Finland have been working together on various projects aimed at developing payment system structures and risk management. This cooperation has been carried out via the Payment Systems Management Group and its subgroup, the Payment Systems Cooperation Group, which acts as a preparatory body. The objective is to ensure that by end-1998 Finnish payment systems comply with international recommendations and EMU criteria. The FSA has not participated in

these projects but has received the groups' written reports, which serve as a basis for supervision.

The banks' payment systems that are being continuously developed include payment transfer settlement (PMJ system), on-line express transfers and cheques (POPS) and loro payments. The Bank of Finland systems involved are its BoF-RTGS system and its linkup with the banks' network. One new payment channel being developed is the linkup of the BoF-RTGS system with the EU-wide TARGET system. Work is also in progress on various agreements and legal issues connected with payments and settlement.

In order to reduce settlement risk in the PMJ system, present plans call for twice-daily clearings: the current afternoon clearing and a new early-morning clearing. In both clearings, receivers' accounts are to be credited only after covering funds have been transferred unless there is proper collateral. Transactions with insufficient cover will be terminated by a termination facility, which is under construction. The new procedure will be introduced in phases during 1998 and 1999.

In order to enhance risk management for the POPS system, the banks have agreed on bilateral gross limits. An individual payment that exceeds the applicable limit is handled on a gross basis in the BoF-RTGS system. Smaller amounts are settled in batches and netted bilaterally; the net limit is twice the gross limit. Net obligations that exceed the gross limit are flagged for coverage by BoF-RTGS transfers. If a net limit is exceeded, the processing of the bank's transactions is interrupted. The gross limits were introduced on 1 June 1997 and the introduction of the net limits is slated for spring 1998.

To reduce settlement risks in loro settlement, it was decided that netting should be discontinued in favour of gross settlement in the BoF-RTGS system using SWIFT messages. Rules for the processing of loro payments will be incorporated in the banks' agreement on settlements. According to plans, the new procedure will be introduced in early autumn 1998.

The BoF-RTGS system has been improved by discontinuing the use of administrative limits on 1 May 1997 and introducing a fully collateralized intraday credit limit. At the same time it was decided to discontinue the uncollateralized overdraft facility following a transition period ending at end-1997. The transition to gross-basis liquidity management will be tested via a simulation model incorporating the new settlement rules and using historical data on payment transfers supplied by banks.

Table 2. **Risk classification scheme for payment system projects aimed at risk reduction**

Payment system / risk type	Small-value credit transfers	Large-value cheques	Large-value credit transfers
Credit risks			
– Bank credit risk	p, s	pp, s	ppp, sss
– POPS limits /limits	limits	limits	limits
– RTGS system	eliminates	eliminates	eliminates
– Settlement before crediting receiver's account	eliminates	eliminates	eliminates
– Use of collateral	reduces	reduces	reduces
– Interruption of transactions	prevents	prevents	prevents
– Additional night-time clearing	reduces		
– Customer credit risk	p, s	pp, s	p, s
– Verification of cover	prevents	prevents	prevents
– Technical limits	limits	limits	limits
Liquidity risks			
– Variation risk	p, s	pp, s	ppp, ss
– Flexible BoF limit	reduces	reduces	reduces
– RTGS system	increases	increases	increases
– Queuing system	evens out	evens out	evens out
– Availability risk	p, s	pp, s	ppp, ss
– Extension of eligible collateral	reduces	reduces	reduces
Operating risks			
Environment risks			
Clearing and settlement risks			
– Systems risks	pp, s	p, s	ppp, sss
– Tested backup systems	reduces	reduces	reduces
– Collateral risks	pp, s	p, s	ppp, sss
– Collateral requirements	reduces	reduces	reduces
– Collateral regulations	eliminates	eliminates	eliminates
– Settlement cancellation risk	pp, s	p, s	ppp, sss
– Finality regulations	eliminates	eliminates	eliminates
– Netting regulations	eliminates	eliminates	eliminates
Overall systemic risk	p, s	pp, s	ppp, ss
– Minimum standards	prevents credit	prevents credit	prevents credit
– Lamfalussy	risk	risk	risk
– Changes in payment method (RTGS, PVP, DVP, CLS)	reduces	reduces	reduces
– Liquidity arrangements (central banks)	prevents contagion	prevents contagion	prevents contagion
– Backup systems	prevents contagion	prevents contagion	prevents contagion

The new risk classification scheme is used in table 2 to show which risks each payment systems project is designed to reduce or eliminate and the means applied for reducing each type of risk. For instance, bank credit risk associated with large-value cheques can be reduced by applying limits (POPS limits) or using collateral; eliminated by gross settlement (RTGS system) or crediting the receiver's account only after transfer of funds.

5 Division of duties in payment system supervision and cooperation between authorities

5.1. Principles behind the division of duties

The division of duties in regulation and supervision between the Bank of Finland, the FSA, various ministries, the Office for Free Competition and the Consumer Ombudsman is based on legislation and the common features for payment systems supervision enunciated by EMI in 1993. According to these, the division of duties is as follows: oversight of payment systems – the central bank (systemic risk); supervision of individual supervised institutions – FSA; legislative changes and authorizations – Ministry of Finance; general legislation – Ministry of Justice; competition matters – Office for Free Competition; and issues related to customer protection – Consumer Ombudsman.

This basic division of duties has been subdivided into areas of operation and the duties have been further broken down into three main groups: regulation; supervision; and information and development. These have also been divided into subgroups (table 3). The Ministry of Finance and Ministry of Justice are primarily responsible for legislative changes and regulation of the industry and the markets. The Bank of Finland and the FSA are jointly responsible inter alia for managing systemic and bank-specific crises as well as the related information requirements and collection.

5.2 Cooperation in supervision

The Bank of Finland, FSA and the ministries have a list of tasks and areas of responsibility, which serves as a general guideline for cooperation in payment system supervision and development of regulation and supervision. Regular cooperation and joint meetings are the fora in which cooperation in supervision, exchange of experience and information, and further development take place. The division of duties must be clearly defined in order to prevent duplication or loopholes in supervisory activities.

Table 3. **Responsible authorities**

Duties	Responsible authorities					
	BoF	FSA	MoF / MoJ	OFC	CO	Jointly resp.
I Regulation						
1. Regulation by authorities						
– Legislative changes			X			
– Overall stability, monetary policy	X					
– Code of conduct		X			X	
– Regulations and instructions		X				
– General recommendations	X					
2. Regulation by the industry			X			
3. Market regulation			X			
– Monetary policy regime	X					
– Customer protection		X				
4. Self-regulation		X	X			(X)
5. Regulation of competition				X		
II Supervision						
1. Supervision by authorities						
– Inspections and supervision of institutions		X				
– Systems supervision	X					
– Systemic crises	X					(X)
– Bank-specific crises		X				(X)
2. Framework for supervision by the industry	X					
3. Framework for market supervision						
– Monitoring of monetary policy	X					
– Supervision of procedures		X			X	
4. Framework for self-supervision		X				
5. Supervision of competition				X		
III Information and development						
1. Information on regulation and supervision						
– Inspections and supervision of institutions		X				
– Overall systems oversight	X					
– Systemic crises	X					(X)
– Bank-specific crises		X				(X)
– Foreign information						
– from central banks	X					
– from supervisory bodies		X				
2. Information about the industry and markets						
– Collection and analysis of data	X					
3. Information on banks						
– Collection of data and analysis		X				
4. Data register		X				(X)
5. Information on competition				X		

BoF = Bank of Finland, FSA = Financial Supervision Authority, MoF = Ministry of Finance, MoJ = Ministry of Justice, OFC = The Office for Free Competition, CO = the Consumer Ombudsman

It should be noted that Finland's largest commercial bank has such significance vis-à-vis the payment systems that it is the object of both oversight (systemic risk) and normal supervision. This is also true of the clearinghouse for the securities market, the Finnish Central Securities Depository. Cooperation between the Bank of Finland and the FSA is crucial in supervising these two institutions.

6 Focal areas of regulation and supervision of payment systems

6.1 Focal areas of the Bank of Finland's payment system oversight

In its overall oversight of payment systems, the Bank of Finland pays particular attention to the stability and functionality of the most essential systems. In the context of the single money market, systems that process large-value payments within the investment and money markets must be particularly reliable and secure. The single monetary policy requires functional payment systems.

The objective is to limit counterparty and administrative risks so as to prevent individual problems from expanding into systemic crises and paralysing the whole system. Interbank settlement systems need to be improved with a view to controlling clearing and settlement risks. The launch of Stage three of EMU will considerably increase the flow of foreign funds transfers and the associated risks. The management of international risks in Finnish systems is in need of improvement. Risk management in Finnish payment systems must also fulfil the EU's minimum standards, eg the Lamfalussy standards for netting systems.

6.2 Focal areas in the Financial Supervision Authority's payment system supervision

In order to make efficient use of scarce resources, the FSA focuses its supervisory efforts in accord with estimated risks for each payment and settlement system and hence on the key participating banks. Supervisory activities focus on systems serving wholesale markets as well as those serving retail markets that are important as regards systemic risk, including the related IT and internal audit systems. Supervision of retail market systems mainly deals with the provision of services to customers but not with the supporting role of such services in supervised entities' other business activities.

In its payment systems supervision, the FSA utilizes inspections and reports done by other bodies by studying beforehand the reports and comments of internal inspectors and auditors from each sector. Supervisory activities of various bodies do not overlap, and efforts are made to ensure that other supervisors' comments are taken into account.

6.3 Areas of development in regulation and supervision

Because of the constantly changing nature of the underlying risks, regulation and supervision of payment systems should be targeted for continuous developmental efforts even as regular supervision is being carried out. Otherwise regulation and supervision may lag behind the times and their effectiveness might suffer. Some areas of regulation and supervision that can be made more effective eg by preparing a development programme are presented in the following.

A development programme might include eg the following areas, as necessary.

a) More efficient collection of risk data

   Supervisory bodies have not had systematic access to data on realized payment system risks and the losses involved, systems disturbances and errors, or faulty payments. The collection and use of such data would help in anticipating risks, estimating realization probabilities and getting a rough idea beforehand of the magnitudes of potential losses. To broaden the base of experience, data on foreign payment systems risks could also be included. Collected data could be stored in a computerized risk database, for easy use in analytical studies and actual supervision.

b) Enhanced supervision

   Payment system supervision could also be improved and made more effective by introducing new techniques, such as computer-aided supervision and probabilistic methods. The expertise of outside supervisory bodies could also be utilized by authorizing

them to make certain special inspections, eg in respect of IT operations or information security. The FSA and the Bank of Finland could cooperate in supervisory work and in a joint working group in respect of cases that clearly belong to their overlapping sphere of supervision.

c) Increased regulation by the industry and market regulation and self-regulation

   The following are examples of how regulation can be broken down into regulation of the industry, market regulation and self-regulation. In order to establish minimum objectives for information security in the banking sector, the Finnish Bankers' Association could be assigned the task of preparing minimum standards applicable to all banks. Correspondingly, the banks could jointly determine minimum standards for the provision of Internet services to customers.

d) Enhanced supervision by the industry and market supervision and self-supervision

   The banks could also, under the auspices of their own cooperative bodies, agree on the enforcement of minimum standards or standards for Internet services deriving from industry self-regulation.

This kind of partial breakdown of regulation into regulation by the industry and market regulation and self-regulation would increase the effectiveness of supervision but would also require clear delineation of supervisory duties and responsibilities, real incentives, and sanctions for infractions. The detailed planning of development is best handled as a special project.

6.4 Outlook for international cooperation

In Europe payment system supervision is becoming a cooperative function of central banks and banking supervisors. According to recent legislation in many countries, the central bank is responsible for broad oversight of payment systems and banking supervisors for payment transactions of individual institutions. In practice, this

implies cooperation between the two bodies because large supervised entities are crucial from the standpoint of systemic risk.

The launching of the ECB and the ESCB on 1 January 1999 signifies a change in the broad oversight of payment systems in the euro area. The EU-wide TARGET payment system will be introduced. Oversight of the EBA clearing system will be transferred from the EMI to the ECB and the central banks of the euro area. The ECB is entitled to issue regulations to secure efficient and reliable clearing and payment systems in the EU. The central banks will be responsible for the oversight of large-value payment systems in their respective countries.

The European Commission regulates oversight of payment systems by issuing directives and participating in preparatory work. The Commission will soon issue directives inter alia on settlement finality and collateral; reorganization and winding up of credit institutions; and the issuance of electronic money. The Commission has also been concerned about consumer protection and has issued related recommendations, which will be extended to include e-money and electronic payments as well as provision of remote services. Within the Banking Advisory Committee (BAC), under the Commission, the supervisory bodies are discussing issues related to international regulation in the EU.

Central banks participate in discussions on payment system risks and their management in a global setting in the Bank for International Settlements and its Committee on Payment and Settlement Systems. In recent years, countries not belonging to the Group of Ten have been increasingly involved in the activities of the BIS, and most Asian countries have become members. The BIS provides a global forum for cooperation in payment system supervision and management of systemic risk as well as an appropriate forum for studies and research. The expansion of banks' operations over several continents and the rapid intercontinental contagion of crises have clearly demonstrated that cooperation in payment system oversight is also needed at the global level.

References

BIS publications

Report on Netting Schemes (1989), Bank for International Settlements, Basle.

Report of the Committee on Interbank Netting Schemes of the Central Banks of the Group of Ten Countries (Lamfalussy Standards 1990), Bank for International Settlements, Basle.

Delivery Versus Payment in Securities Settlement Systems (1992), Bank for International Settlements, Basle.

Central Bank Payment and Settlement Services with Respect to Cross-Border and Multicurrency Transactions (1993), Bank for International Settlements, Basle.

Cross-Border Securities Settlements (1995), Bank for International Settlements, Basle.

Settlement Risk in Foreign Exchange Transactions (1996), Bank for International Settlements, Basle.

EMI background papers

Minimum Common Features for Domestic Payment Systems (1993), Working Group on EC Payment Systems, Frankfurt.

Report to the Council of the European Monetary Institute on Prepaid Cards (1994), Working Group on EU Payment Systems, European Monetary Institute, Frankfurt.

Standards for the Use of EU Securities Settlement Systems in ESCB Credit Operations (1998), European Monetary Institute, Frankfurt.

ISO publications

Banking, securities and other financial services – information security guidelines, ISO/TR 13569 15 Nov 1996.

Appendix 1

Detailed description of payment system risks

1 Risks associated with debit payment instruments

Risks associated with debit payment instruments are mainly domestic since banks' debit payment instruments are still fairly seldom used abroad. It is likely that foreign risks will increase in the future. In Finland debit payment instruments, especially debit cards, have to a large extent replaced cash as a payment medium.

1.1 Credit risks

1.1.1 Bank credit risks

Banks engage in temporary financing of transactions initiated with debit payment instruments since an interbank settlement is generally executed only after crediting the receiving customer's account. Debit cards are issued with a FIM 1000 guarantee. In this regard, there is a difficult legal question with respect to insolvency: In case of insolvency of the card-issuing bank, is it or the redeeming bank responsible for the seller's guarantee?

Electronic money may replace a portion of debit card payments and thus alter banks' credit risks.

The use of debit payment instruments entails relatively little bank risk if a large share of the account payments credited to customers' accounts are initiated with payment instruments certified by other banks, eg cheques and debit card payments.

(Current risk level: –.)

1.1.2 Customer credit risks

A guarantee issued on a debit card carries a risk to the issuing bank. If the issuing bank credits the seller's account for transactions beyond the value of the guarantee, the bank bears a credit risk that is especially serious in the absence of a cover check since it could be liable for a compensation claim. Quick crediting of card payments to sellers' accounts is a competitive tool that is difficult to abandon. However, the credit risks involved are not significant, except in situations where the bank does not verify exceptionally large transactions or turnovers.

(Current risk level: –.)

1.2 Liquidity risks

Payment instrument transactions rarely involve liquidity risk because their total monetary value is only a small share of that for all payment transfers. These transactions are processed in the PMJ clearing system and are relatively well spread between the banks and predicable.

(Current risk level: –.)

1.3 Operating risks

1.3.1 Information system risks

The processing of debit transactions can be characterized as decentralized, batch, nonurgent, off-line, and secured by manual backup systems. Thus the risks involved are due mainly to traditional possibilities for errors, such as multiplication or destruction or distortion of transaction information, which can be corrected fairly quickly after detection. The only critical areas are bank-specific on-line authorization systems and PIN code control systems.

(Current risk level: j.)

1.3.2 Administrative risks

Administrative risks are connected with safe custody of payment instruments and timely updating and accuracy of the information in information systems. Electronification is increasing the need for good and secure controls for card systems. Disappearance of PIN code keys or transfer to criminal hands entail significant risks. Switching to chip cards expands the possibilities for protection but also introduces a new potential source of administrative risks. A wide disruption of the security systems may cause a system-specific crisis, which can lead to a temporary shutdown - eg of a debit card system - for repairs or changes in security arrangements.

(Current risk level: j.)

1.3.3 Crime risks

Debit cards can be used to obtain cash and other items of value. Card payment transactions are partially protected by personal identification numbers (PIN codes). If bank employees work with organized crime, fairly large losses can result, although losses are limited by the small size of individual transactions. Organized crime is however becoming increasingly involved in this area. These risks are being reduced by the introduction of chip cards, increasing emphasis on on-line transactions and the use of statistical verification methods.

Payment instruments always involve various risks of misuse. According to international comparisons, the situation in Finland is fairly good. However, the risks are increasing, and it would be prudent to replace cards with magnetic strips by chip cards during the next few years. Wide use of off-line EFTPOS systems and slow updating of

'hot card files' enable misuse eg using stolen or found payment cards. However, realization of these risks has not yet destabilized payment card services. Investments in this area can be partially based on statistical methods. A wide wave of organized counterfeiting could trigger temporary restrictions on the use of debit cards in order to enable improvements in the security systems.

(Current risk level: j.)

1.4 Environment risks

1.4.1 Risks of changes in legislation or market practices

As regards debit payment instruments, consumer protection and other authorities have continually reduced customers' risks at the expense of the banks. Banks cannot leave their customers with unreasonably large risks to bear, and moreover these risks are relatively small from the banks' viewpoint.

(Current risk level: –.)

1.4.2 Risks of loss of confidence

Payment instruments entail significant risks of loss of confidence (cf the effect of genuine-looking counterfeit notes on the confidence in cash). A massive and successful counterfeiting operation could cause loss of confidence in a debit card system. A wave of bank insolvencies in which merchants were left holding the bag could cause a serious loss of confidence.

(Current risk level: j.)

1.4.3 Risks of technical change

The introduction of microchip-based chip cards impacts the technology and use of debit cards. Supranational chip card systems or e-money issued by the central bank can considerably reduce the use of debit cards. New systems may in certain circumstances quickly displace old procedures. Increased electronification also increases the dependence on technology and specialized suppliers. Failure of electronics or system obsolescence may require a rapid modification of the system.

(Current risk level: j.)

1.4.4 Catastrophic risks

Catastrophic risks are associated mainly with the use of electronic debit payment instruments, ie magnetic cards and, in the future, chip cards. If a malfunction occurs in key IT systems, these payment instruments become difficult to use. The high degree of concentration in the Finnish banking sector means that if a catastrophe were to occur and the IT equipment and systems of two large banks were dysfunctional for a fairly long

time, it would be difficult to use electronic debit payment instruments in Finland. On the other hand, the banks' IT systems are relatively secure.

(Current risk level: j.)

1.5 Clearing and settlement risks

1.5.1 Systems risks

Settlement of debit transactions is executed in the BoF-RTGS system in connection with PMJ clearing. The timing of debit transactions settlement is not critical. There are no significant settlement risks connected with debit payment instruments.

(Current risk level: –.)

1.5.2 Collateral risks

In Finland collateral is not used in the settlement of debit transactions. The sending bank can simply charge the account holder's bank. The account holder's bank can verify the authenticity of the transaction only ex post and then claim compensation for a faulty transaction. The rules and participation criteria for settlement must enable reclamation for faulty transactions in all situations.

(Current risk level: –.)

1.5.3 Settlement cancellation risk

Settlement of debit transactions is done on the basis of multilateral netting. In case of a bank insolvency, the netting can be unwound, which means there is a credit risk. However, debit transactions are small in volume compared to other types of transactions. Amendments to the existing laws will probably guarantee finality of netting in Finland by end-1998

(Current risk level: –.)

1.6 Systemic risk

Realization of systemic risk, particularly in connection with debit payment instruments, seems to be rare; an exception would be a situation involving a massive counterfeiting operation. Debit payment instruments are becoming more important as the use of cash declines. In the long run, dependence on electronic debit payment instruments will increase the danger of technology-related systemic risk in this subsector of payment transfers.

(Current risk level: –.)

1.7 Summary of risks associated with debit payment instruments

The danger of system-specific risk is fairly small in respect of the following:
- paralysis of information systems
- widespread criminal misuse
- loss of confidence
- sudden technical change
- a catastrophe that prevents system usage.

Debit payment instruments do not entail bank-specific risk or systemic risk.

2 Risks associated with small-value credit transfers

In Finland the share of small-value credit transfers in the total value of payment transfers is significant. The volumes are large, and customers are dependent on reliable operation of the credit transfer system, which is heavily electronified.

2.1 Credit risks

2.1.1 Bank credit risks

Small-value interbank credit transfers always involve bank credit risk when a bank credits the receiver's account before the arrival of covering funds. This risk will be realized if a participating bank has liquidity problems or becomes insolvent and cancels its payments. The bank credit risk associated with small-value credit transfers varies considerably according to the day of the month, mainly in connection with the timing of recurrent payments. The total size of bank credit risk is not presently monitored systematically nor subject to limits. This risk will be reduced by the introduction of morning clearing in 1998 and eliminated by the introduction of nighttime clearing in 1999.

In cross-border credit transfers within the EU area (up to ECU 50 000), the sender's bank is responsible for mistakes made by intermediary banks up until the transferred funds are credited to the receiving bank's account. The receiving bank is responsible for transferring the funds to the final receiver (Directive 97/5/EC of the European Parliament and of the Council of 27 January 1997 on cross-border credit transfers).

(Current risk level: p, s.)

2.1.2 Customer credit risk

Banks do not encounter customer credit risk in small-value credit transfers if the cover is verified and reserved in the payer's account before the payment is made. If the account does not contain sufficient funds, the payment order is held up until sufficient funds arrive. Cover verification is one of the basic requirements of risk management, and most, but not all, Finnish banks do it. For some (especially large) customers, there is not always

verification of cover because of a so-called technical limit or an agreement on nonverification of cover.

The bank is responsible for funds transfer that it has accepted and must refund diverted or lost funds according to the agreement with the customer and the principles of contract law.

(Current risk level: p, s.)

2.2 Liquidity risks

Net clearing and settlement of small-value credit transfers at the end of each day in the BoF-RTGS system reduces banks' liquidity needs compared to gross values. Netting also reduces the size of liquidity risk but shifts the timing of the risk to the end of the day when there is little time left to obtain additional liquidity.

Potential cancellation of individual credit transfers does not create liquidity risk for banks because the values of these transfers are small compared to banks' total liquidity and fit easily within the normal random fluctuations.

If an individual bank cancels all its credit transfers to other banks or they are not completed due to insolvency or bankruptcy, liquidity problems may spread to other banks and cause a degree of systemic risk.

(Current risk level: p, s.)

2.3 Operating risks

2.3.1 Information system risks

In Finland the processing of credit transfers is decentralized, ie there is no clearinghouse. Payment information is exchanged bilaterally between banks several times a day on a batch basis but clearing and settlement are done centrally at the Bank of Finland. The advantage of decentralization is less vulnerability compared to a fully centralized system. However, reliable IT operations and data interchange are important because the number of daily transactions is large.

Risks caused by brief disturbances are not significant in terms of aggregate value due to the small value of the transactions and the lag in the value date.

If the credit transfer system of a bank becomes paralysed for an extended period, it may cause a bank-specific risk as the customers shift their credit transfer business to other banks. It is also possible with a computer-based system that a large number of small-value credit transfers are multiplied or lost, which may cause a fairly large risk despite the small values of individual transactions.

Payments executed via terminals located in companies, homes etc are extremely dependent on the functionality of the banks' IT, communications and security systems.

(Current risk level: j, p, s.)

2.3.2 Administrative risks

The manual phases of payment transfers are especially susceptible to error and misuse. Increased electronification of payment information processing has reduced errors (eg transfers to wrong accounts and data corruption or loss) and enabled computerized controls. Verification of the reasonability of transfer amounts cannot be done automatically for small-value credit transfers, because large-value credit transfers are processed in the same system. In the future large-value credit transfers will be channelled to the RTGS and POPS systems, which will reduce risks and enable the introduction of amount limits.

Staff incompetence, carelessness in effecting payment transfers and maintaining systems, neglect of control and reporting procedures, or failure to provide instructions for the employment of backup systems in the event of a disturbance may lead to situations in which customers' orders are delayed or not executed. Credit transfers may go to the wrong accounts and transaction information may be corrupted or lost due to various faults. Banks are able to correct individual errors, but simultaneous occurrence of a number of large errors may – absent clear prior instructions – lead to a situation that is difficult to manage and so a create serious problem.

If a cross-border credit transfer sent by a bank is lost in transit, the sender is entitled to a refund from the credit-transfer sending bank, with costs and interest, within fourteen business days following the request date. The refund limit is ECU 12 500 unless the receiving bank's account has been credited with funds in the amount of the payment transfer. (Directive 97/5/EC of the European Parliament and of the Council of 27 January 1997 on cross-border credit transfers.)

(Current risk level: p, s.)

2.3.3 Crime risks

Criminal activity in connection with credit transfers, which may be bank-external or – internal, may be based eg on someone making credit transfers using the name and account data of a genuine sender but directing the funds to his own account or that of an accomplice. This can be done by creating an unauthorized order in someone else's name, by forging someone else's order, or by appropriating a security code that has not been kept secure etc. A criminal may cause significant losses by multiplying manyfold genuine transactions and transferring the funds to his own account. By acting swiftly, criminals endeavour to transfer funds before they are noticed; in this, they are aided by fast modern information technology.

The current means of transferring express transfers and bank giro envelopes has been vulnerable to crime because of their manual phases, which enable criminals to snatch payment orders outside of banks (via telephone, fax, safe-deposit boxes). Banks and customers are sometimes deceived with stolen information when banks are not extremely careful in verifying authenticity. Hence the use of the telephone or fax is not recommended for the accepting of customers' credit transfer orders.

The security risk in interbank express credit transfers is reduced in the new POPS system. The risk in transfers between customers and banks will remain if banks continue to accept credit transfer orders by telephone or fax from certain customers. The risk of fraudulent payment orders also exists in the provision of payment services since customers' signatures on payment orders are not fully verified in all banks.

Crimes related to electronic services are increasing, and thus banks need to maintain and enhance the security systems used in remote electronic services, provided eg via Internet. The international risks of remote operations are obvious in connection with Internet.

(Current risk level: j, p.)

2.4 Environment risks

2.4.1 Risks of changes in legislation or market practices

There is no specific legislation governing payment systems in Finland. Market practices in respect of customers' small-value credit transfers are based on standard agreements between customers and banks. These agreements contain general clauses inter alia on refund procedures in cases where the bank or the customer is guilty of faulty operations. In disputable cases the Consumer Ombudsman and the courts have usually protected the weaker party, ie the customer. The related danger of loss to banks is usually small due to the small value of credit transfers and the infrequency of disputes.

Banks' duty to intermediate payment transfers with care was defined in a recent court decision in which a bank had to refund a sender for a transfer directed to the wrong account, even though the sender had given the wrong account number (but the proper name). A problem with the present payment systems is that they do not compare the receiver's name as given by the sender to the account number in order to detect a possible error beforehand.

Interbank exchanges of credit transfer information and covering funds are based on interbank agreements. As yet there is no legislation governing payment and settlement finality or the legal validity of netting.

In international credit transfers, banks must take into account national practices and prepare for difficulties in interpreting legislation.

(Current risk level: p, s.)

2.4.2 Risks of loss of confidence

A risk of loss of confidence might arise in the banks' credit transfer system if individual payments are not executed at their full value or if an intermediating bank is unable to intermediate outgoing payments and credit incoming payments to customers' accounts. The problem might be caused by a technical disturbance, liquidity problem or bankruptcy. It is important to resolve the disturbance quickly so as to prevent it from expanding from a bank-specific problem to a threat of loss of confidence in the whole system, ie a systemic risk.

A massive counterfeiting operation may also weaken customers' confidence in the payment system.

(Current risk level: j, p, s.)

2.4.3 Risks of technical change

The banks' payment transfer system is highly automated, technically of high quality and reliable and has so far been a cheap means of handling a large volume of payments. In terms of the technology, it is facing competition from various services provided via data networks, eg cheap payment services provided via Internet, where a services order and payment are combined into a single service. The most serious problem so far in this connection is guaranteeing adequate security and gaining public confidence. Therefore, a significant shift of credit transfers away from the banks is not envisaged for the next few years, especially in light of the fact that banks are starting to provide their own services also via Internet. Security system failures or obsolescence may in certain situations require quick changes.

(Current risk level: j.)

2.4.4 Catastrophic risks

The banks' credit transfer system is extremely dependent on IT technology and interbank communication links and is thus vulnerable eg to electricity interruption, flood damage, fire, sabotage, terrorism etc. However, the system's decentralized structure does reduce its vulnerability. All banks should have backup systems, and these should be tested regularly to ensure that they can be put into operation fairly quickly when the need arises.

Banks' computer centres and other premises are traditionally well protected against external factors, and banks generally have various backup systems. However, the level of readiness of these backup systems varies widely across banks.

In the event of a catastrophe, the major problem for individuals as regards payment transfers concerns the payment of bills and withdrawal of money from accounts should a bank become inoperative. For big companies, the problem is how to quickly find out what phase of payment execution a bank was in at the moment it dropped out of the system and to redirect the payments via another bank.

(Current risk level: j, p, s.)

2.5 Clearing and settlement risks

2.5.1 Systems risks

The Bank of Finland acts as a settlement centre for credit transfer covering funds. It is important that these central bank functions and systems remain operative because a failure could cause paralysation of the entire credit transfer system. It is essential that the Bank of Finland have backup systems and agreed operating procedures for handling settlements in case of an internal technical disturbance. The insolvency of a system participant will cause an interruption of the credit transfer settlement process and possibly cancellations. At the very least, it will cause liquidity problems to other participants. Cancellation of credit transfers also entails a degree of systemic risk.

From the clearing bank's viewpoint the weakest link in clearing consists of the banks' clearing calculations, which are not currently verified ex ante by the receiving bank. As a result, a settlement may be carried out on the basis of unverified, erroneous data. Errors are not corrected until the next day.

Because repeated deliberate errors would result in exclusion of the offending bank from the cooperative clearing operation, exploitation of the possibilities for misuse is unlikely. In 1999 Finnish banks will introduce a procedure by which clearing information is compared to payment order transmissions and funds transfers.

(Current risk level: pp, s.)

2.5.2 Collateral risks

Because interbank clearing debts are not covered by collateral, neither are the banks' clearing positions, which can nowadays be sizable. This, however, does not cause a serious systemic risk.

(Current risk level: pp, s.)

2.5.3 Risks of settlement cancellation

Covering funds for interbank credit transfers are sent to receiving banks at the end of the day on the basis of netting. In case of insolvency or bankruptcy, the bankrupt's estate can demand an unwinding of the settlement because multilateral netting based on an agreement is not valid in the event of bankruptcy. The breaking down of a netting into separate (gross) payments can lead to sudden changes in banks' positions and even losses. This introduces a small degree of systemic risk even as regards small-value credit transfers.

Work is in progress on the related Finnish legislation. New laws and amendments to the existing laws will probably enter into force before 1999.

(Current risk level: pp, s.)

2.6 Systemic risk

There is only a small (but greater than zero) systemic risk associated with small-value credit because contagion is unlikely.

(Current risk level: p, s.)

2.7 Summary of risks associated with small-value credit transfers

System-specific risk is fairly small in respect of the following:
- information systems risks
- crime risks
- risks connected with loss of confidence and technical change
- catastrophic risks.

Bank-specific risk is small or fairly small in respect of the following:
- crediting receivers' accounts before settlement
- interruption of credit transfers
- multiplication of credit transfers
- disturbances to IT systems, sabotage etc
- payment transfers to other banks
- uncollateralized positions
- unwinding of settlement
- cancellation of settlement.

The danger of overall systemic risk associated with small-value credit transfers is fairly small in respect of the following:
- contagion of credit risk associated with the counterparty bank
- contagion of liquidity risk connected with the sending bank
- risks associated with changes in legislation due to obsolescence of laws
- contagion of the risk of loss of confidence when a disturbance is prolonged
- systemic risk due to possible unwinding of netting.

3 Risks associated with large-value cheques and bank drafts

Large-value cheques and bank drafts are used regularly mainly for payments related to securities transactions and companies' payments between banking groups. Large-value cheques are fairly frequently used in making international payments.

3.1 Credit risks

3.1.1 Bank credit risks

If a receiving bank accepts a large-value cheque[1] and credits the value to a customer's account before receiving covering funds from the transferring bank, it is subject to bank credit risk. The introduction of limits in the POPS system in 1998 will effectively control bank credit risks.

Banks often limit their risks associated with international cheques by means of customer commitments.

(Current risk level: pp, s.)

3.1.2 Customer credit risks

There is no customer credit risk for the receiving bank associated with these transactions. A transferring bank incurs a risk, but in the POPS system the immediate reserving of covering funds reduces this risk significantly. There is a risk connected with a bank draft if the customer's account is not debited in the amount of the draft when the draft is written nor is cover reserved in the account. Customer commitments may prove worthless in the event of a bankruptcy.

(Current risk level: pp, s.)

3.2 Liquidity risks

Individual sums transferred by cheque may be quite large. Large-value cheques are nowadays used especially in connection with securities transactions. In the near future developments in respect of payment transfers in the securities market will eliminate cheque-related problems.

Liquidity risk may arise when a bank receiving covering funds evaluates its liquidity position on the basis of redeemed large-value cheques only to find that settlement is not accomplished due to technical problems, delays, errors etc.

(Current risk level: pp, s.)

[1] Hereinafter the term 'cheque' refers to both cheques and bank drafts.

3.3 Operating risks

3.3.1 Information systems risks

Normal cheque transactions are still processed manually because customers' cheques are physically delivered to banks. Presentments and receipts of cheques trigger corresponding entries in banks' information systems, which in some cases have limits on reserving of covering funds. Interbank clearing and settlement of a cheque in the context of the POPS system is done on a net basis within the BoF-RTGS system or as an RTGS gross transfer (the latter method being mandatory if the value exceeds the gross limit for the POPS system). For large-value cheques, the possibility always exists of shifting to manual processing and so there is no system-specific or systemic risk involved.

(Current risk level: p.)

3.3.2 Administrative risks

The banks' current practice of agreeing with large customers on nonverification of cover in connection with payment transaction accounts increases banks' customer risks.

In some cases, the bank may execute a transaction for a customer that irrevocably obligates the bank but does not require settlement at the moment of execution (eg foreign payment transfers). However, in doing this, the bank is obliged to (irrevocably) credit the receiving bank. If the sending bank does not reserve cover in the customer's account, it exposes itself to credit risk. However, since the fault is in the bank's internal procedures, this risk is classified as an administrative risk.

Special care must be taken in the physical processing, safekeeping, archiving and signing of cheques. The bank's processing procedures should ensure that persons responsible for processing and safekeeping of cheques do not have the authority to sign them. Special attention should be paid to the safekeeping, record-keeping and removal from the vault of blank cheques.

Careful observance of procedures is extremely important in accepting cheques. It is the duty of the bank to verify the correctness and authenticity of the cheque, its value and the signatures. It is also bank's duty to identify stolen cheques reported to it.

Banks inform their correspondent banks of their official signatories at regular intervals and supply them with sample signatures, usually on microfilm. It is crucial that this information be kept up-to-date and that banks' procedures minimize potential insider information frauds by observing the practice of always having at least two informants who occupy different positions in the organization.

(Current risk level: p.)

3.3.3 Crime risks

Forged cheques and banks' signatures are rare in Finland. Stolen cheques or bank drafts are seldom presented in Finnish banks. Increased misuse of own cheques has forced banks to limit the issue of cheques to those persons and companies that are known to be reliable users of cheques. Doubts about possible forgeries may cause banks to delay the honouring of cheques by submitting them for collection. Organized crime concentrating on one small bank may cause a bank-specific crisis.

(Current risk level: p.)

3.4 Environment risks

3.4.1 Risks of changes in legislation or market practices

In Finland legislation and market practices governing cheques are firmly established and cheques are turned over very quickly. In foreign payments, even though international practices regarding cheques are well established, banks are vulnerable to local changes, especially in countries with slow turnover of cheques.

(Current risk level: p.)

3.4.2 Risks of loss of confidence

Overall confidence in cheques is good, but large-scale misuse may necessitate more secure payment practices. An individual bank could face a situation where its cheques are no longer trusted.

(Current risk level: j, p.)

3.4.3 Risks of technical change

Paper-based cheques are being replaced by new electronic payment instruments. There have been attempts to electronify cheques. The transition to the new technology will probably take place in a smooth and controlled fashion, without interruptions to banking operations or systems.

(Current risk level: –.)

3.4.4 Catastrophic risks

Settlement of domestic large-value cheques depends on the POPS and BoF-RTGS systems. Catastrophes affecting these systems may thus cause risk realizations related to the use of large-value cheques. The probabilities of bank-specific and system-specific risks are extremely low.

(Current risk level: j, p, s.)

3.5 Clearing and settlement risks

3.5.1 Systems risks

Cheques not exceeding the gross limits are processed in the POPS net clearing system, where interbank cheques can be presented without limitations. This risk will be eliminated in May 1998, when bilateral net limits are introduced in the POPS system.

The BoF-RTGS system has strict requirements for operational reliability since even a brief interruption of services could expose participant banks to cumulating bank-specific risks so long as the real-time settlement is delayed.

The volume of large-value cheques is so small that clearing and settlement can be done manually if necessary. Especially in foreign cheque payments, it must be ensured that settlement is not executed twice.

(Current risk level: p, s.)

3.5.2 Collateral risks

Collateral is not used in bilateral interbank clearing debts. The net limits of the POPS system have effectively controlled cheque debt positions since May 1998.

(Current risk level: p, s.)

3.5.3 Risks of settlement cancellation

A part of the interbank cheque transactions is settled on a net basis at the end of the day (net settlement of the POPS system at closing). According to the existing legislation, a netting may have to be cancelled at the demand of the bankrupt's estate in the case of insolvency or bankruptcy. Unwinding of netting may lead to sudden changes in banks' positions. However, the Finnish legislation governing these matters is under development, and the related amendments will probably enter into force in 1998.

As regards foreign cheques, banks should estimate the risk of settlement cancellation on the basis of legislation and practices in each participating country.

(Current risk level: p, s.)

3.6 Systemic risk

The realization of systemic risk in connection with large-value cheque payments is possible, but highly unlikely. Misuse within a bank is more probable. This may be caused by a breakdown of internal controls and resultant exposure to customer-specific misuse to the extent of threatening the bank's liquidity. This danger affects mainly smaller banks.

(Current risk level: pp, s.)

3.7 Summary of risks associated with large-value cheques and bank drafts

The danger of system-specific risk is fairly small in respect of the following:
- loss of confidence
- catastrophes.

The danger of bank-specific risk is small or fairly small in respect of
- large-value cheques and bank drafts, and the danger of systemic risk is relatively small in respect of large-value cheques and bank drafts.

4 Risks associated with large-value credit transfers

The bulk of payment volumes is accounted for by large-value credit transfers. Most payments connected with the money and investment markets are made with credit transfers.

4.1 Credit risks

4.1.1 Bank credit risks

The receiving bank is exposed to bank credit risk if it credits the account of the final receiver prior to settlement. Presently, banks' control procedures are inadequate. Introduction of 'POPS limits' and conversion of loro payments into RTGS payments are improving the situation considerably in 1998.

The sender's bank is exposed to bank credit risk if its intermediating responsibility extends beyond settlement and transfer of payment information. There is a degree of uncertainty in Finnish legislation concerning the sending bank's responsibility in this regard.

Exact definition of bank credit risk is hampered by the uncertainty of the legal status and obligations of banks within the payment process. According to past cases, a payment cannot be cancelled once it is credited to the final receiver's account. However, it remains unclear whether the payment is to be regarded as the customer's property before it is credited. It is perhaps also be unclear whether the sending bank's responsibility definitely ends once the payment information and covering funds are transferred.

In foreign payment transfers, banks' counterparty risks are connected with the correspondent banks sending and receiving the covering funds. Banks have traditionally assumed particularly large short-term counterparty risks in foreign exchange trades.

(Current risk level: ppp, sss.)

4.1.2 Customer credit risks

Banks assume customer credit risk when they forward credit transfers without verifying covering funds in the customer's account. Banks sometimes have agreements with their largest and most important customers on nonverification of accounts on the presumption that covering funds will arrive later in the day. In such cases, the banks are providing intraday uncollateralized credit.

In the intermediation of payments abroad from domestic accounts, irrevocable transfer of payment funds prior to debiting of the domestic account entails customer credit risk for the sending bank since the account may not contain sufficient cover.

(Current risk level: p, s.)

4.2 Liquidity risks

The sending bank needs liquidity in order to transfer funds to the receiving bank (whether for net settlement or RTGS transfer). The receiving bank will suffer a loss of liquidity only if it credits the customer's account but does not receive covering funds and the receiver immediately transfers the funds from his account to another bank.

Liquidity risks will grow in the future because RTGS transfers are done on a gross basis and POPS nettings must be settled immediately once the total value of payments reaches the limit. If the processing of transactions is skewed over the course of the day (outgoing payments processed first and incoming later), some banks may have huge liquidity needs while others have surpluses.

There is also the danger of a large bank misestimating its liquidity position and thus creating a liquidity shortage that lengthens payment queues for all the banks and causes gridlock of the system.

(Current risk level: ppp, ss.)

4.3 Operating risks

4.3.1 Information systems risks

Large-value credit transfers entail significant information risks because the effects are noticed immediately in real-time systems. Large-value credit transfers have tight schedules and customers depend on timely execution. Banks enter their funds transfer transactions in the BoF-RTGS system for the most part manually, which slows the processing and creates additional risks.

Transaction information may become multiplied or lost in the event of an information system problem. Few banking systems have control limits in order to verify that large-value payments remain within statistically defined limits.

The management of information systems risks connected with large-value payments is facilitated by the relatively small number of such transactions, which means that a significant share can be processed manually in an exceptional situation.

(Current risk level: pp, s.)

4.3.2 Administrative risks

One significant risk associated with large-value payments is that the wrong account may be credited. According to court decisions, this is the banks' risk. Payments are currently credited solely on the basis of account number even though the customer is asked to provide the receiver's name. In one case the Supreme Court decided that the verification practices of Finnish banks are inadequate and that in the present circumstances banks must bear the additional risks. In practice, such risks have been limited by value caps on automated transfers.

In some banks an employee can execute a very large credit transfer on his own, ie without checking and verification by another employee.

(Current risk level: pp, s.)

4.3.3 Crime risks

A criminal may seek financial gain by sending an unauthorized payment order to a bank in another person's name or forging another person's payment order. Defects in the verification of order authenticity facilitate this type of operation. Large-value credit transfers can still to some extent be made via electronic systems using permanent passwords. Paper-based credit transfers are often delivered to banks by mail or similar means, in which case the only verification method is comparison of signatures. Thus the systems of Finnish banks are fairly vulnerable to crime, especially if criminals get inside help from banks or companies. In most cases of crime, the responsibility falls on the banks because it can be shown that their system controls were inadequate.

Another important type of crime is terrorism, which aims to render a bank or a whole system inoperable. In Finland the highly automated payment systems can be made inoperable by incapacitating IT equipment via viruses or physical damage.

(Current risk level: pp, s.)

4.4 Environment risks

4.4.1 Risks of changes in legislation or market practices

Payment transfers are significantly obstructed by unclear legislation as regards the responsible entity for payment arrival at each stage of the processing. Agreements between banks and customers can be helpful mainly in clarifying errors due to carelessness. However, in case of bankruptcy of a contracting party, the validity of a contract is always questionable. Banks' risks have increased due to a clear tendency to shift responsibility from customer to bank.

Another significant risk connected with legislation is that the laws do not support payment netting. In the absence of legislation governing netting, interbank payment transfer risks must be treated on a gross basis, which means that the risks may significantly exceed net positions. Amendments to existing laws will improve the situation by end-1998.

(Current risk level: pp, ss.)

4.4.2 Risks of loss of confidence

Risks of loss of confidence arise mainly when customers do not consider the system secure and reliable (eg payments are delayed because of technical or liquidity problems or are lost or altered). This risk may be realized by customers placing their payment orders at another bank. Customers who send large-value credit transfers probably react quickly to recurrent problems or service breakdowns.

(Current risk level: pp, ss.)

4.4.3 Risks of technical change

The transfer of large-value funds is under continuous pressure for further development. Due to the introduction of the euro and improving risk management, significant development projects concerning large-value payment systems will be implemented

during the next few years. Tight schedules and simultaneity of several projects may complicate the coordination.

Large-value credit transfers represent significant financial benefits. Thus it is possible that a global real-time large-value payment transfer network will be created in the near future. The required technology already exists. Should this kind of network be created, banks' large-value payment transfers outside the network would decrease dramatically.

Dependence on IT, communications and security systems gives rise to the danger of operational breakdown in the event of a serious disturbance.

(Current risk level: jj, pp, ss.)

4.4.4 Catastrophic risks

Catastrophic risks concern IT systems in particular. In Finland the volume of payments is still so small that in exceptional situations large banks can process most of the payment orders manually if necessary.

(Current risk level: pp, ss.)

4.5 Clearing and settlement risks

4.5.1 Systems risks

It will be possible in the future to settle large-value credit transfers via three different channels: net settlement in PMJ clearing or in the POPS system or as an individual RTGS payment. In large-value credit transfers, all the common domestic settlement procedures are used. It is to be expected that the number of RTGS transactions will increase in respect of both domestic and foreign payments. The TARGET system will reduce the risks associated with large-value settlements within the EU.

The BoF-RTGS and TARGET systems have strict requirements concerning operational reliability because even a brief interruption of services could expose participating banks to cumulating bank-specific risks if there are delays in real-time settlements. Real-time settlement is important especially in processing large-value credit transfers due to their significant size. As volumes increase, the backup systems also must be operational.

Systems connected with interbank settlements, current account facility interfaces, clearing systems and liquidity management software comprise a single entity that must operate smoothly also in unusual situations, both within and between banks.

(Current risk level: ppp, sss.)

4.5.2 Collateral risks

Collateral is not currently used in interbank settlement of debts. In the future the largest credit transfers - ie those exceeding the POPS system gross limit, those connected with the operations of the Finnish Central Securities Depository and TARGET payments - will be handled as RTGS payments, which means the settlements are immediately final and hence entail no collateral risk.

(Current risk level: ppp, sss.)

4.5.3 Risks of settlement cancellation

The above-mentioned problems connected with legislation on payment finality and netting validity also apply to large-value credit transfers. The significant volumes of credit transfers underline the importance of these problems. Along with changes in legislation, the settlement finality of the TARGET system will improve the situation considerably in the future.

Banks must individually assess the risks associated with their foreign correspondent account-keeping banks. Settlement risks associated with payments connected with foreign exchange trading are often particularly large.

(Current risk level: ppp, sss.)

4.6 Systemic risk

The systemic risk associated with large-value credit transfers is particularly large.

(Current risk level: ppp, ss.)

4.7 Summary of risks associated with large-value credit transfers

System-specific risk is small in respect to the following:
- technical change.

Bank-specific risk is associated with the following:
- nonverification of cover
- technical disturbances in information systems
- errors caused by carelessness
- forgery of payment orders
- crediting payments prior to settlement.

Overall systemic risk is associated with the following:
- crediting payments prior to settlement
- intermediating large-value credit transfers being dependent on sufficient liquidity
- the legislation does not adequately define banks' responsibilities or support the finality of netting and settlement
- a bank may suffer a loss of confidence, and this may spread to other banks
- information systems may be struck by a terrorist attack or other very serious disturbance

Risks are unclear in respect of:
- banks' responsibilities in bankruptcies.

Appendix 2

Detailed description of means of reducing risks

1 Risk control means for credit risks

1.1 Bank credit risks

RTGS payment method

Simultaneous transfer of the payment order and covering funds eliminates bank credit risk.

Counterparty limits

Risks can be contained in netting payment systems via counterparty limits. Real-time limits, which cannot be exceeded, are quite effective in reducing these risks. When limits are used, the possible structurally-based frequent or continual concentration of payment risks on one of two counterparties (asymmetry of risks) should be taken into account.

Monitoring system

Counterparty position monitoring systems should operate in real time.

Collateral

Risk connected with counterparty debt position can be reduced by the use of collateral.

Legislation and agreements

Rules governing payment finality and clear delineation of responsibility between sending and receiving banks facilitate risk management. If legislation supports netting (eg in case of bankruptcy, the bankrupt's estate cannot unwind executed payments based on obligations), bilateral counterparty positions can be netted without the risk of unwinding. Valid multilateral netting of counterparty positions can also be accomplished via institutional arrangements.

1.2 Customer credit risks

Transaction- and customer-specific limits

Customer limits need to be monitored on a real-time basis in order to be effective.

Collateral

Collateral requirements may reduce risks connected with limits.

Monitoring system

Banks' credit risk monitoring systems should be sufficiently comprehensive and should include short-term customer risks associated with payment transfers.

Risk analysis and classification of customers

Limit setting should be based on substantiated analysis of customer-related risks.

Customer-specific division of responsibilities

For each borrowing customer, a bank should designate a responsible employee.

2 Means of controlling liquidity risks

Payment netting

Netting reduces liquidity needs in payment systems with uneven payment flows.

Payment timing

Liquidity can also be managed by planning the timing of payments and centralizing the queuing system. Planning of the timing of payments and possible use of timetables require cooperation between the parties in order to establish common procedures.

Flexible adjustment of limits and collateral

To avoid unnecessarily large limits and collateral, the limits and collateral arrangements should be flexibly adjustable to changing liquidity needs.

Anticipation of liquidity needs

The bank's internal calculation systems should be able to estimate the bank's intraday liquidity needs with sufficient accuracy.

Relative liquidity requirement

The ratio of the bank's short-term funds to its estimated intraday liquidity position should be kept at a reasonable level.

3 Means of reducing operating risks

3.1 Means of reducing information systems risks

Reliable operation of a payment system is based largely on reliable information systems. Besides the automated elements, these information systems include manual elements, which must be smoothly and functionally interlinked.

Coordinated decisionmaking and standards

Risks connected with the interdependencies of information systems may be reduced by coordinating the related decisionmaking within a single operating unit and between parties. Standards comprise one of the primary means of coordination.

Systematic planning and maintenance

Systematic planning and maintenance reduces the probability of various errors and disturbances and improves recovery possibilities. Quality standards and systematic high-quality work are parts of systematic planning and maintenance.

Solid information systems architecture

Solid information systems architecture, based on wise selection of platforms, communication solutions, implementation and other tools etc reduces risks entailed in an overly complex system.

Qualified personnel

Avoiding and reducing risks, particularly those connected with automated parts of information systems, requires sufficiently skilled employees.

Employee training

Continuous training of employees helps to keep their expertise up to date and to use the changing systems in an appropriate manner.

Written instructions

Written instructions help employees to understand the effects of their actions on the overall operation and guide them in choosing the correct procedures.

Clear interfaces

Clear interfaces reduce the number of errors and help in correctly interpreting information.

Set-format for control of change

Having a set format for controlling change, which includes sufficient testing of changes to the information systems, reduces risks.

Backup systems and backup copies

Pre-planned and tested backup systems reduce the effects of realized risks and accelerate recovery. Sufficient backup copies are critical to the operation of backup systems.

Systems solutions can enhancing the security of information technology

Solutions that enhance the security of information technology, such as user names and passwords, transaction logs, encryption and signature checks, reduce misuse-related internal and information network risks.

Efficient internal control

Efficient internal control helps in anticipating risks in advance. Control can be complemented by internal supervision.

3.2 Means of reducing administrative risks

Administrative risks entailed in payment systems are usually connected with bank procedures, the existence and functionality of internal risk management processes, employee expertise, the existence and functionality of backup systems, readiness for disturbances and problems, and organization of systems maintenance and use. Administrative risks related to payment systems may be avoided and reduced inter alia by the following:

Prudent practices
(Observance of good payment transfer practices)

- requiring sufficient information on payment sender and receiver
- verification of information on incoming and outgoing payments
- care in physical processing, safekeeping, dispatch to customers, archiving and signing (cheques, bank drafts, debit cards, prepaid cards etc) of payment instruments
- observance of practices agreed between banks
- registering and reporting to responsible persons errors, corrections of errors and uncorrected errors
- appropriate customer interfaces based on agreements
- protection of systems from outside intruders.

Effective use of internal means of risk control
(Adequate control practices)

- customer information is sufficient and up to date (use of customer controls)
- operation of all systems, related payments, payments processing and controls are described phase by phase in sufficient detail (use of documentation)
- systems operative functions and monitoring are adequately separated
- all systems are overseen by responsible persons and internal owners
- the practice is observed of having two employees check and verify outgoing payment information or using other checking and protective procedures
- written system-specific risk controls are explained and distributed to everyone who is to observe or oversee them
- risks are controlled via management instructions and responsible persons at various levels of the organization, maxima, monitoring and decisionmaking procedures

- management receives regular reports on customer credit risk and bank credit risk limits and amounts. Express reporting to management and responsible persons of exceptional situations, eg limit overages and causes.

Employees adequate in numbers and skills
(Adequate expertise)

- responsibility for employee numbers and skills is assigned to a staff person and a management person
- adequate training and on-the-job initiation is arranged for all systems users and monitors
- management is sufficiently aware of broad system functions and related risks and takes responsibility for training new managers
- there is and operational personnel backup arrangement and trained substitutes in case of absences
- there is adequate extra training for maintaining expertise.

Good organization of systems maintenance and use
(Conscientious systems maintenance)

- there is sufficient documentation and instructions on systems maintenance, use, service, repair and the related organization, as well as records (verifiable by time and person) of system logins, use and logoffs
- changing and updating of systems software is appropriately secured
- instructions exist on updating, secure storing, destroying, altering, retrieving and archiving system information as well as on assigning responsible persons
- access of service and repair personnel to equipment areas and software is appropriately restricted, monitored and verified

Readiness to handle problems and disturbances
(Adequate instructions for disturbances)

- all banks should have written instructions on how to respond to the most common disturbances and problems
- in case a bank or its customer is removed from the clearing system due to insolvency, all participating banks (incl. the central bank) should must instructions on how to proceed in the event that a bank or customer is removed from the clearing arrangement due to insolvency, especially in respect of processing the payment orders of the removed participant.

Existence and functionality of backup systems
(Adequate backup systems)

- backup systems and arrangements with another party are needed to handle potential technical or other disturbances so as to ensure the availability of system services without undue inconvenience to customers
- backup systems and arrangements should be periodically tested in order to ensure that they will function properly when the need arises.

Written agreements between parties
(Adequate contractual basis)

- adequate agreements are needed between banks and correspondent banks and between banks and their corporate and private customers on compensation claims due to errors and delays connected with payment intermediation
- banks should have lists of those payment orders that have led to disputes and compensation payments.

3.3 Means of reducing crime risks

Security policy and procedural instructions

Written security policy, nomination of persons responsible for its implementation and procedural instructions for risk situations form a basis for secure operations.

Security planning as part of systems planning

Information systems risk can be reduced at the planning stage by a layered approach to protection, which aims at preventing crime, increasing the probability of apprehension and minimizing the effects of crime.

Monitoring

The main monitoring tools for reducing crime risk are alert limits, 'hot card files', exceptional cases reporting, recognition of pattern behaviour and statistical monitoring.

Separation of duties and other administrative measures

Effective administrative means of preventing internal misuse include the requirement of having two persons for certain operations, verification or implementation of a task by a second employee, breaking down tasks into subtasks, each handled by a different person, and occasional rotation of duties.

Procedures that increase security

The security of customer services can be increased via customer identification, verification of document authenticity and signatures, and debiting before crediting accounts.

Physical security

Physical security against crime can be increased by means of locking premises, controlling access, camera surveillance of premises and surrounding areas, and guarding and alarm systems.

Controlling access to information systems

Unauthorized use of information systems can be reduced by user identification, access rights control and monitoring of access violations.

Exchange of experiences

Protection against crime can be improved by exchanging information about criminal methods and means of protection.

Training

Appropriate training of employees helps them in timely recognition of crime risks and taking of appropriate measures.

4 Means of controlling environment risks

4.1 Means of reducing risks of changes in legislation and market practices

Active lobbying and anticipation of changes

It is often difficult to find means of protection against risks of changes in legislation. This is partly due to the fact that in the EU context legislative drafting has become more international. The most important means for avoiding and reducing risks associated with legislative changes will therefore be acquisition of information from various sources and active lobbying with expertise of domestic and foreign legislators and authorities.

Cooperation and discussions with interest groups

Means of protection against changes in market practices are closely connected with protection against changes in legislation. In both cases, the objective of protection is to eliminate the insecurity that hampers operations and the potential financial losses. This approach serves to guide banks' operational policy, information gathering and discussions with various interest groups.

4.2 Means of reducing risks of loss of confidence

Correct and timely information

The spreading of problems and increasing of losses can be avoided in most cases by correct information. Weak and untrustworthy communications can have the opposite effect, in which case a limited loss of confidence can spread through the whole banking system.

It is difficult to find means of protection against changes in confidence based on facts and in situations where the basic problems cannot be addressed immediately. In certain situations there may be eg rumours that are caused by misunderstandings, over-generalizing etc. The related risks of loss of confidence may be reduced by timely and effective communication.

Regular information

Rumours can be effectively prevented by advance and regular communications.

Well organized communications

Successful communication requires a well-functioning communications organization and policy supported by a crisis organization with sufficient decisionmaking authority. This applies to both individual banks and authorities.

4.3 Means of reducing risks of technical change

It is difficult to protect oneself in advance against the risks of technical change. Technological development cannot be prevented. Risks associated with technical change can be identified by following development trends already in the early phases. It is important to quickly find appropriate countermeasures against perceived significant changes or means for adapting to them. The most significant technical risks are connected with new and effective means of penetrating existing security barriers and rapid obsolescence of existing technology.

Adoption of new security techniques

It is worthwhile to invest in advance in new security systems and to use parallel means of protection. Customers are starting to adopt new techniques much faster than before. Automation of customer processes also causes rush hour peaks more often in communication and other systems.

Allowing for expansion of systems

Carefulness in the context of systems includes allowance for growth so as to enable rapid and error-free accommodation of fluctuations/accelerations in payment volumes. Increasing capacity takes time; hence the need to anticipate well in advance.

Technical changes in the banks' operating environment that affect bank services will continue. Customer service is being transformed from personal service to remote service via communication networks. At least some customers will in the future be served via virtual bank offices. Facing these challenges, banks must adopt a survival strategy consisting of utilizing new possibilities and adapting to a changing operating environment.

Preparedness for adaptation

The minimum need in new situations is to create good preconditions for adaptation, under which banks can effectively alter their products according to demand.

4.4 Means of reducing catastrophic risks

Effective access control

Finland has so far been extremely peaceful as regards natural catastrophes and terrorist attacks. Risks have been very small, but they are increasing. This is evidenced inter alia by tightened monitoring of computer centres and gradual upgrading of physical security features and security solutions. In this respect there still is room for improvement in Finland.

Backup equipment and resources

Potential catastrophes call for readiness to quickly employ backup equipment and other backup resources and for persons trained to handle unusual situations. In this respect Finland is very poorly prepared for catastrophes. A serious IT catastrophe in any bank would very likely completely paralyse the bank.

Decentralization of systems

Decentralized systems and backup systems enable partial operation of banking networks during a major disturbance. Finnish banking networks are highly centralized and hence highly vulnerable. Moreover, since the banking sector is also highly centralized, a problem in one of the large banks can easily expand into a systemic crisis.

Advance plans

Banks should have plans in place for handling a crisis and maintaining certain minimum services, and testing should be done on the functionality of these procedures. Banks need to have their own plans for providing limited services in case IT systems are only partially operational. Plans should also be in place for handling possible extended interruptions in IT services, including instructions for manual implementation of services.

5 Means of controlling clearing and settlement risks

Systems functionality

Clearing and settlement risks can be reduced by ensuring that existing systems and communications are of high quality, secure and highly functional. Adverse effects of possible disturbances can be either prevented or at least contained by having ready-to-go backup systems.

Adequate and secure collateral for credit

By requiring that participants post adequate collateral for credit, losses stemming from a participant's insolvency or bankruptcy can be avoided. Moreover, in systems involving international parties in particular, pledged collateral must be legally valid in case of insolvency or bankruptcy.

Irrevocability of settlement

Settlement finality can be ensured and disturbances and losses caused by payment cancellations can be prevented by means of legislation-level regulations governing payment finality in both gross and net payment systems.

6 Means of controlling systemic risk

Structures and procedures

The danger of systemic risk can be reduced via payment system structures that prevent systemic risk from arising (eg Lamfalussy minimum standards for netting systems) or practices that reduce the likelihood of realization or bank-to-bank or system-to-system contagion (eg RTGS, PVP, DVP, CLS).

Liquidity support systems

The danger of systemic risk can be reduced through central bank or clearinghouse provision of liquidity to parties having temporary payments difficulties, eg after a market crash or settlement interruption due to a technical problem.

Good backup systems

Tested and operational backup systems are also crucial. They must be ready to go at the onset of a disturbance. Backup systems can prevent a disturbance from spreading and multiplying into a systemic crisis.

Appendix 3

Abbreviations used in the text

ACCORD	=	SWIFT bilateral netting service provided to member banks
APACS	=	Association for Payment Clearing Services in the UK
BAC	=	Banking Advisory Committee
BIS	=	Bank for International Settlement; owned by central banks and serving as their international cooperation forum
BoF-RTGS	=	Bank of Finland's real-time gross settlement system; an interbank large-value funds transfer system
BOJ-NET	=	Bank of Japan Financial Network System; the large-value funds transfer system of the Japanese central bank
CHIPS	=	Clearing House Interbank Payment System; private net payment settlement system in the US
CLS	=	Continuous Linked Settlement; a planned settlement system for currency-related payments
Directive on cross-border credit transfers	=	Directive 97/5/EC of the European Parliament and of the Council of 27 Jan 1997 on cross-border credit transfers
DVP	=	delivery versus payment
EBA	=	ECU Banking Association, association of ECU clearing banks
EBA-clearing	=	Clearing system for ECU payments
ECB	=	European Central Bank
ESCB	=	European System of Central Banks
ECHO	=	Exchange Clearing House; netting centre for currency transactions in London
ECU	=	European Currency Unit, European basket currency unit calculated as weighted average of the values of the component currencies
EMI	=	European Monetary Institute
EMU	=	Economic and Monetary Union
EU	=	European Union
FCSD	=	Finnish Central Securities Depository
FED	=	Federal Reserve System; the US central bank
FEDWIRE	=	The large-value funds transfer system of the US central bank
FEYCS	=	Foreign Exchange Yen Clearing System; clearing system for externally held yen in Japan
FIBV	=	Federation International des Bourses de Valeurs; an international organization of stock exchanges
FX-NET	=	A private provider of bilateral netting services in London
G-10	=	Group of Ten, a group of ten countries that cooperate particularly via their central banks
G-20	=	Group of Twenty; a group that cooperates in the area of banking
G-30	=	Group of Thirty; a group that cooperates in the area of banking
IOSCO	=	International Organisation of Securities Commissions
ISO	=	International Standardisation Organisation
ISSA	=	International Society of Securities Administrators
IT	=	Information technology

Lamfalussy minimum standards	=	Six minimum requirements that multilateral netting systems should fulfil to be sufficiently stable
LORO	=	Loroclearing; clearing system of markka-denominated cross-border payments in Finland
MJO	=	Payment systems steering group, including the Bank of Finland and the banks
MJY	=	Payment systems cooperation group, including the Bank of Finland and the banks
Multinet	=	A netting bank for currency transactions in New York
PATU	=	Finnish banks' security system for customer communications
PIN	=	Personal Identification Number; used to identify debit card user in ATMs
PMJ	=	Finnish interbank payment system; primarily for bundled payments intermediation
POLT	=	Finnish banks' on-line data transfer network (ATMs and POPS payments)
POPS	=	Finnish banks' on-line express transfers and cheques; express transfer system
PVP	=	payment versus payment
RIX	=	Riksbankens system för avveckling av betalningar; large-value funds transfer system of the Swedish central bank
RTGS	=	real-time gross settlement
SSS	=	securities settlement system
SWIFT	=	Society for Worldwide Interbank Financial Telecommunication; a data transfer organization founded by banks maintaining a global interbank data transfer network
TARGET	=	Trans-European Automated Real-Time Gross Settlement Express Transfer System; a pan-European real-time gross settlement system, including EU countries' RTGS systems and the Interlinking network of central banks, which links the systems
TR	=	Technical Report, published by the ISO
VALUNET	=	A provider of bilateral netting services, managed by International Clearing Systems in connection with Multinet
WGPS	=	Working Group on EU Payment Systems; an EMI working group established in 1994

Bank of Finland publications

Series A (ISSN 1238-1683)

(Nos. 1–35: Publications of the Bank of Finland Institute for Economic Research, "Economic Analyses", a collection of articles from the period 1942–1972, in Finnish and Swedish, ISSN 0081-9476; nos. 36–92: Publications of the Bank of Finland in several languages, ISSN 0355-6034)

A:93 Jarmo Kariluoto **Suomen maksutase. Laadintamenetelmät, tiedonhankinta ja vuosien 1975–92 aikasarjat** (English version – A:98). 1995. 221 p. ISBN 951-686-456-2.

A:94 Juhani Laurila **Finnish-Soviet Clearing Trade and Payment System: History and Lessons**. 1995. 144 p. ISBN 951-686-469-4.

A:95 **Russia's Financial Markets and the Banking Sector in Transtion** (edited by Jouko Rautava). 1996. 201 p. ISBN 951-686-489-9.

A:96 Paavo Peisa (ed.) **Euro, yhteinen raha** (Euro – the Single Currency). 1996. 162 p. ISBN 951-686-499-6.

A:97 Juhani Hirvonen – Matti Virén **Käteisrahan käyttö suomalaisissa yrityksissä** (The Use of Cash in Finnish Business Firms). 1996. 78 p. ISBN 951-686-510-0.

A:98 Jarmo Kariluoto **Finland's Balance of Payments. Compilation methods, sources of information and the time series for 1975 to 1992** (Finnish version – A:93). 1996. 182 p. ISBN 951-686-522-4.

A:99 Markku Malkamäki (ed.) **Suomen rahoitusmarkkinat 1996** (Financial markets in Finland 1996). 1996. 196 p. ISBN 951-686-524-0.

A:100 Harry Leinonen – Veikko Saarinen **Suomalaiset maksujärjestelmäriskit ja niiden sääntely- ja valvontatarpeet** (English version – A:101). 1998. 89 p. ISBN 951-686-565-8.

A:101 Harry Leinonen – Veikko Saarinen **Payment system risks in Finland and the need for regulation and supervision** (Finnish version – A:100). 1998. 89 p. ISBN 951-686-577-1.

ISBN 951-686-577-1
ISSN 1238-1683

Oy Trio-Offset Ab
Helsinki 1998