GROUP OF TEN

ELECTRONIC MONEY

Consumer protection, law enforcement, supervisory and cross border issues

April 1997

Report of the working party on electronic money

This report is available on the world wide web site of the BIS: http://www.bis.org. It can also be obtained from the central banks and finance ministries of the Group of Ten countries and from:

Bank for International Settlements
CH-4002 Basle
Switzerland
Fax: (41-61) 280 9100

International Monetary Fund
66, avenue d'Iéna
F-75116 Paris
Fax: (33-1) 47 23 40 89

ISBN: 92-9131-901-5

Table of contents

I. Introduction

Background to the report

New technologies for making payments, such as multi-purpose prepaid cards and payments via computer networks, could have significant implications for consumers, merchants and financial institutions. In many countries, these products are at a relatively early stage of development, when their benefits, as well as their risks, are yet to be determined. Given the rapid pace of technological innovation, governments and central banks have an interest in anticipating the likely policy implications of these developments. As such, the G-7 Heads of State and Government called for a cooperative study to investigate the implications of recent technological advances that have made possible the creation of sophisticated methods for making retail electronic payments, including means to ensure that their benefits are fully realised.[1]

In response, the G-10 Deputies formed a Working Party in the Autumn of 1996, which was comprised of representatives from finance ministries, central banks and international organisations, and benefited from consultation with law enforcement authorities. The Working Party was asked to examine three broad policy areas: (1) consumer issues; (2) law enforcement issues; and (3) supervisory issues. In this effort, the Working Party reviewed, integrated and built upon the substantial body of existing work completed or underway by other international bodies on the policy implications of electronic money. This work included reports and other research by committees working under the auspices of the G-10 central bank Governors, including the Committee on Payment and Settlement Systems (CPSS); the European Monetary Institute (EMI); the Financial Action Task Force (FATF); the Basle Committee on Banking Supervision; the European Commission (EC); and the Organisation for Economic Cooperation and Development (OECD). The primary objectives of the report are to develop a broader understanding of the policy issues facing governments as a result of the development and use of certain types of innovative retail electronic payment systems, and to identify any issues that could benefit from additional international cooperative efforts. The report focuses on the identification of broad policy objectives among the G-10 countries and the analysis of national approaches taken to date.

---

1 Lyon Summit Economic Communiqué, June 28, 1996.

Other important issues, such as monetary policy and seigniorage implications of electronic money were not addressed by the Working Party, as they have been the subject of extensive analysis elsewhere, in particular under the auspices of the G-10 central bank Governors.

Given its broad representation from authorities within the G-10 countries, the Working Party was able to draw on a wide range of experience in analysing policy issues and assessing how authorities have responded to electronic money developments across the three policy areas.[2] The Working Party also consulted with private sector organisations that are developing or implementing electronic money systems.

The report is structured as follows. The remainder of this introductory section provides background on electronic money and a set of broad policy objectives. Sections II, III, and IV address consumer, law enforcement and supervisory issues, respectively. Each section discusses risks and policy concerns, private-sector measures to address these concerns and potential policy approaches. The experience in the G-10 countries to date is also summarised. Section V highlights cross-border considerations that may arise in the context of electronic money systems. Finally, the report offers conclusions and findings.

Background on electronic money

Payment systems encompass small-value funds transfer systems used by businesses and consumers as well as large-value interbank funds transfer systems that underpin national and international money and capital markets.[3] Payment systems consist of a number of key components, including money, or monetary liabilities, typically issued by monetary authorities or financial institutions, and the vast array of instruments, systems and procedures for recording, communicating and transferring ownership of these liabilities between users. Large-value interbank funds transfer systems in most industrialised countries, as well as a growing number of retail payment systems, use predominantly electronic technologies for these purposes.

New electronic means of retail payment that are currently being tested or implemented in a number of markets include multi-purpose prepaid cards, sometimes called "electronic purses" or "stored-value cards", and prepaid or stored-value payment

---

2 Annex 1 provides a cross-country comparison of regulatory and policy approaches toward electronic money.

3 For a general description of payment systems and their components, see *Payment Systems in the Group of Ten Countries*, Bank for International Settlements, December 1993.

mechanisms for executing payments over open computer networks, such as the Internet. For the purposes of this report, these products are referred to as electronic money. A precise definition of electronic money is difficult to provide; indeed, a number of official bodies have described and categorised these products in different ways.[4] Conventional electronic payment methods, such as large-value interbank funds transfer systems, giro, automated clearing house and direct debit systems, as well as new means of access to credit card payments or home banking systems, are not covered in the analysis of this report. In addition, single-purpose prepaid cards which often use conventional magnetic stripe technologies are quite common in the G-10 countries for services such as telephone calls; these are also not included in the scope of this report.

There is considerable variation in the features of the current range of electronic money products. While definitive classifications may be premature given changing technology, current products can be viewed as hardware or card-based, in which the consumer uses specialised hardware such as a plastic card with a magnetic stripe or computer chip, or software or network-based, in which the product functions via software installed on a standard personal computer connected to a network. The card or personal computer contains electronic records representing the value of an amount of funds which are drawn down when the consumer presents the device at the point of sale or initiates an electronic message from the device to a merchant. Unlike existing forms of payment such as cheques, direct debits, debit cards, or credit cards which allow the holder to access a bank deposit account or a credit line, funds stored on an electronic money device typically represent a general or "pooled" liability of an issuer.[5]

Electronic money products differ in their technical aspects from many conventional forms of payment. At present, there are two basic ways of representing the value of funds stored on an electronic money device: (1) a "balance-based" type in which a single balance is stored and updated with each transaction; and (2) a "note-based" type in which electronic "notes," each with a fixed value and serial number, are

---

4 These include, for example, definitions found in Committee on Payment and Settlement Systems and the Group of Computer Experts, *Security of Electronic Money*, Bank for International Settlements, August 1996; Working Group on EU Payment Systems, *Report to the Council of the European Monetary Institute on Prepaid Cards*, European Monetary Institute, May 1994; Bank for International Settlements, *Implications for Central Banks of the Development of Electronic Money*, October 1996; *Financial Action Task Force, FATF-VIII Money Laundering Typologies Exercise Public Report*, 1997.

5 The term “issuer” is used in this report to indicate the entity or entities in a particular scheme whose liabilities include electronic money balances outstanding and who receive the proceeds from the sale or distribution of electronic money balances. The term “provider” is used to include issuers and any other entities involved in implementing an electronic money scheme.

transferred from one device to another.[6] Cryptography is commonly used to authenticate messages and devices and to protect the integrity and confidentiality of data, instead of the physical security features applied to cash and other paper-based instruments. Digital signatures are one such application of cryptography used as a security measure in some electronic money products. Some electronic money products allow person-to-person payments without the intervention by the issuer or another central clearing system. The experience in this area is very limited, however, due to the fact that this capability is not offered in most electronic money schemes that are currently operational.

General-purpose stored-value cards using "smart card" technology have been introduced in regional pilot tests in all of the G-10 countries.[7] Nationwide implementation is underway in a few countries. Evidence from pilot projects indicates that, to date, such cards are most widely used for small-value purchases, particularly at unattended locations such as vending machines, public transport systems and parking meters, as well as at locations where other forms of electronic payments such as credit or debit cards have not traditionally been accepted. In this respect, stored-value cards have the potential to provide important efficiency benefits by reducing cash handling costs for merchants and improving speed and convenience for consumers in making small-value payments.

Electronic money products that have been developed primarily for use over open computer networks rather than for face-to-face purchases are available in a limited manner in only a small number of G-10 countries. Such systems could provide means of purchasing goods and services via the Internet, particularly for smaller payments where other payment methods such as credit cards might prove to be less cost-effective.[8] In addition, some multi-purpose prepaid cards could have capabilities for payments over computer networks. If "electronic commerce" conducted over computer networks grows, as some observers anticipate, it could also provide impetus for the growth of electronic money. To the extent that these products also serve to make cross-border retail payments more convenient and less expensive, such payments could also increase.

---

6 See *Security of Electronic Money*.

7 A smart card is a card containing a computer chip; smart cards are increasingly used for financial as well as non-financial purposes, such as access to buildings or storage of medical records.

8 Both multi-purpose prepaid cards and software-based electronic money systems could technically be used for larger-value payments as well; in current implementations, payments by consumers are typically limited by the maximum balance allowed on the device, although larger transfers may be necessary between merchants and their banks.

In the future, if electronic money usage reaches a critical mass, it may replace other payment products and become diffused quite rapidly in some countries, but otherwise may never be widely used. The potentially lower transaction costs relative to many paper-based retail payment products and cash handling services could make electronic money instruments more attractive for issuers and potentially for consumers as well. The ease with which the instrument can be used, its perceived security and the general acceptability of electronic money as a medium of payment are other factors that may affect the public's willingness to use it. For merchants and consumers, the amount and nature of fees imposed and the perceived soundness of the product will probably constitute key factors in deciding whether to participate in electronic money schemes.

General policy objectives

To provide a coherent framework for the discussion of issues raised by electronic money across the three policy areas, the Working Party reviewed underlying objectives authorities may have in the banking and financial system. These include:

- Limiting systemic and other risks that could threaten the stability of financial markets or undermine confidence in the payment system;
- Providing consumers with adequate protection from fraud and unfair practices, financial loss, or unnecessary intrusions on personal privacy;
- Encouraging the development of effective, low-risk, low-cost, and convenient payment and financial services for consumers and businesses;
- Ensuring the central bank’s ability to conduct monetary policy;
- Not hindering the ability of law enforcement authorities to prevent and detect movements of funds associated with criminal activity.

Some countries have formulated these objectives in different ways or have additional specific objectives, such as the implementation of fair competitive conditions and the prevention of "regulatory arbitrage". In addition, the Working Party found that governments and central banks of different countries generally agree on broad financial policy objectives, although not all countries may view all of these policy objectives as relevant to electronic money.[9] Moreover, different countries may place differing relative emphasis on specific objectives, and may pursue different approaches in achieving these objectives. Differences in approaches may be based on factors such as

---

9 For example, work conducted under the auspices of the G-10 central bank Governors in 1996 has generally indicated that, unlike large-value payment systems, electronic money is unlikely to raise significant systemic risk concerns in the near term. Moreover, the view of most G-10 central banks at that time was that, under most scenarios for the future growth of electronic money, tools for formulating and implementing monetary policy could be adapted effectively, although future developments could alter this assessment.

statutory mandates or regulatory traditions, features of existing banking and payment systems, or other factors that may influence the expected costs and benefits of particular policy stances across countries.

In addition, the way in which countries balance particular objectives in the case of new electronic money products may depend on the assessment of the likely future development and diffusion of these products, which may affect the potential costs and benefits. For example, in some countries the evolution of electronic money may be viewed as complementing the existing payment system, while in others the possibility for electronic money to replace on a large scale existing forms of retail payment is viewed as less remote. Moreover, the actual and prospective diffusion of electronic money may differ significantly across G-10 countries.

II. Consumer Issues

Introduction

Consumers benefit from the ability to use payment methods that are inexpensive, rapid, convenient, accessible and reliable, with an acceptable level of risk. Governments typically have a general interest in encouraging these qualities in payment systems. In some cases, as noted earlier, authorities may also have specific objectives with respect to protecting consumers and perhaps other users of the payment system such as merchants and smaller financial institutions against financial or other types of risks.

The use of electronic money could influence the level of costs, benefits and risks facing consumers in their day-to-day economic transactions. Potential consumer benefits could include the availability of lower cost, faster and more convenient means of payment, as well as increasing the diversity of payment options available to consumers who have a diversity of preferences and circumstances. This section discusses potential consumer risks in using electronic money and approaches to addressing those risks.

Potential consumer risks posed by electronic money

The magnitude of risks, as well as benefits, to consumers in using electronic money products is uncertain given the lack of large-scale operation of any electronic money schemes. Risks may also vary across products. However, these risks may be viewed as falling into the same general categories as those presented by existing

payment mechanisms. In some cases, electronic money may actually pose lower risks to consumers than some existing forms of payment, for example if issuer guarantees are provided.

First, as is the case when using any payment method, consumers face the risk of financial loss. With conventional payment instruments, common causes of financial loss include theft of currency or fraudulent use of credit cards, cheques or other instruments. In the case of electronic money, financial risks could arise from intentional acts such as theft of the consumer's card or manipulation or interception of electronic messages sent over computer networks. Consumers also risk accidental loss or damage of an electronic money device or operational errors or malfunctions. In some cases, electronic money products could pose different risks from existing forms of payment, such as cash or credit and debit cards, for example, if transaction records are insufficiently detailed to allow prompt resolution of errors or disputes.

Consumers and other users could also suffer financial loss if the issuer of the electronic money became insolvent, bankrupt or otherwise unable to honour payments made with its electronic money liabilities. In such situations users could be left with a claim on the assets of the issuer whose value might depend on various factors, including whether assets are segregated for the benefit of electronic money holders, the quality of those assets and whether any third-party guarantees are available.

Second, as with any payment instrument, consumers face the risk that they may be unable to complete payments in the amount or at the time and location they desire, despite having adequate financial resources to do so. This risk is evident in some existing payment methods in the form of expired or deactivated credit cards, a merchant's inability to make change for currency, or the refusal to accept personal checks. The prepaid nature of electronic money could result in a lower risk of refusal than with cheques or credit cards, for example, but malfunctions of cards or terminals as well as lack of merchant acceptance or interoperability between products could limit the scope of usage.

Third, consumers may face the risk that information generated through their use of electronic money products may be disclosed without their consent, used for fraudulent purposes or otherwise used in a manner adverse to their interests. In many countries electronic payment information is commonly gathered and used for marketing as well as credit evaluation purposes; in addition, it may be used for fraud prevention or made available for law enforcement purposes. Many existing electronic money schemes do not permit anonymous payments. In others, even if the consumer could not be

identified, for example, if the products were sold "anonymously" for cash, it might still be possible to trace the transactions made with a particular card or device.

Private-sector measures to address consumer risks

As with existing payment methods, there are a number of approaches that consumers, merchants and issuers can take to help limit the risks discussed above. These approaches entail costs and benefits for users. At one extreme, consumers may choose not to use electronic money services that present unacceptable levels of risks or for which information on risks is inadequate. Alternatively, consumers can take various risk-reducing measures. For example, consumers can protect themselves against the risk of financial loss in using electronic money by safeguarding their cards or computers on which the electronic money is stored and any access codes or PIN numbers, and by limiting the amount of funds they choose to hold in this form.

The limited experience from electronic money pilot projects to date indicates that consumers tend to hold relatively small amounts, in some cases considerably less than the maximum balance permitted. Consumers also commonly protect themselves against the risk that they will be unable to make payments with a particular instrument by carrying more than one type of instrument with them. In addition, those consumers concerned about unauthorised disclosures about their payments may choose to rely on currency, or may use payment products offered by institutions with publicly disclosed privacy policies.

In order to make informed decisions about the relative risks of different payment methods, consumers require adequate information. At the same time, issuers of electronic money products have incentives to disclose relevant information about the functions and terms of use of electronic money products in order to help consumers use the products and to prevent legal actions in the event that problems arise. For example, in many stored-value card schemes, certain key terms and conditions such as policies on lost or stolen cards and unused balances as well as customer service telephone numbers, are printed on cards or detailed in accompanying literature provided to the consumer. Information about the privacy attributes of a particular product may help consumers choose whether to use a particular electronic money product with its particular privacy implications or another payment instrument.

Providers of electronic money also have incentives to reduce risks that could cause their product to be unacceptable to consumers or to damage their reputation and commercial viability. At the same time electronic money providers will also face commercial pressures to keep system costs down. Most issuers of stored-value cards

have, to date, imposed relatively low maximum balance limits which prevent consumers from taking inordinate risks and reduce incentives for fraud. The development of physical and electronic security features can also help prevent fraud and counterfeiting, as well as improve the reliability of the product. For example, terminals are designed such that cards that have been tampered with are automatically rejected. Issuers can adopt prudent investment and liquidity management techniques and hold assets with relatively low credit and market risk, such as short-term government securities.

In addition, providers of electronic money products may be concerned that problems experienced with other providers could cause consumers to view all electronic money products, or at least those carrying the same brand name, with suspicion. As a result, industry participants may adopt coordinated measures to address some consumer protection concerns. In fact, voluntary industry guidelines and self-regulatory regimes have been a feature of other retail payment methods, such as credit and debit cards, in a number of G-10 countries (see Annex 1). For example, banking industries in Belgium, Canada, Germany, Italy, the Netherlands, Switzerland and the United Kingdom have established voluntary "ombudsman" programs that provide avenues for resolving customer complaints against banks. General banking industry codes of conduct or best practices are utilised in Canada and the United Kingdom. In countries that do not have overarching national privacy protection laws, such as Canada and Japan, some trade associations have voluntarily adopted privacy principles or policies specifying how personal information on customers may be used in financial transactions. In some countries industry groups have established private deposit insurance systems or other guarantee schemes for retail payment networks.

Given that electronic money is still in its nascent or exploratory stage in many G-10 countries, there appear to be few explicit applications of such self-regulatory approaches to electronic money to date, although general provisions of existing codes of practice regarding disclosures and fair practices may apply in a number of cases. In some multi-issuer electronic money schemes voluntary insurance or loss sharing arrangements are anticipated, such that if one institution became insolvent the others would jointly honour electronic money claims issued by that institution. In general, industry structure could play a role in the speed and scope of such cooperative efforts. For example, in countries with a small number of electronic money schemes or providers that have similar interests, agreement on private-sector standards or practices may be more likely. Such agreements may, however, carry risks for the degree of competition in the industry, or may be designed to benefit certain providers at the expense of others.

Potential policy approaches to consumer protection

The Working Party observed that the various risk control measures which can be taken by consumers, industry and governments may be complementary. At a basic level, governments can further their policy objectives in the banking and payment sectors by ensuring that the relevant legal framework provides adequate incentives for fair practices and a strong foundation for reasonable private agreements and contracts. In this respect, electronic money products and their providers are likely to rely heavily on existing laws and industry practices. For example, all G-10 countries have laws applying criminal penalties to fraud and theft of payment instruments. Often, a country's commercial law framework or civil code is designed to encourage fair trade practices and full disclosures of fees and terms for banking services, disallow unreasonable contracts, and provide avenues for legal recourse for the consumer in the event of disputes or negligence.

Governments may also choose to encourage or sanction industry-designed codes of behaviour and self-regulatory measures aimed at ensuring that consumer concerns are adequately addressed; several G-10 governments have done so in the case of banking industry codes of conduct.

In some areas, some governments may determine that such private-sector measures are not sufficient for protecting consumer interests. For example, consumer and provider incentives may be seen not to be sufficient or aligned, or procedures for judicial remedy may be inefficient or costly for resolving consumer problems. For other types of payments, explicit statutory provisions have been enacted in some G-10 countries, as in the case of credit cards in the United Kingdom, credit and debit cards in the United States, and prepaid cards in Japan.

Several G-10 governments are considering whether or not electronic money products are adequately covered by existing laws, or whether specific consumer protection policies should apply to electronic money. Authorities are likely to consider the nature and transparency of risks of electronic money products to consumers; the implications of regulation for supplier costs and consumer acceptance; the likely effects on innovation in the payment system; and the incentives for measures that can be taken by consumers and providers to address given risks without government action. In this regard, adequate information for consumers would help ensure that they are better able to make informed choices among different products and issuers based on the risks and benefits involved.

Policies regarding deposit insurance and the supervision of banking organisations, while not necessarily intended primarily as consumer protection mechanisms, may serve to limit consumer risks in these areas. In two of the G-10 countries (France and Italy), deposit insurance will most likely apply to multi-purpose prepaid cards. In Switzerland, banks participating in a prepaid card arrangement assume full liability for the debts of the "pool" jointly and severally; a similar loss-sharing arrangement is being developed by banks in the Netherlands. In the United States, it has been determined that most stored-value card funds issued by insured depository institutions are generally not deposits under U.S. deposit insurance laws and are therefore not covered by federal deposit insurance. Other G-10 countries are reviewing the question of whether deposit insurance will apply to electronic money. Existing legal definitions of a "deposit," which vary across the G-10 countries, as well as the interpretation of such definitions in light of the policy stance toward the introduction of electronic money, would appear to play an important role in these and other policy determinations. In addition, some countries may view government deposit insurance as less comprehensive and less timely than private-sector measures, such as issuer loss-sharing arrangements.

In addition, some authorities may view restricting electronic money activity to supervised banking organisations as a means of addressing indirectly a broad range of consumer risks, including issuer insolvency and fair customer practices. These issues are addressed further in section IV.

In most of the G-10 countries, general laws on privacy are applicable to banks and other financial institutions. These laws generally require that such institutions preserve the confidentiality of customer information. For other countries, including Canada and Japan, governments or industry groups are considering whether additional privacy protections, beyond those in existing laws and civil codes, are needed. The European privacy directive is expected to apply to electronic money products and their providers in the same manner as for other payment systems, or at least where the scheme permits the storage of information about an individual.[10]

---

[10] EC Directive 95/46/EEC on the Protection of Personal Data. Member States must incorporate the Directive into their national laws by October, 1998. Pursuant to the Directive, personal data may be processed only if at least one of six criteria are satisfied, one of which is that the data subject gives his prior consent. The Directive lays down common rules to be observed by those who collect, hold, or transmit personal data. However, the Directive is not applicable to national legislation aimed at preventing, investigating and prosecuting criminal activity affecting the payment system.

Overall, the Working Party's review of current consumer protection policy stances among the G-10 countries yields two main observations. First, most countries are currently relying on existing laws and regulations in addressing risks such as loss, fraud, insolvency, and privacy concerns, rather than enacting comprehensive new measures specifically aimed at electronic money products. Second, government policies toward consumer protection issues as they relate to electronic money are evolving in each of the G-10 countries. This process can be expected to continue as market developments unfold and more experience is gained with potential policy concerns and corresponding private market initiatives.

III. Law Enforcement

Introduction

As new retail electronic means of payment, such as electronic money, have been developed, law enforcement agencies of the G-10 countries have considered possible approaches to further law enforcement policy objectives with respect to preventing, investigating, and prosecuting criminal activity affecting the payment system. This section summarises some of the potential features of electronic money products that could pose new challenges or heighten existing risks to law enforcement efforts, as well as possible policy approaches that may be taken in this area. It should also be noted that electronic money may have the potential to bring benefits to law enforcement efforts, such as reduced usage and theft of cash and greater electronic record-keeping capabilities, compared with some existing means of payment.

Potential criminal offences involving electronic money

Two general types of criminal offences associated with payment systems can be identified. First, payment systems may be exploited in connection with criminal activities, such as money laundering, tax evasion, or illegal gambling. Although to date, G-10 countries have not seen evidence of this type of activity in connection with electronic money products, if such products come to be used on a large scale, it is conceivable the criminals may seek to explore their potential for transferring illicit funds.

The second type of criminal offence is attacks on electronic money products themselves, i.e., counterfeiting, fraud, or disruption of the system. Fraud and counterfeiting are unfortunately common aspects of existing payment mechanisms. For

example, credit cards are subject to fraud and counterfeiting losses that are estimated to be well over US$1 billion each year. Such losses may ultimately be passed through to consumers and merchants, and investigating and prosecuting these crimes absorb considerable resources of law enforcement authorities. It can be expected that electronic money products will also be subject to such attacks, although to date, no criminal attacks on multi-purpose prepaid cards have been reported.[11] Further, a report prepared by staff of the G-10 central banks concluded that electronic money products, particularly those implemented with hardware-based security (e.g. using a smart card) can be designed with an adequate level of security relative to other forms of retail payment.[12]

Characteristics of electronic money affecting potential usage for criminal activities

Specific characteristics of payment instruments influence their attractiveness for illicit activities. For example, paper currency is commonly used for such activities because it virtually guarantees the anonymity of payers and payees and is widely available and accepted; however, its physical bulk makes it difficult to conceal when large sums are transported. Traditional electronic payments, such as wire transfers, avoid the latter problem but may be less attractive for criminals, as they typically generate some degree of transaction records. Attacks on payment instruments may be expected to be more likely the larger the values involved relative to the costs of fraudulently reproducing or tampering with the product.

Many current electronic money products do not appear to be attractive for transferring illicit funds or as targets of large-scale fraud or counterfeiting because they are currently focused on low-value, consumer transactions. However, certain characteristics could increase or decrease their attractiveness for money laundering or other criminal activities. Stored-value cards could provide a less bulky and conspicuous means of transporting or transferring funds relative to currency, depending on the value limits on the cards as well as the ease of concealing card balances. Most stored-value-card and electronic-purse pilot projects have established limits for consumer cards ranging up to the equivalent of US$1,000, or in Europe, 100 ECU, although the technology exists to transact in much greater amounts. In the case of stored-value products designed for open computer networks, it is not yet clear whether value limits

---

11 Instances of counterfeiting or fraudulent modification of certain single-purpose payment or access cards, such as those for telephones or pay-television, have been reported in some countries; electronic money products typically use more sophisticated security measures than these products.

12 *Security of Electronic Money*.

for consumer devices or for transfers will be implemented. Although they may not prevent criminal use altogether, lower value limits can be expected to raise the costs and reduce the speed for those attempting to launder funds. Merchant terminals may necessarily have much higher limits to accommodate a reasonable volume of transactions, and thus may be a more likely avenue for criminal usage.

Some stored-value cards and electronic money products for use via personal computers could be used to transfer funds over telephone or computer networks, such as the Internet. Such products could eliminate the need to transport bulky payment instruments over long distances. Of course, the obstacle of moving the illicit funds from currency or other accounts into and out of the stored-value product without detection would remain.

Electronic money providers have developed a range of security measures to help combat fraud and counterfeiting risks. Many of these security features may also serve to deter the use electronic money for criminal activities. These measures include the use of tamper-resistant smart cards or other devices, cryptographic protocols, on-line authorisation of some or all transactions, administrative controls on transactions and participants, record-keeping systems, expiration dates and value limits. The effectiveness of such measures has yet to be demonstrated in large-scale usage of the products. The encryption of transactions could be an effective tool for enhancing security, but also has the potential to make some electronic money products more attractive for criminal use if they permit large, anonymous transfers.

Many of the electronic money schemes currently being implemented restrict transactions to those between consumers and merchants or financial institutions. A few schemes, however, may permit the direct transfer of value between individuals without centralised clearing or intervention by a financial institution or central system (sometimes called "purse-to-purse" transfers). Depending on the system design and any associated records that are generated, such transfers between individuals could increase the attractiveness for money laundering by reducing the scope for monitoring and detection by others. However, most electronic money products have been designed with expiration dates or other limits intended to compel regular interaction with an issuer or central system operator. In the case of software-based electronic money products, real-time authorisation of transactions by a central system is a common security feature, as these products cannot rely on specialised tamper-resistant hardware, such as a smart card. As data processing and communications costs continue to decline, such added security measures could become more cost-effective for a broader range of products.

The degree and type of transaction record-keeping, which varies across electronic money products, is particularly relevant to the attractiveness of a particular payment method for criminal use as well as its vulnerability to attack. Many electronic money schemes would retain detailed records in a centralised database, which would be available for fraud control and other purposes, while others would not gather complete records. Some issuers anticipate offering stored-value cards through vending machines, in which case the transactions of a particular card might be tracked but the identity of the user would not. Others contemplate requiring that an account be opened in the name of a specific user in order to perform transactions.

As electronic money products are introduced more widely, their providers are likely to attempt to balance the costs of implementing security features against the likely losses due to fraud and counterfeiting. For example, while cost-reduction incentives, as well as consumer privacy concerns, could induce product developers and operators to implement systems with limited record-keeping or centralised monitoring, anti-fraud considerations may provide incentives for greater systems controls. Consumers might choose to use systems with full record-keeping to assist in budgeting and resolution of errors, rather than those that provide greater anonymity and potentially greater risks in the event of an operational failure or lost card. In the near term, as long as the volume of transactions is relatively low, irregularities in payment activity due to criminal usage are likely to be more easily detected than would be the case with relatively higher volumes. More generally, in order to be useful for criminal purposes, a payment mechanism must be widely available and accepted, as well as more cost effective and convenient and less subject to scrutiny than other alternatives.

Regulatory and enforcement regimes

To prevent and detect illegal movements of funds, law enforcement and regulatory officials have historically relied upon the intermediation of banks and other types of financial institutions where records of both transactions and customer identities are typically maintained. Traditional techniques used throughout the G-10 countries for preventing and detecting financial crime rely to a great extent on customer identification, reporting of suspicious transactions and large currency transactions to authorities, as well as the creation and maintenance of records of certain transactions. Many countries also have laws prohibiting counterfeiting and fraud involving bank notes as well as other payment instruments; supervisory policies in these areas are discussed further in section IV. The remainder of this section primarily addresses policy responses to potential criminal use of electronic money systems.

In 1990, the FATF issued "Forty Recommendations", which set out the basic framework for anti-money laundering efforts and which were designed to be of universal application.[13] In June 1996, the Forty Recommendations were revised to take into account the experience gained over the previous six years and to reflect changes that have occurred in money laundering activities. In this context, a specific recommendation dealing with new technological developments was adopted.[14]

At the end of 1996, the FATF held discussions among law enforcement and regulatory experts from its members, electronic money providers, and a number of banking groups to discuss means of preventing new technologies in the payment system from being used by money launderers. As a result of these discussions, the FATF concluded that law enforcement authorities and regulators must anticipate and identify potential new issues and challenges. The FATF concluded that important features of electronic money technologies, which may affect the degree to which they can be used by criminals, include value limits, transferability between individuals, record-keeping, and the potentially changing role of intermediaries. Through cooperation with industry, the FATF intends to continue to study this issue as payment systems develop, and to work to develop effective anti-money laundering measures before problems arise.

Staffs of the G-10 central banks also prepared a preliminary analysis of the implications of electronic money for money laundering under the auspices of the CPSS. This report outlined potential characteristics of electronic money products that could make them more vulnerable to money laundering, as well as some potential policy responses.

Other authorities have been examining the implications of emerging payment methods for other types of financial crimes. In particular, the OECD is undertaking a project to assess tax evasion issues in electronic commerce and the implications of the development of electronic money for the relevance of existing tax principles (e.g., traditional source, residency and permanent establishment concepts) and for tax administration.

---

13 The Financial Action Task Force on Money Laundering (FATF) is an inter-governmental body created by the G-7 countries in 1989, whose purpose is the development and promotion of policies to combat money laundering--the processing of criminal proceeds in order to disguise their illegal origin. These policies aim to prevent such proceeds from being utilised in future criminal activities and from affecting legitimate economic activities. The FATF currently consists of 26 governments and two regional organisations.

14 Recommendation 13 states: “Countries should pay special attention to money laundering threats inherent in new or developing technologies that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes.”

Many G-10 countries are currently considering whether or not to apply existing anti-money laundering laws, such as transaction reporting, customer identification, and record-keeping, to some or all electronic money products. In this respect, governments must consider the potential impact on innovation and costs to providers, as well as consumer concerns, such as privacy. A requirement to record or report every electronic money transaction would generate substantial volumes of data of dubious commercial or law enforcement value and would impose costs on electronic money products that do not currently apply to other payment instruments, such as currency.[15] At the same time, however, there may be records that electronic money scheme operators keep for their own business purposes, as well as to protect against fraud, which could be employed to combat financial crime; even so, privacy considerations of consumers would need to be taken into account. Although record-keeping and privacy appear to pose a trade-off, technology might improve the terms of this trade-off.[16]

Law enforcement authorities may also need to consider some potentially new challenges posed by technological innovation and other changes in the payment system more generally. For example, electronic money products in some countries may be offered by entities other than institutions subject to banking supervision, although many countries apply anti-money laundering laws to all institutions. Another example is newer encryption techniques, such as those used in some electronic money products, which could make it more difficult for law enforcement authorities to gather information necessary to detect and prosecute criminal activity. Several G-10 countries are considering appropriate policies in this area, which could have implications for the design and use of electronic money products as well as for consumer privacy concerns. Law enforcement authorities may also need to consider new techniques, including the use of new technologies, in carrying out their objectives. In addition, authorities may find it necessary to ensure that laws against counterfeiting and fraud involving payment instruments remain adequate in light of new technological developments.

In summary, emerging electronic money products are currently focused on low-value, consumer transactions which may present less of a concern to law enforcement

---

15 In the case of currency, law enforcement authorities have generally established a threshold of the equivalent of about US$10,000 for triggering certain activity and reporting procedures designed to deter and detect money laundering. Some countries also have established record-keeping rules for large-value payment systems; few apply such rules to retail payment systems.

16 For example, records could afford privacy protections ranging from no anonymity (full records of each consumer's transactions) to full anonymity. An intermediate level of privacy would result in systems where codes or serial numbers are used in transactions, and consumers' identities could be found only by cross-reference, and potentially only in certain law enforcement situations.

authorities because they are less likely to attract the attention of criminals. In many cases, market incentives and supervisory arrangements exist that are complementary to the interests of law enforcement authorities. Over the longer term, it is too early to determine whether market pressures will cause products to evolve in such a manner as to become more or less attractive for money laundering, tax evasion, and other financial crimes or more vulnerable to fraud and counterfeiting.

A survey of policies across G-10 countries indicates that, at this stage, G-10 countries have generally not seen the need to develop new anti-crime laws or regulations specifically pertaining to electronic money. Nevertheless, because of the potential for money laundering and other criminal activities, and because of rapidly changing technologies and commercial environments, law enforcement authorities will need to continue to monitor the development of electronic money products. Continuing dialogue and cooperation with developers and providers of electronic money products may also help to detect and address potential law enforcement problems at an early stage.

IV. Supervisory Issues

Introduction

Electronic money products present new opportunities. They may also raise some new challenges to supervisors of financial institutions that participate in providing retail electronic money services. This section discusses the basic types of risks for institutions that choose to provide electronic money products, particularly as issuers, measures that institutions may take to address these risks, and policy approaches toward the supervision of institutions participating in electronic money schemes.

Risks to providers of electronic money

Issuance of electronic money implies the creation of liabilities on the balance sheet of the issuer that are generally payable (or redeemable) at face value to those entities accepting electronic money as payment. This entails both operational and liquidity risks for the issuer. Issuers could also face credit and market risks in their assets, depending on their policies for investing the proceeds from electronic money issuance. Other financial risks related to electronic money issuance could include those arising from participation in loss-sharing or guarantee arrangements between issuers

that are planned for some systems (as noted in section II), as well as potential clearing and settlement and foreign exchange risks, in some schemes.

New forms of operational risks could also arise for institutions acting as issuers or playing an operational role for electronic money products. Although many electronic money products are based on existing banking technologies, including encryption of messages and electronic authorisation of payments, they may also involve newer techniques, such as smart cards and transmission of data over open computer networks. Issuers may bear risks of fraud or operational failure or of redeeming counterfeit electronic money accepted by merchants or consumers for which no corresponding payment has been received. Issuers will also need to address a range of traditional risks, including strategic and reputational risks, compliance risks, and risks associated with outsourcing of operations.

For a general-purpose banking organisation in which electronic money activities make up a small part of its overall business, financial risks arising from electronic money issuance may not generate significant new liquidity needs or credit or market risks, and may therefore not raise new financial risk management considerations. Developments in many G-10 countries indicate that a special-purpose organisation, in many cases licensed as a bank or owned by a group of banks, is a potentially common vehicle for issuance of electronic money. A special-purpose entity established solely to issue electronic money would also face credit, market, operational, and liquidity risks. However, the nature and magnitude of risks may be somewhat different than those inherent in the range of traditional banking activities. On the one hand, such an entity could be more sensitive to sudden liquidity changes, but on the other hand, it may be able to limit its credit and market risks significantly relative to a general-purpose banking institution.

Private-sector measures to address risks

Issuers and other providers of electronic money products whose capital is at risk in electronic money schemes have strong incentives to protect themselves against financial as well as operational risks. The need to retain market reputation and attract new capital will provide significant motivation for issuers to develop effective financial risk management practices, including incentives to maintain sufficient liquid assets on hand to meet demands for redemption of electronic money. Such practices could include investing the proceeds from issuance in high-quality, short-term, liquid securities, although issuers may also have conflicting pressures to increase asset returns by investing in higher risk assets.

Other measures that can be taken by providers include establishing strong internal controls to prevent employee fraud, instituting risk management procedures for new products, as well as designing robust security measures and procedures to defend against external fraud and counterfeiting attacks. A recent report by a G-10 central bank committee indicated that developers of electronic money products are implementing a range of security measures.[17] The report concluded that a combination of security measures for an electronic money product, rather than any single measure or standard, should be most effective. Electronic money schemes may also develop risk-management measures to protect against settlement and operational risks, as is common in existing retail payment networks.

Potential supervisory approaches

Each G-10 country is seeking to determine the appropriate nature and scope of official oversight or supervision of electronic money issuance. In making this determination, the authorities are considering the degree to which market incentives can be used to achieve public policy objectives. Properly functioning market incentives and controls can help to provide a solid foundation for the operation and further development of electronic money schemes. At the same time, consumers, merchants and other entities may not always be able or willing to assess adequately all the risks related to the issuance and use of electronic money.

A number of considerations affect the policy choices made by different countries with respect to their approach to the oversight of electronic money. Government supervision may help to enhance the confidence of consumers in electronic money schemes. At the same time in some countries it may lead to the expectation of official support in the event of difficulties. Licensing requirements or similar arrangements may help to promote fair competition among authorised issuers but they may also in some countries constitute barriers to entry, which could lead to a reduction in competition by excluding some potential suppliers. Some countries may view the issuance of electronic money as analogous to deposit taking, an activity for which established supervisory frameworks exist. Others may view it in a different light, and adopt a different approach.

In this respect, the Working Party considered whether electronic money could raise systemic risk concerns. The general sense of the Working Party was that in the short term, there is no prospect of electronic money giving rise to systemic risk.

---

17 See *Security of Electronic Money*.

Existing schemes are too small, both in terms of the total amounts outstanding, and the amounts held by individual users, for a failure to have contagion effects. Over the longer term, if electronic money does grow to displace currency to a substantial degree, loss of confidence in a scheme could conceivably have broader consequences for the financial system and the economy. At this point, this is a remote possibility, but one which nevertheless warrants continued monitoring and assessment of developments.

An analysis of regulatory structures for potential providers of electronic money prepared under the auspices of the G-10 central bank Governors in 1996 revealed differences and evolving perspectives across countries with respect to the supervision of issuers. In addition, in 1994, the EMI published an influential report on prepaid cards, which analysed the development and implications of electronic purses for central banks.[18] The report concluded that the balances on multi-purpose prepaid cards represent funding that is equivalent, in economic terms, to deposit-taking for the issuer. As a result, to help ensure the soundness of the issuer, the report recommended that only credit institutions should be allowed to issue electronic purses.[19] A number of countries have adopted this recommendation. For those countries that determine that issuance of electronic money is analogous to deposit-taking, application of some or all of the banking regulatory regime may be considered appropriate.

Other countries have not made any changes to laws or policies to date. Some authorities are currently considering whether issuance of electronic money should be regulated in the same manner as deposit-taking under their laws, or whether other regulations should apply. Authorities in some countries may view such determinations as premature, or may choose to rely more on market incentives and self-regulatory approaches for providers to manage their financial and operational risks.

Different approaches across countries can be explained by a number of factors, including existing market and regulatory structures. For example, in countries in which banking and commerce have traditionally been separated by law, government restrictions on issuance of electronic money to credit institutions may be viewed as limiting the degree of potential participation by other entities, such as those in the

---

[18] Working Group on EU Payment Systems, *Report to the Council of the European Monetary Institute on Prepaid Cards*, European Monetary Institute (May 1994).

[19] The report noted, however, that some issuers may not have to be full credit institutions provided that (1) they provide only domestic payment services; (2) they are subject to appropriate regulations, in particular, with respect to liquidity requirements; and (3) they are supervised by the institution which supervises credit institutions. The report also did not include in its recommendations "limited-purpose" prepaid cards, namely those which can be used only at a small number of points of sale within a certain geographic area.

technology industry. Likewise, the existing financial industry structure may also play an important role. In countries in which credit institutions are the primary providers of payment services and financial intermediation functions for the economy, they may reasonably be expected to play an important role in the provision of electronic money as well. Where such functions have traditionally been performed by a range of different entities, such as securities firms, specialised lending companies, and non-bank payment providers, as well as credit institutions, it may be expected that new services, such as electronic money, would be provided by a diverse range of entities as well.[20]

Furthermore, authorities in some countries emphasise a cautious attitude toward regulation in order to avoid imposing regulatory costs that later turn out to be unnecessary, while others may be concerned that regulatory restrictions applied retroactively could create added costs for providers which could have been avoided if requirements were known in advance. The supervisory framework may also be relevant for achieving law enforcement or consumer protection objectives. For example in countries with consumer protection and anti-money laundering regimes that apply broadly across different types of institutions, authorities may see less need to address these issues primarily through the generalised supervision of issuers.

In the case of credit institutions that act as issuers or participate in other roles in electronic money schemes, supervisors in many G-10 countries expect to rely primarily on aspects of the existing supervisory framework, for example, those regarding liquidity and operational risks as well as requirements for internal controls and the fitness and properness of management.[21] As illustrated in Annex 1, there are a range of approaches for implementing such requirements. Some countries are developing more targeted procedures to assess electronic money products in some areas.

For special-purpose issuers of electronic money, authorities in some countries may determine that some other type of prudential requirements are warranted, rather than the general range of measures applicable to standard banking organisations. Solvency requirements, liquidity guidelines and other types of prudential rules developed for traditional banking organisations may not be especially relevant or

---

[20] For example, in the United States, non-banks issue other types of payment and monetary liabilities, such as travellers checks, money orders, and money market mutual funds, although it is not yet known whether any of these entities will also issue electronic money. Non-bank issuers of travellers checks and money orders have traditionally been subject to prudential regulation at the state level; it is not yet clear whether or not such rules may extend to electronic money issuance.

[21] For example, credit or deposit-taking institutions are subject to the Basle Capital Accord, which sets minimum amounts of capital to be held against risk-weighted assets.

appropriate. For example, to ensure that issuers are able to meet the large payment outflows that could occur from time to time as the result of the varying pattern of transactions, their investments could be limited to high-quality, short-term assets that could be liquidated in the financial market at short notice. Given the simplicity of the issuer's balance sheet, however, there might be less need for complex and intensive supervisory examinations. Indeed, some countries are considering whether exemptions from certain aspects of credit institution supervision and regulation would be appropriate for specialised issuers of electronic money that do not engage in other banking functions.[22]

Supervisors may be concerned that some institutions may not have the technical capability to assess security features of electronic money products to ensure that the risk of fraud and counterfeiting can be adequately managed. The focus among international banking supervisory efforts has been on strengthening institutions' risk management capabilities and internal controls, rather than on conducting detailed evaluation of their activities and operations. In particular, it may be costly and impractical for banking supervisors to assemble and maintain the necessary technical expertise to assess the security aspects of a range of electronic money products. A number of G-10 central banks have addressed this issue at the level of the overall scheme, and have conducted security reviews or requested system developers to commission external security audits of electronic money schemes in their countries.[23]

A few general points can be made about the approaches toward supervisory issues taken in the G-10 countries to date. (Section V discusses international supervisory approaches.) First, for credit institutions, authorities in some countries view existing supervisory procedures as sufficient, while other countries are considering some modifications to existing procedures. Second, special-purpose issuers, often owned by credit institutions, could become an important vehicle for some electronic money schemes, and further analysis of their risks may be appropriate once additional experience is gained. Third, policy stances toward the supervision of potential electronic money issuers, particularly those that are not credit institutions, currently

---

22 For example, in Germany, authorities are considering whether modifications of existing banking supervisory rules and exemptions from certain aspects of credit institutions supervision would be appropriate for some specialised issuers of prepaid cards. The Federal Banking Supervisory Office could grant exemptions from the full set of banking supervisory requirements (e.g., licensing requirements, provisions on solvency and liquidity) if an issuer does not pose a threat to the payment system in view of the limited use and dissemination of the cards issued.

23 The 1994 EMI report on prepaid cards recommended that central banks examine carefully the security features of prepaid card schemes, with a view toward promoting the soundness of the instrument.

vary across the G-10 countries, although in practice to date, most issuers are credit institutions or their affiliates.

V. Cross-border Issues

One of the primary goals of the Working Party was to identify issues raised by the development and use of electronic money that could benefit most from discussion in an international forum. In this context, the Working Party considered whether the potential international operation of electronic money schemes raises additional concerns for the effective implementation and enforcement of the consumer, law enforcement, or supervisory objectives of individual countries. A second question, perhaps more difficult to assess, is the potential effect on the development of emerging electronic money products of differences in laws or policy approaches across countries in these areas.

The Working Party was not aware of any major electronic money schemes that have implemented multi-currency features or permitted cross-border use by consumers at this stage. However, several prominent electronic money projects have established an international ownership structure and anticipate cross-border usage by consumers in different countries. Multi-currency functions of stored-value cards could be useful for foreign travel, for example, and some electronic money products could potentially be used for remote purchases of goods and services from other countries, such as over the Internet. In the member states of the European Union, electronic purses could facilitate the use of the Euro, especially prior to the introduction of Euro-denominated bank notes and coins, which could, in turn, promote usage of electronic money.

Potential cross-border concerns

Two basic scenarios for cross-border usage of electronic money can be envisioned. (Either scenario could involve issuance of electronic money in foreign currencies.) First, consumers could use prepaid cards issued by domestic institutions to make payments to foreign-based merchants, for example, while travelling, or in making purchases over a computer network. In this case, the consumer and the issuer may be located in one country, while the merchant (and potentially the merchant's financial institution) is located in another. Although consumers may have different legal rights if transactions occur in different jurisdictions, these aspects also arise for other cross-border payment methods, such as credit cards and travellers cheques.

Second, an issuer in one country could issue electronic money to consumers in another country, potentially in the consumer's home currency, for use at either domestic or foreign merchants. The second scenario could raise more difficult issues, although the Working Party recognised that cross-border banking activities, such as cross-border deposits, have existed for many years. Like these traditional activities, cross-border issuance of electronic money could limit the reach of national laws and regulations, particularly in the consumer area, or create jurisdictional ambiguities. As a result, some countries may be concerned that issuers of electronic money have incentives to incorporate or establish facilities in countries with the least stringent regulatory requirements, giving rise to "regulatory arbitrage".

For card-based electronic money products, the feasibility of an issuer implementing a system from completely outside a country seems impractical, given the physical presence and infrastructure needed to distribute and maintain cards and terminals and gain acceptance by consumers and merchants.[24] In contrast, some electronic money products for use over open computer networks would not require specialised hardware for the consumer or merchant or a physical presence. In either case, however, offshore issuers might have a commercial disadvantage with respect to established, reputable institutions that are familiar to residents and that have direct access to that country’s interbank payment clearing and settlement systems.

It is also possible that cross-country policy differences might have adverse effects on the development of electronic money. The Working Party's analysis indicates that even though authorities in the G-10 countries may share a number of important policy objectives, the means of reaching them may differ considerably across countries. Given the uncertainties about regulatory approaches as well as market developments, it is difficult to determine whether these differences will hinder the development of electronic money. Uncertainty about jurisdiction for or application of consumer protection regulations or enforceability of contracts for electronic money products could discourage cross-border usage. Incompatible laws across countries might potentially hamper or preclude cross-border operation of electronic money schemes in some instances, for example, if they prohibit the transmission of personal data across borders.

The extent to which electronic money schemes can operate in multiple jurisdictions may increase their attractiveness as a tool to facilitate crime if they can be

---

[24] Even the more practical alternative of establishing an agreement with a local firm may involve additional costs and provide an avenue for potential exercise of regulatory jurisdiction.

used to make large payments anonymously to individuals in other jurisdictions. Anti-money laundering provisions are fairly consistent across the G-10 countries. Nevertheless, jurisdictional ambiguities may arise, as in other contexts, with respect to the authority for investigating or prosecuting particular criminal activities.

Policy approaches to addressing cross-border concerns

A number of the issues discussed above are already under active discussion by existing international groups. The recent tendency has been toward the establishment of international cooperative channels to provide a basis for assessing the severity of cross-border concerns and addressing specific problems. The CPSS, for example, has conducted a range of research, information sharing, and in some cases policy coordination, relating to retail and wholesale payment system issues and has been directed by the G-10 central bank Governors to monitor electronic money developments on an ongoing basis.

In the area of consumer policies, there has not historically been an emphasis on extensive international cooperation, despite the fact that many existing retail payment instruments, including travellers cheques, credit cards, and ATM cards, are commonly used by consumers outside the country of issue. More generally, cross-border usage of electronic money may highlight well known legal and jurisdictional issues that are not unique to electronic money. Additional international discussions on broader consumer policy issues and their interaction with technological innovation may, therefore, become appropriate.[25] Discussion of technical security measures for electronic money systems among authorities and the private sector providers might also be useful for nurturing a common understanding of such aspects among industry and supervisory authorities.

As discussed in Section III, the FATF provides a well established forum for international cooperation in addressing money laundering. Law enforcement, banking supervisors and other authorities have a strong interest in the continued exchange of information about any criminal activity involving electronic money products and in a cooperative approach toward monitoring the development of such systems, both within and outside the G-10 countries.

Many of the proposed issuers of electronic money schemes in the G-10 countries to date are banking organisations or are owned primarily by banking

---

[25] For example, an OECD committee is currently examining international differences in consumer redress for disputes or “charge backs” in remote purchases made with credit cards.

organisations. In light of this, the Basle Committee on Banking Supervision has also undertaken a review of supervisory issues stemming from electronic money and banking, including cross-border issues. Coordination among supervisors of credit institutions involved in cross-border electronic money schemes is likely to occur within existing international bodies. The G-10 Concordat on banking supervision, which embodies cooperative principles, such as consolidated supervision, division of responsibilities between home and host country supervisors, and exchange of information between supervisors, may be a useful framework for credit institutions that issue electronic money. Banking supervisors are currently examining to what extent these approaches may be useful for electronic money providers under their supervision. Furthermore, it may be appropriate for supervisors to share information on electronic money schemes with international ownership and operation to understand fully any cross-border liability issues that may affect institutions in particular countries.

VI. Summary and Conclusions

In June 1996, the G-7 Heads of State called for a cooperative study to investigate the implications of recent technological advances that make possible the creation of sophisticated methods for making retail electronic payments. Consistent with this objective, the Working Party was asked to produce a report that developed a broader understanding of the policy issues facing governments as a result of electronic money and to identify any issues that could benefit from additional international cooperation. Building on the extensive body of previous analysis and work on this subject, the Working Party concentrated on three broad policy areas: consumer issues, law enforcement issues, and supervisory issues. The Working Party also met with a broad cross-section of firms and organisations associated with electronic money in many of the G-10 countries.

The various electronic money products are still at a relatively early stage in their development. Providers of products in various pilot projects and early nation-wide implementations indicate that the potential exists for stored-value cards and their network equivalents to provide important efficiency benefits by reducing cash handling costs and improving speed and convenience for consumers in making small-value payments. It is still, unclear, however, how quickly these products will spread in the G-10 countries.

On consumer issues, overall, the Working Party's review of current consumer protection stances within the G-10 yielded two main observations: 1) most countries are

relying on existing laws and regulations in addressing risks such as loss, fraud, insolvency, and privacy concerns rather than enacting comprehensive new measures specifically aimed at electronic money; and 2) government policies on consumer protection and electronic money are still evolving as this technology continues to develop.

Regarding law enforcement issues, emerging electronic money systems are currently focused on low-value consumer transactions, which may present less of a concern to law enforcement authorities. It is too early to determine whether or not over the longer term these products will evolve in such a way as to become more or less attractive for money laundering, tax evasion, and other financial crimes or more vulnerable to fraud and counterfeiting. To date, G-10 countries have generally not seen the need to develop new anti-crime laws specifically directed at electronic money. Continued monitoring, as well as dialogue and cooperation with developers of electronic money, will be required.

On supervisory issues, the Working Party noted that G-10 countries had adopted a wide variety of responses to the supervision and regulation of electronic money products. To the extent traditional banks and other regulated financial institutions are playing the key roles in the issuance of electronic money, existing supervisory and regulatory approaches are being adapted as appropriate. In order to accommodate non-traditional issuers, some countries are considering a more specialised supervisory framework specifically for electronic money issuers. Some view the market as providing strong incentives for electronic money issuers to protect themselves against operational and financial risks. Market incentives are seen as being useful in encouraging providers to address consumer protection and law enforcement issues as well.

The Working Party's discussions of consumer, law enforcement, and supervisory issues suggested several key considerations to which consumers, providers, and authorities may wish to give attention in the implementation and use of electronic money products as well as in the development of national policies. The formulation of these considerations is meant to highlight potentially important aspects without implying any particular policy approach.

Key considerations:

Transparency: Potential users can best make informed choices about the relative merits of electronic money products if their features, costs, and risks are sufficiently transparent. Useful disclosures for consumers could include

information about significant user rights, relevant information on the issuer and its obligations towards consumers, applicability of any deposit insurance or other guarantees, and intentions regarding any use of personal data.

Financial integrity: The financial integrity of any electronic money issuer rests importantly on adequate liquidity, capital, and internal controls. Liquidity should be adequate to ensure that issuers can meet demands for funds; investment policies should be appropriate to ensure the solvency of the electronic money scheme; management should establish risk management policies and procedures and internal controls consistent with protecting the financial integrity of the scheme.

Technical security: Technical security measures have important implications for the financial and operational reliability of an electronic money scheme. These measures should be assessed comprehensively with the aim of protecting against fraud or counterfeiting attacks that could threaten the overall integrity of the electronic money scheme.

Vulnerability to criminal activity: The design of electronic money schemes can affect importantly the risks of criminal usage of and attacks on electronic money. As a result, realistic evaluation should be conducted of the vulnerabilities of particular products to these risks.

On cross-border issues, given the early stage of commercial development, the Working Party saw virtue in adopting a flexible response to electronic money issues. The Working Party recognised that innovation and competition in the payment system can provide important efficiency and consumer benefits. For example, some electronic money schemes may facilitate cross-border retail payments. Given that a range of national policy approaches have emerged across G-10 countries, authorities may need to consider how best to design, develop and apply national policies so as to minimise any impediments to the cross-border use of, or competition in the provision of, electronic money.

Efforts in this area of such groups as the CPSS, the BIS, the Basle Committee on Banking Supervision, the FATF, the OECD, the EC, and the EMI are likely to be beneficial. In the Working Party's view, while additional discussions may become appropriate in certain areas, it is not necessary at this time to establish new formal international coordinating mechanisms specifically addressing electronic money developments. The Working Party has provided a useful forum for bringing together the perspectives of central banks, finance ministries and law enforcement authorities

and has promoted constructive international dialogue on potential policy implications. As more experience with electronic money is gained, governments may wish to take a similar approach to reviewing electronic money developments in the future if circumstances warrant.

ANNEX 1

Survey of Policies Toward Electronic Money in the G-10 Countries

Country	Fraud, loss, theft, disputes	Disclosure requirements
Belgium	General applicability of civil code and rules for credit institutions. Voluntary banking association ombudsman program for settling disputes may be applicable to electronic money.	General applicability of civil code and rules for credit institutions.
Canada	General applicability of civil code and rules for credit institutions. Banking industry ombudsman. Industry association developing standards on security against fraud and theft for electronic money for stored-value cards.	Disclosures required for all service charges related to bank and trust and loan company accounts, including charges for electronic funds transfers from deposit accounts. Disclosure is also required regarding consumer rights and obligations respecting credit cards.
France	General applicability of civil code (errors and disputes) and rules for credit institutions (currently applies to loss or theft of checks and credit cards).	General applicability of civil code and rules for credit institutions.
Germany	General applicability of civil code. Ombudsman programme.	General applicability of civil code and rules for credit institutions.
Italy	General applicability of civil code and 1993 banking law. Banking industry self-regulatory code applicable to electronic money schemes. Banking industry ombudsman to settle disputes.	Regulatory authorities plan to require broad disclosure of information to consumers.
Japan	General applicability of civil code and rules for credit institutions. Financial and technology entities have developed technical standards to prevent fraud, loss, theft for computer systems of financial institutions.	General applicability of civil code and rules for credit institutions. Prepaid Card Law requires that any limits on term and location of use must be disclosed on the card.
Netherlands	Dispute resolution procedures of courts and banking industry committee apply to electronic money. Banking industry Code of Best Practices on consumer protection. Dutch government recognises self-regulatory measures.	General applicability of civil code and rules for credit institutions.
Sweden	General applicability of civil code and rules for credit institutions.	General applicability of civil code and rules for credit institutions.
Switzerland	General applicability of civil and penal codes.	General applicability of civil code
United Kingdom	Dispute resolution and unfair terms addressed in Fair Trading Act, Unfair Terms in Consumer Contracts Act. Code of Banking Practice covers loss and errors where banks or building societies are involved. Voluntary banking ombudsman and statutory building societies ombudsman.	General provisions of the Code of Banking Practice apply to banks and building societies.
United States	Applicability of general commercial law. Applicability of the Electronic Fund Transfer Act to stored-value products under review by the Federal Reserve.	Applicability of disclosure requirements of Electronic Fund Transfer Act to stored-value products under review by the Federal Reserve. Office of the Comptroller of the Currency has issued guidance to national banks.

Note: This table is intended to provide a general sense of the current status of policies in different countries and does not indicate determinations about any particular institution, product, or scheme.

Country	Deposit insurance or other guarantees	Privacy
Belgium	Applicability of deposit insurance scheme to electronic money products is under review.	Belgian law incorporates the EC Directive on Protection of Personal Data.
Canada	Applicability of deposit insurance to electronic money under review.	Regulations to be introduced in 1997 for federally regulated financial institutions. Broad privacy legislation at federal level to be developed by 2000. Quebec has adopted privacy legislation applicable to the private sector. Financial institutions to adopt the Canadian Standards Association's privacy code in 1997. Canadian Payments Association imposes general privacy obligations.
France	Deposit insurance scheme applies to electronic money.	General applicability of civil code. Applicability of French banking law. Consent of consumer required for transfer of personal information.
Germany	Rules for credit institutions.	General applicability of civil code.
Italy	Deposit insurance scheme applies to electronic money. Bearer cards are excluded.	EC Directive recently implemented by Parliament.
Japan	Applicability of deposit insurance to electronic money under review. Under the Prepaid Card Law, card holders have priority claim on funds issuers must deposit with the Depository Office.	Industry groups have issued detailed guidelines on consumer privacy for financial institutions.
Netherlands	Applicability of deposit insurance scheme to electronic money under consideration Banks participating in electronic money systems have developed loss-sharing plan in the event of insolvency of one of the group.	Dutch Act on the Registration of Personal Data and EC Directive apply to electronic money.
Sweden	Deposit Guarantee Board has determined that the deposit guarantee scheme is applicable to existing prepaid cards issued by banks.	General laws on privacy applicable to banks and other credit institutions.
Switzerland	Banks participating in electronic money systems have developed loss-sharing plan in the event of the insolvency of one of the group.	Federal law on data protection, banking secrecy laws, Swiss penal code on computer crime and the Swiss Civil code may be applicable to electronic money.
United Kingdom	Applicability of deposit insurance to electronic money unclear.	Data Protection Act
United States	The Federal Deposit Insurance Corporation has determined that federal deposit insurance does not apply to most stored-value cards issued by depository institutions.	Limited federal statutory protections and state laws for financial institutions may apply.

Note: This table is intended to provide a general sense of the current status of policies in different countries and does not indicate determinations about any particular institution, product, or scheme.

Country	Anti-money laundering measures
Belgium	Anti-money laundering laws applicable to credit institutions.
Canada	Measures apply if issuer is a regulated financial institution.
France	Anti-money laundering laws and regulations applicable to credit institutions.
Germany	Anti-money laundering laws and regulations applicable to credit institutions.
Italy	Anti-money laundering laws and regulations applicable to credit institutions.
Japan	Anti-money laundering laws and regulations applicable to credit institutions and other institutions.
Netherlands	Anti-money laundering law applies, including "know-your-customer" and reporting of unusual transactions.
Sweden	Anti-money laundering laws and regulations applicable to credit institutions.
Switzerland	Proposed law on money laundering will be applicable to all financial intermediaries, including electronic money issuers; the proposed law requires that financial intermediaries provide any kind of information that will allow the reconstruction of transactions. Banks subject to Swiss Banking Law.
United Kingdom	Money Laundering Regulations of 1993 apply to electronic money. Requirements for reporting suspicious transactions and ability to supply an audit trail.
United States	Anti-money laundering laws and regulations applicable to banks and other institutions. Applicability to electronic money products under review.

Note: This table is intended to provide a general sense of the current status of policies in different countries and does not indicate determinations about any particular institution, product, or scheme.

Country	Licensing
Belgium	Currently, no legal restriction on issuance of electronic money. Only credit institutions have issued electronic money to date. No special authorisation needed for those institutions to issue electronic money.
Canada	No current prohibition on electronic money issuance by non-financial institutions (only regulated deposit-taking financial institutions have issued electronic money to date). Approval may be required for a financial institutions to establish a subsidiary.
France	French Banking Act requires electronic money issuers to be credit institutions, with the exception of limited-purpose prepaid cards. No special authorisation needed for credit institutions to issue electronic money but any scheme must be submitted to the Bank of France.
Germany	Electronic money issuers must be credit institutions, except for limited-purpose (2-party) prepaid cards. No special authorisation needed for full-scale credit institutions to issue prepaid cards or network electronic money. A general-purpose prepaid card issuer may be exempted from the licensing requirements at the discretion of the Federal Bank Supervisory Office.
Italy	Issuers of multi-purpose electronic money must be credit institutions. No special authorisation needed for credit institutions.
Japan	Restriction of issuance of electronic money redeemable with cash to credit institutions is under review. Under the Prepaid Card Law, 2-party issuers (issuer and merchant are the same) must notify the Ministry of Finance; issuers of 3-party (other than 2-party type) cards must register with the Ministry of Finance.
Netherlands	Issuers of electronic money are considered credit institutions, which have to obtain authorisation from the Netherlands Bank. Exceptions can be made for small-scale electronic money schemes. Entities involved in implementing an electronic money scheme, but not issuing electronic money themselves, are not considered to be credit institutions.
Sweden	Currently no restrictions on issuance of electronic money. No special authorisation needed for banks. To date, only banks and credit institutions have issued electronic money.
Switzerland	Authorities have not delivered an opinion on issuance of electronic money. To date, only banks and the Swiss Postal Office participate in general-purpose electronic money schemes. In the opinion of the Federal Banking Commission, issuance of e-money is linked to a professional offer in public to accept clients' assets, which is restricted to banks. Proposed money laundering laws will require electronic money issuers to belong to a self-regulatory organisation or be licensed by a special government entity.
United Kingdom	Banks subject to general authorisation in Banking Act, or building societies in the Building Societies Act. Non-bank issuers of electronic money schemes that do not have characteristics of deposit taking would not require authorisation. Non-banks involved with electronic money schemes that do have the characteristics of deposit taking would have either to apply for authorisation themselves, or enter into a joint venture with an authorised institution, which would be responsible for the deposit taking element.
United States	No special authorisation needed for banks to issue electronic money products. Authorisation may be required for a bank to invest in a separate entity to conduct such activities. State money transmitter laws may require non-depository institutions that issue electronic money products to be licensed.

Note: This table is intended to provide a general sense of the current status of policies in different countries and does not indicate determinations about any particular institution, product, or scheme.

Country	Prudential requirements for issuers	Examinations, internal controls, and information systems security
Belgium	For credit institutions same as for other banking activities.	Procedures applicable to credit institutions. National Bank of Belgium collects statistical information from electronic money system operators twice each year. It has conducted an informal audit of the electronic money scheme.
Canada	For regulated financial institutions, existing legislation and regulatory requirements apply, including capital requirements.	Procedures applicable to regulated financial institutions.
France	Regular banking regulations	Same procedures for credit institutions (on-site examinations, internal controls, information security audits).
Germany	Standard minimum capital, solvency and liquidity requirements for credit institutions that take deposits and make loans. Modified requirements possible for institutions that only issue electronic money.	Credit institutions submit monthly reports to the Bundesbank and annual accounts, annual reports, and auditor reports to the FBSO and Bundesbank.
Italy	Same as for other banking activities.	Standard examination and reporting requirements for credit institutions. Electronic money schemes currently subject to off-site controls. The Bank of Italy is considering introduction of specific information systems security and internal control requirements.
Japan	Credit institutions subject to requirements of Banking Law. Issuers covered by the Prepaid Card Law must deposit funds with the Depository Office of not less than 50% of unused balances of cards issued.	Credit institutions subject to regular reporting requirements and examinations. Issuers under the Prepaid Card Law subject to regular reporting requirements and, for 3-party issuers, subject to examinations.
Netherlands	Issuers must comply with all requirements of the Act on the Supervision of Credit System, including liquidity and capital adequacy requirements.	Same procedures for credit institutions, including qualifications of management and system operator to fulfil security and integrity requirements of the electronic money scheme. On-site and off-site examinations and external audits.
Sweden	Standard banking laws and regulatory procedures apply to banks.	Standard banking requirements apply. On-site and off-site examinations and external audits.
Switzerland	Swiss Banking Law specifies financial requirements for banks, which are supervised by the Federal Banking Commission.	External auditor reports for banks. Swiss Code of Obligation subjects other companies to examination procedures in order to fulfil common industry standards.
United Kingdom	Standard banking laws and regulatory procedures apply to banks.	Banks and building societies must show evidence of a realistic business plan and adequate systems and controls.
United States	No special financial requirements for banks issuing electronic money. Some states prescribe investment standards for non-bank money transmitters; applicability to electronic money issuers unclear.	On-site, generally annual examinations for banks, covering information systems security, internal controls, etc. Examination authority for bank holding companies and subsidiaries of banks. Some states examine non-bank money transmitters or have other requirements.

Note: This table is intended to provide a general sense of the current status of policies in different countries and does not indicate determinations about any particular institution, product, or scheme.

ANNEX 2

BIBLIOGRAPHY

Bank for International Settlements, Implications for Central Banks of the Development of Electronic Money, October 1996.

Committee on Payment and Settlement Systems, Payment Systems in the Group of Ten Countries, Bank for International Settlements, December 1993.

Committee on Payment and Settlement Systems and the Group of Computer Experts, Security of Electronic Money, Bank for International Settlements, August 1996.

Financial Action Task Force, FATF-VIII Money Laundering Typologies Exercise Public Report, February 1997.

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

ANNEX 3

Members of the Working Party on Electronic Money

Chairman

Mr. Timothy Geithner

Belgium	Pierre Verly Benoit Bourtembourg	Ministry of Finance National Bank of Belgium
Canada	David Iwaasa Kevin Clinton	Department of Finance Bank of Canada
France	Thierry Francq Jacqueline Lacoste	Ministry of Finance and Economy Bank of France
Germany	Wolfgang Michalik Udo Franke	Deutsche Bundesbank Ministry of Finance
Italy	Alberto Contessa Marcello Condemi	Bank of Italy Bank of Italy
Japan	Yukio Yoshimura Eiji Mutoh	Ministry of Finance Bank of Japan
Netherlands	J. Rietrae/P. Verheugd Martin Santema	Ministry of Finance Netherlands Bank
Sweden	Monica Rodrigo Peter Stenkula	Ministry of Finance Bank of Sweden
Switzerland	Urs Bischof Marie-Armelle Libbrecht	Swiss National Bank Federal Department of Finance
United Kingdom	Colin Farthing Dean Blagden	HM Treasury Bank of England
United States	James Kamihachi Jeffrey Marquardt	Department of the Treasury Board of Governors of the Federal Reserve System

Bank for International Settlements	Paul Van den Bergh Masao Okawa
International Monetary Fund	Warren Coats
European Commission Brussels	Helmut Bauer
Organisation for Economic Co-operation and Development	Rinaldo Pecchioli
European Monetary Institute	Emily Witt
Secretaries*	Gavin Bingham Edward Gardner Charles Pigott

* Heidi Richards and Daniel Nolle made important contributions to the preparation of the report.