The Report of the Consumer Electronic Payments Task Force

April 1998

TABLE OF CONTENTS

EXECUTIVE SUMMARY

To ensure that consumer concerns arising from new electronic payment technologies receive appropriate consideration, the Secretary of the Treasury Robert E. Rubin established the Consumer Electronic Payments Task Force ("Task Force") in the fall of 1996. Eugene A. Ludwig, Comptroller of the Currency, chaired the Task Force, which included Richard L. Gregg, Commissioner of the Financial Management Service; Jack Guynn, President of the Federal Reserve Bank of Atlanta; Andrew C. Hove, Jr., Chairman of the Federal Deposit Insurance Corporation; Edward W. Kelley, Jr., Member of the Board of Governors of the Federal Reserve System; Robert Pitofsky, Chairman of the Federal Trade Commission; and Ellen Seidman, Director of the Office of Thrift Supervision.

The Task Force focused its attention primarily on new payment technologies known as electronic money. The Task Force members recognized that a widespread market for electronic money ("e-money") products could offer merchants, financial service providers, and government entities the opportunity for greater cost efficiencies and consumers the opportunity for greater convenience and security. However, they also recognized that these benefits cannot be fully realized without wide consumer acceptance of e-money. Consumer acceptance in turn requires that consumers have confidence in the new products, understand the benefits and risks of the products, and believe that their concerns about the products have been considered and addressed. Thus, the Task Force established as its mission to identify, in partnership with the industry and the public, consumer issues raised by emerging electronic money technologies and to explore the extent to which innovative responses are being developed that are consistent with the needs of this developing market.

This report documents the Task Force's findings and its recommendations for future action.[1] The report is divided into four sections focusing on the four areas of consumer concern: Access, Privacy, Financial Condition of Issuers, and Consumer Protections and Disclosures. Each section describes a different set of consumer concerns, evaluates whether the market has or is likely to address these concerns, summarizes existing laws, regulations, and industry responses relevant to these concerns, and assesses the existing protections.

Access: The first section of the report — Access — is designed to provide a background for other areas discussed. The Task Force recognizes that e-money holds the potential to provide convenience and security for consumers. However, such benefits can only be achieved fully if e-money products are widely accessible. Although existing legal requirements that financial institutions provide certain financial services to the communities they serve may not apply to e-money products, there is no evidence that issuers will only provide e-money products to certain segments of consumers. However, the Task Force encourages financial literacy efforts by

[1] The report, however, does not constitute final agency action nor bind any agency members of the Task Force.

industry representatives and consumer organizations, in cooperation with the government, to help educate all segments of the population on the use of technology in financial services.

Privacy: The second section of the report is devoted to privacy. Many consumer concerns about privacy extend beyond e-money alone to all financial services. Consumer concerns are also not uniform — some consumers are extremely protective of their privacy and view any collection or use of personally identifiable information as an intrusion, while others are far less concerned about privacy-related matters.

Current e-money technology is capable of delivering products with varying effects on privacy, ranging from fully anonymous, cash-like systems, in which no personally identifiable transaction records are created, to fully auditable systems that can identify and store every transaction conducted by every consumer.

Market forces, including competition from cash and from other anonymous payment instruments, may encourage e-money issuers to be responsive to significant consumer privacy concerns. Many financial industry participants, either individually or as part of industry groups, are exploring self-regulatory responses to consumer privacy concerns in the financial services industry more generally. The Task Force urges industry to develop self-regulatory initiatives that include effective and meaningful controls on the collection and use of information pertaining to consumers and their use of e-money. Such initiatives also tend to be more viable when they involve some mechanism to assure adherence. Of course, such initiatives must be designed not to produce anti-competitive effects in the market more generally. The Task Force urges industry members to take the necessary actions to implement these policies and to disclose their privacy policies to consumers.

Financial Condition of Issuers: The third section of the report addresses consumer concerns surrounding e-money issuer insolvency. Although it may be too early to tell whether market developments will address these concerns adequately, early indications are that industry participants have strong incentives to do so. Fears about the impact of issuer default on the reputation of other issuers will likely cause those institutions to take steps to limit this risk. Issuers may also encourage consumer acceptance by disclosing the existence of available financial guarantees. Additionally, the industry may develop disclosure policies to inform consumers of their rights in the event of issuer default, on the insured/uninsured status of the e-money product, and on the extent to which an issuer is subject to regulatory oversight.

Moreover, existing regulatory schemes may provide consumers with additional protections. Depository institutions that issue e-money will be subject to the supervision and examination of the federal and state depository institution regulatory agencies. Additionally, these issuers are expected to disclose the insured or non-insured status of the e-money products they issue. Nonbank issuers may also be subject to state supervisory oversight, and are subject to the enforcement authority of the Federal Trade Commission. The Task Force urges all e-money

issuers to establish policies and procedures to safeguard customer funds and ensure that e-money transactions will be honored.

Consumer Disclosure and Protections: The fourth section of the report addresses consumer concerns about their rights and liabilities with respect to e-money systems and whether they will receive adequate disclosure of these rights and liabilities. Although it is uncertain whether existing statutory protections apply to e-money, other governmental actions may address some of the consumer concerns expressed to the Task Force. For example, some of the federal banking agencies have issued guidance encouraging banks that engage in e-money activities to provide adequate disclosures with respect to their e-money products.

Recommendations for Future Action: The report concludes with recommendations for future action. The Task Force recommends that government activities with respect to electronic money generally be limited at present to:

> (1) *Providing Consumer Financial Education.* Government may supplement information provided by industry to help consumers become better educated and empowered to seek financial and payment products that will meet their individual needs.
> (2) *Monitoring Industry Developments.* Relevant government agencies should continue studying consumer concerns on e-money to protect the public interest. If self-regulatory or other efforts fail to address consumer concerns adequately, other alternatives may need to be explored.
> (3) *Encouraging Appropriate Industry Action.* Through its monitoring efforts, government can act effectively as a clearinghouse for information relating to the electronic money industry, and as the industry continues to evolve can advise industry participants and groups as to the nature of consumer concerns and suggest possible avenues for addressing those concerns. Most significantly, government should encourage and foster meaningful and responsive self-regulatory efforts, where feasible, without hampering innovation and experimentation in the marketplace.

The Task Force also recommends that actions be taken to help address specific concerns discussed in the report.

> *Access*. The Task Force recommends that government address one subset of access issues — potential concerns about knowledge of how to use these products — through appropriate consumer education efforts that take into account the ongoing changes in these products and their intended markets.
>
> *Privacy.* The Task Force recommends that industry groups continue to explore self-regulatory initiatives that are meaningful and effective in that they both respond to consumers' privacy concerns and involve some means to assure

adherence by individual participants. These means can include a variety of flexible approaches.

Financial Integrity. The Task Force urges issuers of e-money to establish policies and procedures to safeguard consumer funds and ensure that transactions will be honored as promised. The Task Force also encourages all e-money issuers to disclose to consumers information relevant to issuer soundness and to inform consumers of their ability to recover funds in the event of issuer insolvency.

Consumer Protection and Disclosures. The Task Force recommends that issuers either individually or as part of industry groups move toward adopting effective and meaningful approaches for other consumer protection and disclosure issues, as appropriate. These could include, for example, information about applicable fees, deposit insurance, and error resolution procedures, if any, and liability for lost or stolen e-money. The Task Force further recommends that industry participants explore means to implement such policies through measures that could include product features, consumer education and marketing information, model disclosures, promotion of the policies among industry participants, and the development of means to monitor, certify, and report the extent of their adoption.

Finally, relevant government agencies should continue to monitor consumer concerns and industry initiatives in each of the four areas reviewed and consider whether alternative approaches are warranted in the future.

BACKGROUND

The emergence of electronic money (e-money) has prompted much research and study by both the public and private sectors. Although many have lauded the promise of these new payment methods for industry and government, less attention has been focused on the implications of e-money for consumers.

To ensure that consumer concerns arising from these new payment technologies receive appropriate consideration, the Secretary of the Treasury Robert E. Rubin established the Consumer Electronic Payments Task Force ("Task Force") in the fall of 1996. Eugene A. Ludwig, Comptroller of the Currency, chairs the Task Force, which includes Richard L. Gregg, Commissioner of the Financial Management Service ("FMS"); Jack Guynn, President of the Federal Reserve Bank of Atlanta; Andrew C. Hove, Jr., Chairman of the Federal Deposit Insurance Corporation ("FDIC"); Edward W. Kelley, Jr., Member of the Board of Governors of the Federal Reserve System; Robert Pitofsky, Chairman of the Federal Trade Commission ("FTC"); and Ellen Seidman, Director of the Office of Thrift Supervision ("OTS").

The Task Force members recognized that a widespread market for e-money products could offer merchants, financial service providers, and government entities the opportunity for greater cost efficiencies and consumers the opportunity for greater convenience and security. However, they also recognized that these benefits cannot be fully realized without wide consumer acceptance of electronic money. Consumer acceptance in turn requires that consumers have confidence in the product; understand the benefits and risks of the new products; and believe that their concerns about the products have been considered and addressed.

The Task Force set out to identify consumer issues raised by emerging electronic money technologies and to determine how to address these issues without unnecessarily inhibiting the development of this market.

Thus, the Task Force established as its mission to identify, in partnership with the industry and the public, consumer issues raised by emerging electronic money technologies and to explore the extent to which innovative responses are being developed that are consistent with the needs of this developing market. Accordingly, each of the major sections of the report describes a different set of consumer concerns, evaluates whether the market has or is likely to address these concerns, provides a summary of the existing laws, regulations, and industry efforts relevant to these concerns, and concludes with an assessment of those existing protections.

Task Force Proceedings

To gain insight into consumers' concerns arising from electronic money, the Task Force conducted a series of informal information exchanges with firms involved in e-money systems, financial services industry representatives, and consumer and other public interest advocates.[2]

---

[2] Summaries of these meetings appear at http://occ.treas.gov/emoney/htm.

The purpose of these initial exchanges was to expand the understanding of Task Force members and others about how emerging payment technologies may affect consumers, to identify potential issues, and to plan public meetings through which to explore those issues further.

Once the Task Force completed this series of information exchanges, the Task Force published notices in the Federal Register announcing two public meetings inviting both participation at the meetings and the submission of written comments in response to issues raised in the notice.[3] The Task Force's first public meeting was held on June 9, 1997 and consisted of four panel discussions. That meeting began with a presentation by e-money industry participants addressing the status and development of the e-money market. Panel discussions on consumer protections and disclosures, financial condition of issuers, and access followed. Most panels consisted of a mix of representatives of the industry and public interest organizations to provide varied perspectives. The second public meeting was held on July 17, 1997 and consisted of two panel discussions. The first panel discussion began with a demonstration of an anonymous digital Internet-based payment system, followed by a discussion on privacy concerns. The second panel began with a presentation on digital signatures, followed by a discussion of security issues arising from e-money.

The Task Force supplemented the information obtained through the informal information exchanges and public meetings with publicly available information, including the Group of Ten's Working Party on Electronic Money, *Report on Electronic Money*, the G-10 central bank's *Report on Security of Electronic Money*, the Federal Reserve Board's *Report to Congress on the Application of the Electronic Fund Transfer Act to Electronic Stored Value Products* and *Report to Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud*, the Clinton Administration's *Framework for Electronic Commerce*, the Federal Trade Commission's *Report on Individual Reference Services* and *Staff Report on the Public Workshop on Consumer Privacy on the Global Information Infrastructure*, the National Telecommunications and Information Agency's studies entitled *Privacy and Self Regulation in the Information Age* and *Falling through the Net*, the Congressional Budget Office's *Emerging Electronic Methods for Making Payments*, and the Department of Treasury's *Study on American Finance for the 21st Century*.

E-Money Systems

The term "e-money" encompasses a wide variety of existing and planned products designed to provide an alternative to traditional means of payment. This diversity of potential and existing e-money products makes it difficult to render a single description that encompasses all electronic money systems in terms of technological, market, or legal distinctions. For purposes of this report, however, an "e-money" or "electronic stored-value" product is a prepaid balance of funds,

[3] *See* 62 Fed. Reg. 19173 (April 17, 1997); 62 Fed. Reg. 29392 (May 30, 1997).

or "value," recorded on a device controlled by the consumer, generally either a card or the consumer's personal computer.[4]

E-money can be used for point of sale or for Internet-based purchases. The balance on the device is decreased, or debited, when the device is used for payment. A wide variety of card-based systems are possible, differing according to the technology used, whether the system is "open" or "closed," whether transactions occur on-line to a central system or off-line, and whether the cards are disposable or reloadable.

Card-based stored value has been in existence for many years. Early generations of card-based stored value, often known as pre-paid cards, involve recording a balance of funds on a magnetic stripe that is debited by the terminal after each use. Although magnetic stripe technology provides a low-cost means to distribute stored value, it does not provide sufficient safety from tampering or counterfeiting to be applied to off-line systems in which relatively large amounts of value will be placed on the cards. In addition, options for reloading of magnetic cards are limited as is the ability to store transaction information.

Smart cards, *i.e.*, cards with an embedded microprocessor chip, provide features superior to those of magnetic stripe cards. The microprocessor chip can store and manipulate data according to pre-programmed functions on the chip and external instructions from a card-reading unit. Smart cards promise additional security by permitting sophisticated encryption technology to protect the value on the card from counterfeiting. In addition, smart cards may bundle various products on a single card, that could function as a credit card, a debit card, a stored value card, and a repository of personal information (such as a driver's license, medical information, etc.).

Many card-based systems presently in use are "closed" systems — systems where the value is only redeemable in exchange for the issuer's goods or services. Most of these systems use magnetic stripe technology. Common examples of closed systems include transportation systems in major metropolitan areas, photocopiers in public libraries, and long distance telephone cards. Utilities, laundry and parking facilities are also increasingly incorporating stored value systems.[5]

---

[4] This value may be "balanced-based" where a single balance is stored and updated with each transaction; or "note-based" where electronic "notes," each with a fixed value and serial number, are transferred from one device to another. *See Security of Electronic Money*, Bank for International Settlements, 1996. Electronic stored value products may also be thought of as products sharing similar characteristics including: (i) a card or other device that electronically stores or provides access to a specified amount of funds selected by the holder of the device and available for making payments to others; (ii) the device being the only means for routine access to the funds; (iii) the issuer not recording the funds associated with the device as an account in the name of (or credited to) the holder. *See* Federal Reserve Board Report to Congress on the Application of the Electronic Fund Transfer Act to Electronic Stored Value Products ("FRB Report"), March 1997.

[5] *See* Mary Jo Bohr and Thomas Zack, *A New Billing Strategy for a Local Gas Distributor*, Public Utilities *Fortnightly*, 26 (January 15, 1997).

Other closed systems are multi-functional, and usually involve smart card technology. These systems generally involve a narrowly defined group of consumers (for example, college students), a small group of merchants, and a relatively small geographic area over which to install the necessary infrastructure. Such systems are also gaining in popularity. These semi-closed systems are most often seen on university and corporate campuses and surrounding environs, and on military installations.[6]

In truly open systems, on the other hand, e-money could be used with many merchants over an extended geographic area and function as a general medium of exchange. Such systems only exist in limited pilots such as the Mondex pilot in Guelph, Canada. In a press release dated March 11, 1998 Mondex stated that 560 merchants representing over 90 percent of all merchants in Guelph accept Mondex as a payment option.[7]

Some stored-value card systems, such as pre-paid phone cards in the United States, interact with a central database system that maintains the records of funds associated with each card and require verification of every transaction on-line with the central system. However, most of the e-money systems envision that transactions will typically be off-line except for purposes of purchasing, reloading or redeeming the stored-value.[8]

Many of the current stored-value systems are reloadable, permitting consumers to add to the value on the cards through machines that accept currency or credit cards. Where cards are linked to the consumer's depository institution account, they can be reloaded through ATMs and in some cases through personal computers equipped with remote computer banking software and a card reader device.[9]

---

[6] Florida State University (FSU) currently has 36,000 smart cards outstanding with a total card malfunction of 100 cards. FSU expanded its system to include card based systems and credit card transactions. Remarks and Prepared Statement, Bill Norwood, Vice President for Business Relations at CyberMark, Task Force Public Meeting (June 9, 1997), Panel on Internet and Stored Value Payment Activities/Pace of Internet Developments.

[7] Additionally, Mondex states that there are 12,000 cardholders in Guelph and that it has issued $2 million (CAN) to date. *See Latest News on Mondex Website*, www.mondex.com.

[8] Visa is currently marketing a magnetic stripe electronic travelers check, Visa TravelMoney, that permits consumers to access monies with a PIN at all 250,000 Visa ATMs worldwide. Visa TravelMoney is an online system and the average value stored on a card is $1500. Remarks and Prepared Statement, Lamar Smith, Senior Vice President of Government Relations, Visa, Task Force Public Meeting (June 9, 1997), Panel on Internet and Stored Value Payment Activities/Pace of Internet Developments and Panel on Disclosures and Consumer Protections.

American Express is marketing a similar on-line product to the federal government. This card is also magnetic stripe based and is designed to hold per diem travel monies. Remarks and Prepared Statement, Judie Rinearson, Group Counsel for American Express, Task Force Public Meeting (June 9, 1997), Panel on Disclosures and Consumer Protections.

[9] For example, Citibank is testing a Visa Cash system that enables consumers to load value on their cards through the use of a "Personal ATM" (devices that plug into standard telephone lines and enable users to reload value on their cards). *See Smart Cards: It's up to you New York, New York*, Bank Network News, October 14, 1997.

A few e-money systems are designed primarily for Internet transactions, permitting consumers to use personal computers to make payments to other parties via Internet e-mail or other computer-to-computer communication methods. Consumers wishing to utilize these Internet systems must first install specialized software on their computers. In these systems, the device that stores the value is generally the consumer's personal computer rather than a card.

The distinction between smart card and Internet based e-money systems appears to be diminishing as some providers of stored value cards are testing their systems internationally for Internet payments.[10] Future systems may integrate these and other payment methods, possibly through the use of a smart card reader attached to the consumer's personal computer.[11]

The Market for E-Money Products

Consumers in the United States have a wide array of choices of payment mechanisms. They can use cash, checks, credit cards, debit cards, or money orders for many payments. Credit and debit cards are increasingly being accepted for smaller dollar payments — payments that traditionally were made in cash. Whether open e-money systems will succeed against this array of competing products in this market is unclear.

Most retail payments in the U.S. are made using one of six payment instruments: cash, checks, credit cards, debit cards, and Automated Clearing House ("ACH") debits and credits.[12] The U.S. has a predominantly paper-based payment system for retail transactions, relying on checks for 87 percent of noncash retail payments. The U.S. is also the only developed country in which check use is increasing.[13]

---

[10] Mondex, in conjunction with AT&T, is testing such a system. Remarks and Prepared Statement, Matthew Miller, Senior Manager, Mondex USA, Task Force Public Meeting (June 9, 1997), Panel on Internet and Stored Value Payment Activities/ Pace of Internet Developments. Visa is also experimenting with Internet applications. *See First Union to Offer Smart Cards on Net*, Vol. II, Financial Network News, No. 42, pg.8.

[11] Some believe that all future e-money systems will be designed for both Internet and stored-value card payments. *See* David C. Stewart, *Picking Winners and Losers in Digital Cash*, Bank Technology News, October 1997.

[12] For figures on checks, credit cards, debit cards, and ACH payments, *see Statistics on Payment Systems in the Group of Ten Countries*, Bank for International Settlements, Dec. 1997. For figures on consumer payment media, including cash, see *The Nilson Report*, issue 656, Nov. 1997. Those figures show that money orders and travelers checks account for less than 2 percent of all consumer payments.

[13] There are several possible explanations for the popularity of checks in the United States. First, the well developed market for paper checks in the U.S. provides fewer incentives for consumers to use electronic payments. Second, consumers are generally not charged directly for the costs associated with checks, and consumers are accustomed to the float associated with checks. Third, checks are convenient for consumers, readily accepted for payment, and the legal foundations are well established. *See The Federal Reserve in the Payments Mechanism*, Board of Governors of the Federal Reserve System, January 1998.

Adoption of retail electronic payments has been relatively slow. However, there has been strong growth in electronic payments over the last several years as American consumers have become more familiar with these alternatives. For example, since 1990 consumers have increased their annual charge volume on bank credit cards by 128 percent. There has also been strong growth in the debit card market in recent years. Approximately 40 percent of financial consumers now use debit cards and the average number of monthly transactions grew from 4.7 to 7.3 in January of 1997.[14] To date, e-money, whether card or Internet-based, remains a very minor player in the payments system.

Current Usage

E-money has been widely touted as an alternative to cash that provides consumers with added security and convenience for small-dollar transactions, while providing merchants greater efficiency in cash handling, and lower transaction fees.[15] Although some have expressed doubts about the viability of e-money, these concerns have not stopped the proliferation of pilot programs worldwide. The major e-money sponsors are currently participating in pilot programs in Argentina, Australia, Brazil, Canada, Colombia, the Czech Republic, Hong Kong, Italy, Japan, Mexico, Norway, New Zealand, Poland, South Africa, Sweden, Switzerland and the United Kingdom.[16] Additionally, Austria, China, Costa Rica, Greece, Israel, Korea, Malaysia, Moldova, the Netherlands, Saudi Arabia, and Singapore are also either presently or soon will be experimenting with domestic corporations' proprietary e-money products.

Belgium, Denmark, Finland, France, Germany, Portugal, Spain, and Thailand have completed the experimentation stage and have begun implementing e-money systems nationwide. For example, Proton, founded by Banksys (a consortium of 60 banks), has issued 900,000 cards in Belgium alone, and more than 14 million cards worldwide.[17]

---

[14] *See* Block, Valerie, *Debit Use Takes Off; ATM Cards Hit a Wall*, *The American Banker*, January 2, 1997.

[15] *See* John Wenninger and David Laster, *The Electronic Purse*, Current Issues in Economics and Finance, Federal Reserve Bank of New York, Vol. 1, No. 1 (April 1995). Many believe that electronic stored value cards promise consumers greater convenience than cash, avoiding the necessity of carrying change and decreasing trips to the ATM. Such products may also provide consumers greater physical security, particularly when consumers can add value to the cards at home using their personal computer. However, preliminary indications from several U.S. pilot projects reveal that these benefits may not result in greater use until widespread merchant acceptance of stored value cards is achieved.

[16] These sponsors include American Express, Europay, MasterCard, Mondex, Proton, and Visa. For example, as of September 1997, Visa had approximately 7 million Visa Cash cards outstanding worldwide, with an average load amount of $46.70. Approximately 6.2 million transactions had been conducted with an average transaction amount $4.38 and a total sales volume of $27 million. Approximately 54 percent of Visa Cash cards are reloadable. *See* Visa, *Chip Programs Around the World*, October 30, 1997.

[17] Belgian consumers pay BFr1,200 (approximately $6) per year. Merchants, have paid Banksys up to BFr15,000 (approximately $70) per terminal and 0.7 percent of every sale in which the card is used. *See Electronic*

Several open e-money systems are currently in pilot phases in the United States. For example, over 1.7 million cards were produced at the 1996 Olympic Summer Games in Atlanta, and 200,000 transactions totaling about $1.1 million were conducted. Other pilot programs currently underway in the U.S. involve multipurpose multi-application smart cards that permit loyalty programs and ticketless airline travel.[18]

One large-scale U.S. pilot program involving 50,000 consumers and over 500 merchants is currently underway on the Upper West Side of Manhattan. In this pilot, MasterCard and Mondex (in conjunction with Chase Manhattan Bank) and Visa (in conjunction with Citibank) in tandem are issuing their own products supported by interoperable readers capable of accepting value from either product.[19] The results of these pilots to date indicate that consumer and merchant acceptance may be slower than initially thought.[20]

Internet-based e-money systems also promise consumers great convenience and security for Internet transactions. However, the development of the Secure Electronic Transactions protocol, encrypting consumer credit card numbers when used over the Internet, as well as the development of other security features for credit card transactions, may have satisfied consumers' desire for additional security in connection with an already-accepted payment mechanism. This development may cause Internet based e-money issuers to develop their product as a niche product for micro-payments, such as for purchases of information over the Internet. Additionally, as mentioned earlier, some stored value card issuers are exploring using their transaction protocols for Internet-based transactions.[21]

Money, Chipper, for now, The Economist, p. 72, 77 (April 26, 1997).

[18] For example, American Express has joined Hilton Hotels and IBM/American Airlines to offer co-branded multifunction smart cards that permit ticketless travel. Remarks and Prepared Statement, Glenn Weiner, Vice President of Smart Card Center at American Express, Task Force Public Meeting (June 9, 1997), Panel on Internet and Stored Value Payment Activities/ Pace of Internet Developments. *See also* Jeffrey Kutler, *Card Frontiers: Amex Proposes Standards for Virtual Payments*, 162 American Banker 10 (December 3, 1997)

[19] Jason Chervakas and Tom Watson, *Changing the Nature of Money — and Perhaps of Banking*, CyberTimes, The New York Times on the Web (May 9, 1997).

[20] *See* Peter Pae and Devon Spurgeon, *Smart Cards Get off to a Slow Start*, The Washington Post (March 21, 1998).

[21] *See* Jeffrey Kutler, *Digicash Eager to Reap Latest ECash Harvest*, 163 American Banker 18 (December 11, 1997).

Internet based e-money systems, however, have not yet been widely introduced or adopted by consumers or merchants. In fact, the three largest issuers of Internet payments products have conducted less than $3 million in transactions combined.[22]

Potential Usage and Market Structure

In addition to promising consumers greater convenience than cash, such products may also provide consumers greater physical security, particularly when consumers can add value to the cards at home using their personal computer. However, preliminary indications from several U.S. pilot projects are that these benefits may not result in greater use until widespread merchant acceptance of stored value cards is achieved.

E-money will likely remain a minor segment of the U.S. payments system for the near future. Consumers generally will not be compelled to use or accept e-money. Thus, issuers will face considerable market pressure to address factors that give rise to consumers' concerns in order to promote use of their products. Over time, advances in technology and decreasing costs in the storage of information should enable issuers to design stored value products with enhanced safety and security features that respond to consumers' demands. In addition, to promote use of their products, issuers will have an incentive to help consumers learn and become comfortable with the products through advertising, promotional campaigns, demonstration projects, and consumer education programs.[23]

E-money could also provide merchants the ability to reduce cash-handling costs, such as those resulting from employee theft. Additionally, some institutions with specialized needs are increasingly adopting stored value card systems. University campuses and their surrounding environs are one such specialized market. Universities, using smart card technology, can integrate payment capabilities with student identification cards, and provide students the convenience of only needing to carry one card. Other possible markets include corporate campuses, military installations and planned communities.[24] For example, the U.S. military is currently experimenting with stored value cards systems for their trainee's payroll.[25]

---

[22] These issuers include CyberCash, First Virtual, and Wave Systems. Survey Electronic Commerce, *Cash Poor,* The Economist (May 10, 1997).

[23] FRB Report at 68.

[24] *See Diebold, Visa and M&I Data Systems Implement Visa Cash Technology*, Financial News, PR Newswire, December 2, 1997 (discussing Visa Cash pilot at Diebold's corporate campus); SunTrust and VISA USA to Pilot Chip Cards, Financial News, PR Newswire, September 16, 1997 (discussing Visa Cash pilot in Celebration, Florida).

[25] Previously, military trainees often had difficulty receiving their initial salary payments in a timely manner as existing electronic payment systems required several weeks to establish accounts and begin direct deposit. *See Amex, Marine Corps Begin N.C. Smart Card Test,* American Banker, p. 18, September, 17, 1997.

Government actions also may serve to help develop a larger market for e-money products. The Debt Collection Improvement Act of 1996 requires all federal government payments (with certain exceptions) to be made via electronic means by 1999 ("EFT'99"). The Financial Management Service currently anticipates delivering federal payments via direct deposit to all recipients with a deposit account at a financial institution. Federal payment recipients who do not have a deposit account at a financial institution (estimated to be about 10 percent of all U.S. households) have the option of receiving electronic payments at an account established on their behalf by Treasury or if receiving an electronic deposit would be burdensome, recipients can exercise a hardship waiver and continue to receive paper checks by mail.[26]

Although e-money does not play an immediate role in the EFT'99 mandate, it may ultimately help eliminate government-issued paper checks in the near future. Currently, traditional EFT payment mechanisms limit the government from making all payments electronically.[27] For example, because direct deposit transactions require enrollment and authorization by the account holder well in advance of payment, the government must issue paper checks to individuals and businesses that require immediate payment. E-money products could eliminate the necessity for paper checks in this situation by allowing the government to execute electronic payments immediately.

Even now, some state governments are testing smart cards for the distribution of certain state administered benefits programs, such as food coupons and Women, Infants, and Children ("WIC") programs. Although the vast majority of these programs presently use on-line magnetic stripe cards, several states are exploring whether smart cards could be useful for the distribution of coupon-based benefit programs such as food stamps.[28]

Structure of E-money Market

---

[26] See Notice of Proposed Rulemaking, 31 C.F.R. Part 208, 62 Fed. Reg. 48714 (Sept. 16, 1997), implementing the mandatory electronic funds transfer component of the Debt Collection Improvement Act of 1996, Pub. L. No. 104-134.

[27] *Id.* The 31 C.F.R. Part 208, Notice of Proposed Rulemaking, includes waiver provisions for the following federal payments for which there is no convenient or cost effective electronic funds transfer solution: (1) non-recurring payments where the cost of making the payment via EFT exceeds the cost of making the payment by check; (2) payments where an agency's need for goods and services is of such an unusual and compelling urgency that the government would be severely injured unless payment is made by a method other than EFT; and, (3) payments where there is only one source for goods or services, and the government would be seriously injured unless payment is made by a method other than EFT.

[28] Ohio is currently disbursing food stamps through stored value smart cards, and Wyoming is currently running a pilot program under which it is distributing WIC benefits and food stamps using smart cards. Food benefit distribution through smart cards is now considered an available alternative for state issuance through the Department of Agriculture. Congress has mandated that all states implement electronic benefit transfer systems by (either standard debit card or smart card) by 2002. *See* The Food Stamp Act of 1977, as amended, codified at 7 U.S.C. 2011-2036.

At the present time, the market for e-money is still developing, and it is difficult to predict its eventual structure. However, several important aspects of electronic money may affect the market's eventual development. E-money, like other electronic payment methods in use today, may display network characteristics, *i.e*. the value of the product to any user is increased as other potential users adopt the system. In particular, widespread e-money installation of point-of-sale devices capable of reading stored-value cards may be necessary to spur consumer demand while consumers may not demand stored value cards unless there are sufficient locations to use them.[29] Conversely, merchants may lack the incentives to deploy terminals capable of accepting stored value cards unless consumers appear to be willing to use that payment mechanism. Additionally, the technologies themselves often involve economies of scale (*i.e.*, large fixed costs to establish the network and low marginal costs for additional transactions).[30]

For these reasons, some believe that the e-money market will develop similarly to other network industries such as ATMs and credit cards. Initially, there will be a large number of products. However, due to many factors including economies of scale, the number of systems will decrease, resulting in a smaller number of large "branded networks" controlling a majority of the e-money transactions.[31] In these networks, the network and its brand — not the individual issuer — would have a strong retail presence and would be the foremost link in the consumer's mind. Although it is impossible to determine whether such a structure will develop in the U.S., evidence indicates that this may already have occurred for open systems, since there are only a limited number of dominant "brands" of e-money emerging at this time.

Policy Approach for Analysis of Consumer Concerns

The Task Force looked to published governmental policy objectives for a conceptual background for its analyses of the appropriate role of the government in the area of electronic money. In

---

[29] For detailed discussion of network effects *see* Michael Katz and Carl Shapiro, *Network Externalities, Competition, and Compatibility*, 75 American Economic Review 424- 40 (June 1985); Nicolas Economides, *The Economics of Networks*, 14 International Journal of Industrial Organization, pp. 231-47(October 1996). Other features of networks include the need for compatible infrastructures and standard operating procedures. Early leaders in network industries can establish dominant market positions when they have, and can control access to, an installed infrastructure. *See* James J. McAndrews, *Network Issues and Payment Systems*, *Business Review*, Federal Reserve Bank of Philadelphia, pp. 15-25, November/December 1997.

[30] *See* Paul M. Horovitz and Lawrence White, *The Challenges of the New Electronic Technologies in Banking: Private Strategies and Public Policies*, New York University, Salomon Center, Working Paper Series 96-44.

[31] Branded networks would consist of a group of providers using a retail brand identification for marketing purposes and a central organization for establishing network operating rules, business strategy, and network operations. *See* James J. McAndrews, *Banking and Payment System Stability in an Electronic Money World*, Federal Reserve Bank of Philadelphia, Working Paper Series No. 97-9.

particular, the G-10 Working Party Report on Electronic Money[32] noted that government policy should seek to achieve the following objectives with respect to e-money:

> (1) Limiting systemic and other risks that could threaten the stability of the markets or undermine confidence in the payment system,
>
> (2) Providing consumers with adequate protections from fraud and unfair practices, financial loss, or unnecessary intrusions on personal privacy,
>
> (3) Encouraging the development of effective low-risk, low-cost, and convenient payment and financial services for consumers and business,
>
> (4) Ensuring the central bank's ability to conduct monetary policy,
>
> (5) Not hindering law enforcement authorities to prevent and detect the movement of funds associated with criminal activity. [33]

In keeping with this approach, the Clinton Administration, in *A Framework for Electronic Commerce*, has advocated a regulatory policy premised on allowing the private sector to lead the development of electronic commerce in a relatively unfettered environment. The report recommends that the government avoid placing undue restrictions on electronic commerce.

---

[32] At the Lyon Summit in June 1996, the G-7 heads of state and government called for a joint study to investigate the implications of recent technological advances that have made possible the creation of sophisticated methods for making retail electronic payments, including the means to ensure that their benefits are fully realized.

In response, the G-10 deputies formed a Working Party in the autumn of 1996, comprised of representatives from finance ministries, central banks and international organizations, and consulted 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 Organization for Economic Cooperation and Development (OECD). The primary objectives of the report were 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 focused on the identification of broad policy objectives among the G-10 countries and the analysis of national approaches taken to date. G-10 Report, Introduction.

[33] G-10 Report, Policy Objectives at p. 5. This approach is largely consistent with the three broad policy objectives stated by the Federal Reserve Board as critical to determining the need for government regulation of financial services: minimizing the risks to the public associated with instability of financial markets and the failure of financial institutions, limiting the ability of financial institutions to exercise undue market power, and protecting consumers against unfair practices. FRB Report, at p. 11.

Where governmental involvement is needed, its aim should be to support a simple and predictable legal environment for electronic commerce.[34]

Market responses, including actions by individual institutions, merchants, and other participants in e-money systems and other self-regulatory efforts, can be sufficient if they have a high probability of ameliorating concerns for all ranges of consumers (including low- and moderate-income ("LMI") consumers) without resulting in reduced access to these products. Self-regulatory efforts in particular can be sufficient if they provide standards that respond to consumer concerns in a specific and meaningful manner and can influence the practices of the industry. Their effectiveness can be enhanced through means to promote adherence with those approaches, such as providing incentives for adherence and remedies to consumers harmed by non-adherence. Additionally, self-regulatory efforts should not impede market development or consumers' access to e-money products. Finally, such efforts and their implementation must be designed, so as not to produce anti-competitive effects or constrain innovation in the market.

This report documents the Task Force's findings and recommends steps for future action.[35] The report is divided into four sections addressing consumer concerns. Each section describes a different set of consumer concerns, evaluates whether the market has or is likely to address these concerns, provides a summary of existing laws, regulations, and industry responses relevant to those concerns, and concludes with an assessment of the adequacy of existing protections.

The first section discusses issues of consumer access to e-money. This section is designed to provide a contextual background for discussions of market-based and self-regulatory responses appearing in the subsequent sections.[36] The second, third, and fourth sections discuss consumer concerns relating to privacy, the financial condition of issuers, and consumer protections and disclosures, respectively. The conclusion of the report summarizes the analysis contained in each

---

[34] With respect to electronic payment systems the report notes:

> At this early stage in the development of electronic payment systems, the commercial and technological environment is changing rapidly. It would be hard to develop policy that is both timely and appropriate. For these reasons, inflexible and highly prescriptive regulations and rules are inappropriate and potentially harmful. Rather, in the near term, case-by-case monitoring of electronic payment experiments is preferred.

A Framework For Electronic Commerce, p. 6.

[35] The report, however, does not constitute final agency action nor bind any agency members of the Task Force.

[36] Decisions made to address some consumer concerns may also affect other consumer issues, including access to e-money products. For example, the provision of consumer protections or disclosures may increase an issuer's costs and the cost of the e-money products, thereby limiting the afford ability of the products for some consumers possibly negatively affecting access. Accordingly, the Task Force believes that access issues should be considered in all analyses of consumer concerns in the report.

section and offers recommendations for future action consistent with the conceptual approach outlined above.

ACCESS

E-money may provide many benefits to consumers, including convenience and, for some products, added security. However, as with other financial services, e-money may raise important access issues.

Summary of Comments

Many commenters expressed concern that stored value products will be available only to affluent consumers. These commenters urged the government to ensure that new payment methods are equally available to all consumers. Similarly, several commenters expressed concern that a tiered market in e-money, segmented along socioeconomic and demographic lines, would arise in which lower income consumers would have access only to less attractive products for higher fees.[37] Other commenters expressed the concern that high fees to obtain and use e-money may bar low-income consumers from having effective access to these products.[38]

Another commenter stated that only banks should be permitted to issue e-money since banks are located in most communities, they are already subject to comprehensive federal regulation for safety and soundness, and have a fiduciary responsibility to consumers in their communities. This commenter further stated that the federal government should subsidize establishing the e- money infrastructure in low- and moderate income ("LMI") communities to ensure all consumers have access to e-money.[39] Similarly, some commenters stated their belief that banks should remain central to the distribution of e-money to ensure that LMI consumers are not segregated in a separate e-money system.[40]

Several commenters were further concerned that LMI consumers would purchase a large amount of e-money products without fully understanding the risks of the products. These commenters were concerned that similar abuses to those allegedly occurring in the phone card industry may

---

[37] Remarks of Prof. Mark Budnitz, Professor of Law, Georgia State University College of Law, Task Force Public Meeting (June 9, 1997), Panel on Consumer Protections; Remarks of Margot Saunders, Managing Attorney, National Consumers Law Center, Task Force Public Meeting (June 9, 1997), Panel on Consumer Protections and Disclosure; Remarks of Janice Shields, Director, Institute for Business Research, Task Force Public Meeting (June 9, 1997), Panel on Financial Integrity.

[38] Remarks and Written Statement of Donet Graves, Jr., Vice President for Policy Programs, Director, Washington Office, Organization for a New Equality, Task Force Public Meeting (June 9, 1997), Panel on Access.

[39] Remarks and Written Statement of John Harshaw, Regulatory and Legislative Director, National Community Reinvestment Coalition, Task Force Public Meeting (June 9, 1997), Panel on Access.

[40] See Graves, *supra*.

result.[41] Another commenter stated that older persons' use and acceptance of these products would be affected by whether these systems meet their needs, the level of confidence older persons develop in the safety, security and financial soundness of these systems, government actions to assure minimum levels of consumer protection, and consumer education regarding these new technologies and their potential benefits.[42] This commenter also noted that some older persons will never accept e-money products.

Some industry commenters noted that e-money products will be useful for consumers without bank accounts, because such accounts are not required for these products.[43] An industry commenter added that e-money may result in a decreased reliance on check cashers and money order sellers and could potentially bring unbanked consumers into quasi-banking environments. This commenter added that the security against theft accorded by this technology may have the potential of bringing some merchants back into the inner city and LMI areas without adequate retail services.[44] Another industry commenter stated that nonbanks have been more active than banks in providing financial services to low-income persons, and thus may be better than depository institutions at meeting the needs of such consumers with respect to electronic money products.[45]

Several industry commenters noted that LMI consumers, because they use cash for a greater proportion of transactions than does any other segment of the population, are in many ways a target market for e-money issuers.[46] Additionally, several industry commenters noted that issuers will provide consumer education to help develop consumer confidence and market acceptance of their products, because they recognize these efforts to be necessary for e-money's success.[47]

---

[41] *See* Budnitz, *supra*.

[42] Remarks and Prepared Statement of Marcy Creque, Midwest Regional Volunteer Director, American Association of Retired Persons (AARP), Task Force Public Meeting (July 17, 1997), Panel on Access.

[43] Smith, Remarks, Panel on Consumer Protections and Disclosure, *supra*.

[44] *Id.*

[45] *See* Remarks of Ezra Levine, Howrey & Simon, representing the Association of Money Transmitters, Task Force Public Meeting (June 9, 1997), Panel on Issuer Financial Condition and Reliability.

[46] Remarks and Prepared Statement of Mark Plotkin, Covington and Burling, representing Mondex, Task Force Public Meeting (June 9, 1997), Panel on Consumer Protections and Disclosure.

[47] Remarks and Prepared Statement of Steven Zeisel, Consumer Bankers Association, Task Force Public Meeting (July 17, 1997), Panel on Access. *Also see*, Plotkin, Panel on Consumer Protections and Disclosures, *supra*; Smith, Panel on Consumer Protections and Disclosures, *supra.*

Many commenters noted that any discussion of consumers' access to e-money must also consider the consumer's base of knowledge, experience, and comfort level with such technologies and financial services generally. These commenters stressed that education and training in these new technologies is necessary to ensure that all consumers have effective access to new payment technologies.[48] Several commenters suggested that the risks and opportunities of e-money should be part of an ongoing curriculum to promote financial literacy targeted to inner city, rural, and Native American communities.[49] Other commenters stated that education efforts may help to equalize information about stored-value cards available to different segments of society.[50] Many commenters also suggested that the industry should work with community-based organizations to ensure that all consumers understand the risks and opportunities of e-money.[51]

Assessment of Consumer Concerns

Traditionally, new technologically advanced products are often introduced to the more affluent segments of society, and over time, as costs decline, they are offered to wider segments of society. For example, credit cards were offered initially only to affluent consumers. However, this pattern of market developments may not hold true for stored value cards.

Unlike other retail electronic payment products, e-money does not require a bank account or a credit relationship with the issuer — factors often limiting LMI consumers access to financial services. In addition, stored-value card systems are increasingly being viewed and marketed as a cash management solution for firms with high cash-handling fees or unique needs. For example, merchants with a high volume of low dollar value transactions are presently participating in pilot programs testing stored-value card products. In fact, some believe that such markets may be the likeliest area of initial success for e-money products. Accordingly, several issuers have joined with large franchise corporations, many of whose franchises are located in LMI communities, to offer a co-branded product for customer loyalty programs.[52]

Additionally, as suggested previously, several issuers have indicated that e-money is designed to be a cash substitute. Thus, a natural target market may be low- and moderate-income consumers,

---

[48] *See* Harshaw Remarks, *supra*; Graves, Remarks, *supra*.

[49] Harshaw, Remarks, *supra*.

[50] *See* Graves, Remarks, *supra*.

[51] *See*, e.g. Zeisel, Remarks, and Creque, Remarks, *supra*.

[52] For example, Mondex has licensed its product to Burger King to create a consumer loyalty program denominated in "burger bucks." *See* Antoinette Coulton and Jeffrey Kutler, *Smart Cards: Fast Food Trials May Point to Killer Card App*, 163 American Banker 15 (February 11, 1998). Similarly, Blockbuster Video has developed a stored value loyalty program and Kmart is offering stored value card gift certificates. Antoinette Coulton, *Incentives Field Moving to Card-Based Awards*, American Banker p. 16 (March 25, 1998).

the segment of the population that uses cash as a payment mechanism proportionally more than others. In this light, it is likely that e-money issuers will seek to provide stored value card products to this potential market.

Moreover, several state and federal government programs may also expand access to e-money products for LMI consumers. For example, the Financial Management Service is currently experimenting with several types of stored value card products to disburse salary payments to military personnel as well as for purchases at military facilities.[53] Moreover, the existence of state stored value pilot programs for needs-tested benefits may result in a great number of LMI consumers having access to and training in the use of these products before many other consumers.

Internet-based payment systems, however, may raise unique issues concerning consumer access to e-money products.[54] The Task Force recognizes, for example, that Internet-based payment systems currently require that consumers have access to and training in the use of personal computers and the Internet. These larger issues, however, are currently being addressed by other Administration initiatives. For example, the Commerce Department, through its National Telecommunications Information Agency ("NTIA"), is presently studying how to ensure that the benefits of technology, particularly the National Information Infrastructure ("NII", *i.e.*, Internet),

---

[53] FMS is currently operating five pilot programs: three with the U.S. Army at Fort Leonard Wood, Fort Knox, and Fort Sill, and two with the Department of Veterans Affairs at the Bronx and Tampa Medical Centers.

The Fort Leonard Wood pilot began on May 15, 1997, and replaced all cash payroll payments to basic training recruits with a VisaCash model disposable stored value card. These cards are preloaded, and trainees receive a card with their name printed on it.

The Fort Knox Pilot began in June 1997 and involves 10,000 disposable cards that were given to trainees. This program, using the PTI SmartCity transaction protocol, replaces check and money order payroll payments to trainees with a stored value card. Unlike the VisaCash program at Ft. Leonard Wood, this is not an open system but a closed, campus system and offers many product configurations. For example, PINs are being used at Fort Knox whereas VisaCash pilot programs do not support PINs.

The pilot at Fort Sill began on March 2, 1998, and, unlike the other two pilots, uses biometric fingerprint identification to authorize card transactions.

The Department of Veterans Affairs Bronx and Tampa Medical Centers pilots test both reloadable and disposable cards for employees, patients, volunteers, and visitors. The cards are using the VisaCash transaction protocol and can be used at all Veterans Canteen Service cafeteria, food shop, retail store, and vending machine locations throughout the medical center. Unlike the Army pilot programs, use of the cards is not mandatory, except for the replacement of meal tickets for volunteers and doctors. Half of the approximately 48,000 cards issued are disposable. In addition, this is the first pilot to test multi-application cards (combination ID badge and Visa electronic purse), Visa vending applications, cash-less ATMs (value loaded on ID badges), POS terminal integration with cash registers, and loyalty programs.

[54] However, considering the present trend toward a joint card-based Internet payment system, it is premature to determine whether access to Internet based e-money systems will be an issue for all consumers, separate and apart from access to stored value card systems.

are accessible to all consumers.[55] Additionally, President Clinton and Vice President Gore have announced the "Technology Literacy Challenge" to help ensure that all American students become "technology literate," *i.e.*, develop the computer skills necessary to improve learning, productivity and performance.[56]

Financial Literacy

Many commenters stressed that merely providing consumers access to e-money will not help ensure that all consumers will be able to enjoy whatever benefits are offered by these products. Some consumers may not be sufficiently knowledgeable about other payment methods and providers of such services to make an informed decision about which products and services best meet their needs. This lack of information could cause them to make decisions without adequately understanding how their decisions impact their rights and liabilities in different circumstances.

There are several governmental initiatives currently underway to promote financial literacy.[57]

---

[55] In 1995, the NTIA released a report entitled *Falling Through the Net: a Survey of the "Have Nots" in Rural and Urban America*, focusing on the impact that the current lack of telephone connections in LMI rural and urban communities will have on individuals' access to the Internet. The NTIA continues to explore how the government can assist in developing the physical infrastructure necessary to ensure all Americans have access to the Internet. In February 1998, the NTIA sponsored a conference, "Connecting All Americans for the 21st Century: Telecommunications Links in Low Income & Rural Communities," that continued focusing attention on the issue of how to ensure that all consumers have access to telecommunications technology.

[56] The four central goals of this challenge are: (1) All teachers in the nation will have the training and support they need to help students learn using computers and the information superhighway; (2) All teachers and students will have modern multimedia computers in their classroom; (3) Every classroom will be connected to the information superhighway; and (4) Effective software and on-line learning resources will be an integral part of every school's curriculum. The Department of Education is currently studying this issue and has proposed a plan for meeting this challenge in its report *Getting America's Students Ready for the 21st Century, Meeting the Technology Literacy Challenge*.

[57] Similarly, several other federal agencies have worked with community organizations to help promote financial literacy. For example, the Federal Reserve Board and the Federal Trade Commission are members of the Jump$tart Coalition for Personal Financial Literacy. Jump$tart's purpose is to evaluate the financial literacy of young adults; develop, disseminate, and encourage the use of guidelines for grades K-12; and promote the teaching of finance. The Jump$tart Coalition believes that all young adults need to have financial literacy to make informed financial decisions. The FDIC is organizing an educational campaign this year aimed at educating LMI consumers about financial services, the benefits of using insured depository institutions, and federal deposit insurance. The FDIC is also working with a coalition composed of the FMS, the Department of Agriculture's extension services, trade groups and nonprofit consumer organizations, to educate the public about basic financial services and the implications of EFT'99.

In addition, the OCC recently co-sponsored, with the Consumer Bankers Association, a forum on financial services access in the 21st Century to study why people do not have banking relationships and to consider what can be done to address the underlying problems. *See Financial Access in the 21st Century*, Proceedings of a Forum held February 11, 1997. The OCC will also conduct a survey later this year to determine why many LMI consumers do not use banks. *See* 63 Fed. Reg. 66718 (December 17, 1997). The OCC hopes that the information obtained from this

In connection with the implementation of EFT'99, the FMS has launched an extensive public education campaign to help persuade consumers to receive their federal payments electronically and to encourage payment recipients to establish accounts with depository institutions. FMS hopes, through these efforts, to maximize awareness of EFT'99 benefits and options and to increase the public's knowledge about the banking system and financial issues generally. This initiative should help consumers become informed about the range of available financial services and providers.[58]

Statutes Regarding Access to Financial Services

To help ensure that consumers have access to financial services, Congress enacted the Community Reinvestment Act of 1977 ("CRA").[59] The CRA requires federal financial regulatory agencies to consider, in reviewing certain merger and branching applications involving an insured depository institution, the institution's record of helping to meet the credit needs of its community, including LMI neighborhoods.[60] The federal financial institution regulatory agencies evaluate a depository institution's CRA performance by looking at its performance in making loans, investments, and services available in its community.[61] For example, the federal financial institution regulatory agencies evaluate an insured depository institution's record of helping to meet the needs of its assessment areas by analyzing both the availability and effectiveness of its system for delivering retail banking services and the extent and innovativeness of its community development services.[62] The provision of a basic electronic deposit account enabling LMI federal payment recipients to receive their payments via direct deposit is an example of a service that may receive positive CRA consideration.[63]

---

study will form the basis for future educational efforts and industry responses. *Id.*

[58] This education program may also help correct the widespread misunderstanding of state-needs tested benefit income thresholds often cited as a barrier to LMI consumers' maintaining a savings account. Studies have indicated that many benefit recipients underestimate the amount of savings that would make them ineligible for future needs-tested benefits. FMS expects to work with consumer and community-based organizations to ensure that all federal payment recipients receive this information.

[59] Community Reinvestment Act of 1977, 12 U.S.C. 2901 *et seq.*

[60] *Id.* Several states have also adopted their own CRA laws. These laws either establish additional statutory obligations or only require consideration of an institution's compliance with federal requirements in connection with state applications. In addition, both state and federal CRA requirements apply only to depository institutions.

[61] 12 C.F.R. 228.22-228.24.

[62] 12 C.F.R. 228.24(a).

[63] *See OCC Interpretive Letter No. 728* (June 18, 1996).

Additionally, several states have enacted basic banking or lifeline banking statutes to further promote consumers' access to basic financial services. These statutes usually require a depository institution to make a low-cost basic transaction account available to consumers.[64] Whether any of these state laws apply to e-money products offered by depository institutions is unclear at this time.

Conclusion

Many commenters expressed concern that e-money products will be available, at least on acceptable terms, only to affluent consumers. Several commenters were concerned that LMI consumers would not have effective access to e-money as they often do not have the same base of knowledge, experience, and comfort level with such technologies and financial services generally, as more affluent consumers.

Industry indicates that they intend to market e-money products to consumers at all economic levels. In addition, governmental initiatives also may help address consumer concerns by ensuring consumers have both access to and training in the use of new payment technologies.

The Task Force believes that financial literacy can help address access concerns. Therefore, the Task Force encourages financial literacy efforts by industry representatives and consumer organizations, in cooperation with the government, that address the use of technology in financial services. These efforts may include electronic money products, as this emerging industry matures over time.

[64] Some consumer organizations, however, believe that consumers should be guaranteed access to transaction accounts that offer a variety of services. *See* John P, Caskey, *Beyond the Cash-and-carry: Financial Savings, Financial Services, and Low-Income Households in Two Communities*, report written for the Consumer Federation of America and the Ford Foundation. October 1997.

PRIVACY

Consumers are becoming increasingly concerned about how personally identifiable information is being used. This concern, if unaddressed, could have the potential to act as an impediment to widespread consumer acceptance of e-money.

Summary of Comments

Several commenters stated that a significant barrier to the widespread usage of e-money will be lack of consumer trust or confidence in the privacy of the new payment systems. These commenters suggested that both fair information practices and anonymous payments will help build that trust.[65] Other commenters stated the belief that systems should be developed to ensure consumer privacy and security, rather than having to add privacy protections later in response to demonstrated problems. Several commenters stated that the appropriate role for government is to set basic privacy principles to guide businesses as they build consumer privacy and security into their systems.

Many commenters expressed concern that the increase in data collection efficiency associated with e-money could provide merchants and other system participants with an increased ability to obtain personally identifiable consumer information. Similarly, other commenters stated that the diversity, quality, and quantity of information that is collected and the fact that there are multiple places it can be captured and stored, increase the privacy concerns that could arise with electronic money.

Several commenters noted that the trend toward electronic money may eventually reduce a consumer's ability to use cash or other anonymous payment methods, whereas other commenters believed that the new technology could promote anonymous payment methods.[66] Similarly, several industry commenters noted that the use of encryption can enhance the technical security of products and provide greater privacy protection for consumers.[67]

---

[65] *See* Remarks and Prepared Statement of Mary J. Culnan, Commissioner, President's Commission on Critical Infrastructure Protection, Task Force Public Meeting (July 17, 1997), Panel on Privacy Issues.

[66] *See* Demonstration and Remarks of David Chaum, Founder and Chief Technology Officer, DigiCash, Task Force Public Meeting (July 17, 1997), Panel on Privacy Issues.

[67] Remarks and Prepared Statement of Paul Lampru, Strategic Marketing, VeriFone, Task Force Public Meeting (July 17, 1997), Panel on Security Issues; Remarks and Prepared Statement of Elliot C. McEntee, President and CEO, National Automated Clearing House Association (NACHA), Task Force Public Meeting (July 17, 1997), Panel on Security Issues; Remarks and Prepared Statement of Russell B. Stevensen, Jr., General Counsel, CyberCash, Task Force Public Meeting (July 17, 1997), Panel on Security Issues; and Demonstration and Prepared Statement of Thomas Smedinghoff, Esq., McBride, Baker, & Coles, Task Force Public Meeting (July 17, 1997), Panel on Security Issues.

Some commenters noted that the number of parties involved in new payment methods, including issuers, distributors and processors, could result in more people having access to consumer information. Other commenters noted that the potential for privacy invasions may be greater as cards become multifunctional because more information could be collected and stored in one place.

Many commenters were also concerned that consumers may not receive adequate disclosure of what personal data is being collected, who will receive that data, and how the data will be used.[68] Some commenters worried that information consumers voluntarily reveal to the issuer and information about their transactions with merchants would be transferred to the issuer's affiliates and to other parties.[69] Several commenters asserted that self-regulatory actions, such as industry guidelines and privacy policies, do not provide any meaningful protections for consumers because they are largely unenforceable. Additionally, some commenters were concerned that the personal information collected through these new electronic payment methods may not be secure from illegal or unauthorized access and use.

Other commenters stated that most consumers do not understand and will not be informed of the privacy implications of choosing different payment methods. These commenters stressed that there must be significant efforts to educate the public about information security and to seek fair information practices. Some commenters suggested that the government should work with consumer organizations to help educate consumers about privacy considerations related to e-money. Other commenters suggested that the government should establish model disclosures and vocabulary to help consumers understand these products.

Several commenters expressed concerns that e-money would give the government greater access to consumers' financial information by eliminating their ability to make payments anonymously. These commenters noted that consumers may believe that auditable e-money systems will increase the government's ability to gain access to financial information.

Industry commenters expressed the belief that it is premature to prescribe a particular form of consumer disclosure about privacy, particularly when stored value products are in such an early stage of development and implementation.[70] These industry commenters also stated that they currently require their third party servicers or contractors to agree to provisions limiting their use

---

[68] Remarks and Prepared Statement of Dierdre K. Mulligan, Staff Counsel, Center for Democracy and Technology, Task Force Public Meeting (July 17, 1997), Panel on Privacy Issues (expressing the view that most e-money issuers presently do not provide adequate disclosures).

[69] *See* Culnan Remarks and Statement, *supra*. *See also* Mulligan Remarks and Remarks and Prepared Statement of Susan Grant, Vice President for Public Policy, National Consumers League, Task Force Public Meeting (July 17, 1997), Panel on Privacy Issues.

[70] *See* Remarks and Prepared Statement of Janet Koehler, Senior Manager, AT&T Universal Card Services, on behalf of SmartCard Forum, Task Force Public Meeting (July 17, 1997), Panel on Privacy Issues.

of information.[71] Several commenters also noted that statutory and common law restricts third party access to many types of information.[72] Some commenters noted that they currently provide consumers with general information about what information is being collected and the use of that information.[73]

Representatives of law enforcement expressed concerns that some of the new payment methods will diminish the government's ability to identify participants in financial transactions. These commenters stated that the use of encryption in e-money systems might make it more difficult for law enforcement authorities to identify, apprehend, and prosecute criminals who use encryption systems to facilitate money-laundering and counterfeiting.[74] These commenters also stressed that existing constitutional and statutory provisions place many restrictions on governmental access to confidential information. Other commenters noted that requiring that e-money issuers maintain detailed transaction records to facilitate law enforcement could chill product innovation and increase issuer costs, possibly hindering market acceptance of new payment products.[75]

Assessment of Consumer Concerns

Consumer concerns about the privacy of their financial information extend beyond privacy in e-money transactions, and are varied and complex. Some consumers are extremely protective of their privacy and view any collection or use of personally identifiable information as an intrusion, while others are far less concerned about privacy-related matters. Although consumers' privacy thresholds are not uniform, consumers generally share certain key privacy concerns. First, consumers want to receive adequate information about an entity's information collection and use policies. Consumers also appear to be concerned about secondary use of information — the use of information for purposes other than the original transaction, either by the information collector or by a third-party to whom the information is sold or transferred (*e.g.*, a third party processor).[76]

---

[71] *See* Remarks and Prepared Statement of Marcia Z. Sullivan, Director of Government Relations, Consumer Bankers Association, Task Force Public Meeting (July 17, 1997), Panel on Privacy Issues.

[72] *See* Remarks and Prepared Statement of Peter Toren, Trial Attorney, Computer Crime and Intellectual Property Section, Department of Justice, Task Force Public Meeting (July 17, 1997), Panel on Security Issues.

[73] *See* Koehler Statement and Remarks, Sullivan Statement and Remarks, *supra*.

[74] On the other hand, encryption techniques can also serve as a deterrent to counterfeiting and other criminal attacks on e-money systems. *See* Security of Electronic Money, BIS, 1996.

[75] *See* Remarks and Prepared Statement of Pamela J. Johnson, Counselor to the Director, Department of the Treasury, Financial Crimes Enforcement Network (FinCEN), Task Force Public Meeting (July 17, 1997), Panel on Privacy Issues and Toren, Statement and Remarks, *supra*.

[76] Some commenters noted that consumers are less concerned about primary uses of information because consumers may, in effect, bargain to a desired privacy outcome by either paying a "premium" for fair information

The potential for privacy intrusions seems to be at its greatest in these cases, where consumers may not be aware that their personal information is being put to new uses or have any control over those uses.[77] Obtaining knowledge of an issuer's information use policies would allow consumers choice, *i.e.*, so that they can make an informed decision about what e-money product is appropriate for their privacy needs. Additionally, disclosures could provide consumers with rights of redress should the issuer misuse their personal information in a way that is inconsistent with the disclosures or violated public policy.[78]

Privacy Protections in Law

Existing laws may limit access to, and use of, consumers' e-money information by issuers and third parties. However, unlike the nations of Western Europe, the United States does not have universal or omnibus privacy laws.[79] A consumer's right to *financial* privacy has not been established as a fundamental right by the United States Supreme Court.[80] Privacy protections in

---

practices addressing notice, choice, access, verification, and remedy or look for benefits in exchange for allowing a vendor to collect and use information. *See* Remarks and Prepared Statement of Marc Rotenberg, Director, Electronic Privacy Information Center, Task Force Public Meeting (July 17, 1997), Panel on Privacy Issues.

[77] This latter element — control over how information is put to use — appears to be especially important. Mary Culnan of Georgetown University argues that business practices are less likely to appear invasive when the consumer has a relationship with the business, only relevant information is collected, and the consumer is able to control the use of the information. Culnan, Mary J., *How Did They Get My Name: An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use,* MIS Quarterly, Vol. 17, No. 3, September 1993, pp. 341-363. Even consumers who do not object to how the information is put to use raise privacy objections if they have no control over secondary use. Culnan, Mary J. and Pamela K. Armstrong, *Information Privacy Concerns and Procedural Fairness: An Empirical Investigation,* Paper presented at INFORMS National Meeting, May 1996.

[78] The Federal Trade Commission has studied online privacy issues since 1995. Through a series of public meetings convened as part of the Bureau of Consumer Protection's Consumer Privacy Initiative, the FTC has received extensive commentary on consumers' concerns regarding these issues. The testimony presented at these meetings demonstrates that consumers care deeply about the security and confidentiality of their personal information in the online environment. Of all the information that businesses collect about them, consumers are especially troubled by the potential for unauthorized disclosure of their financial information. Federal Trade Commission, *Staff Report: Consumer Privacy on the Global Information Infrastructure,* 12 (1996).

Research presented at the Commission's 1997 public workshop on Consumer Information Privacy shows that consumers have much less confidence in online companies with respect to the handling of their personal information than they have in many other institutions -- including banks -- doing business offline. Louis Harris & Associates and Alan F. Westin, *Commerce, Communication, and Privacy Online: A National Survey of Computer Users,* ix (conducted for *Privacy & American Business* 1997).

[79] *See* Fred Cate, Privacy in the Information Age (Brookings Institute 1997).

[80] For example, the U.S. Supreme Court has not considered whether the implied right of personal privacy extends to personal financial records. The Supreme Court has held, in the context of the Fourth Amendment, that no "reasonable expectation of privacy" exists in the bank records of individuals and that a bank customer "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the government." *United States v.*

the United States, have evolved on a sectoral basis (applying to certain sectors of society, *e.g.*, banking industry or the public sector), reflecting in part how federal and state legislatures address competing policy objectives, including the prevention and prosecution of criminal acts. This report discusses several existing privacy laws that may or may not apply to e-money.

Laws Requiring Disclosure of Privacy Practices

Many commenters expressed concern that consumers would not receive adequate information about an issuer's information practices. Some issuers will provide these disclosures, in an effort to distinguish their products from those of their competitors; however, market incentives may be insufficient to ensure that all consumers receive disclosures about an issuer's information policies. Moreover, existing legal requirements for disclosure of information policies may be inapplicable to most forms of e-money presently in the marketplace.[81]

The Electronic Fund Transfer Act ("EFTA") and its implementing regulation, the Federal Reserve Board's Regulation E, establish the rights and liabilities of consumers who maintain an account[82] at a financial institution and use electronic funds transfers ("EFTs") into or out of the account.[83] Among other things, Regulation E requires financial institutions to document EFTs in writing and to disclose certain information to their customers.[84] Among the disclosures financial institutions must provide to consumers is a description of the circumstances in the institution's "ordinary course of business" in which it will disclose information about the consumer's account to third parties.[85] As discussed in greater detail in the Consumer Protections and Disclosures section of

---

Miller, 425 U.S. 435 (1976).

However, several state courts have found that a reasonable expectation of privacy exists in financial records. *See* e.g., *Charnes v. DiGiacomo*, 612 P.2d 1117 (Colo. 1980); *People v. Jackson*, 452 N.E.2d 85 (Ill. App. Ct. 1983); *Commonwealth v. DeJohn*, 403 A.2d 1283 (Pa. 1983); *Utah v. Thompson*, 810 P.2d 415 (Utah 1991).

[81] This brief survey of U.S. privacy laws is specifically limited to the nascent electronic money product. It would be inappropriate to apply this survey to assess the level of privacy protection in broader or more established financial services.

[82] An "account" for the purposes of the EFTA is defined as a demand deposit, savings deposit, or other consumer asset account held directly or indirectly by a financial institution, for personal, family, or household purposes. 15 U.S.C. 1693a(2); 12 C.F.R. 205.2(b)(1).

[83] Several states also have EFT laws requiring privacy-related disclosures. These laws either (1) require only that a financial institution disclose its electronic funds transfer information policies or (2) specifically create confidentiality obligations with respect to EFT transfers. *See, e.g.*, Ill. Ann. Stat. Ch. 17, 44(a)(9) (1981) (mandating disclosure of EFT information policies); Mich. Comp. Laws. Ann. 488.12 (1987); Minn. Stat. Ann. 47.49 (1988); NM Stat. Ann. 58-16-12 (Supp. 1984)(creating confidentiality requirements).

[84] *Id.* 1693d.

[85] *Id.* 1693c(a)(9); 12 C.F.R. 205.7(a)(9).

this Report, however, the Federal Reserve Board has not yet determined to what extent, if any, Regulation E applies to e-money systems.

Laws Limiting Access to Consumer Information

Under the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. 1681 *et seq*, a "consumer reporting agency" may furnish a "consumer report" only to a third party who has a "permissible purpose" for using the information.[86] The FCRA enumerates the permissible purposes for obtaining a consumer report, including: where the consumer has given his or her written permission; in connection with a credit transaction or insurance underwriting; for employment purposes; and, if there is a legitimate business need, in connection with a business transaction initiated by the consumer. Information solely about transactions or experiences between a consumer and an entity, however, may be shared generally by the entity.[87]

Recent amendments to the FCRA expand the scope of permissible information-sharing among affiliates. Affiliated persons and entities are now permitted to share and use consumer information — including consumer reports — among themselves without becoming consumer reporting agencies subject to the FCRA, provided the consumer receives notice and an opportunity before the consumer's information is shared to direct that the information not be shared ("opt-out").[88]

Businesses may communicate their own transactional information about a consumer to a consumer reporting agency without notice to the consumer. To ensure the accuracy of this information, however, the FCRA amendments require that persons who furnish information to a consumer reporting agency avoid furnishing knowingly inaccurate information, correct and update information reported, and notify the consumer reporting agency of disputes and account closures.[89]

---

[86] A "consumer reporting agency" is defined as any person who regularly assembles or evaluates consumer information for the purpose of furnishing consumer reports to third parties. *Id.* 1681a(f). A "consumer report" is any communication, by a "consumer reporting agency," of any information that bears on a consumer's credit-worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living that is collected or used (or expected to be used) as a in factor establishing the consumer's eligibility for credit, insurance, employment, or any other purpose permissible under the Act. *Id.* 1681a(d)(1).

[87] This is because reports containing information solely about transactions or experiences between the consumer and the entity making the report are not "consumer reports" for purposes of the FCRA. *Id.* 1681a (d)(2)(A)(i), 1681a(f).

[88] *Id.* 1681a(d)(2)(A)(iii) (as amended by Pub. L. No. 104-208, tit. II, ch. 1, 2402(e)). The notice and opt-out requirements do not apply to the sharing of pure identification information, such as names and addresses, or "experience" information, which relates solely to an entity's own transactions or experiences with the customer.

[89] *Id.* 1681s-2 (as added by Pub. L. 104-208, tit. II, ch. 1, 2413(a)(2)). Several states have fair credit reporting laws that mirror the general scheme of the federal FCRA. Some of these laws provide stricter penalties, greater

It is uncertain whether consumer's e-money transaction information would fall under the protection of the FCRA for several reasons. First, e-money issuers may not be considered "consumer reporting agencies." Second, the data collected -- information on the consumer's spending patterns -- may not fall within the definition of a "consumer report," for example, if the information is considered to be experience information. However, e-money issuers that provided information to a consumer reporting agency would be subject to the requirements of the FCRA regarding furnishers, discussed above.

Laws Restricting Governmental Access to Information

Several federal statutes may limit the government's access to consumers' e-money information. The Privacy Act of 1974 ("Privacy Act") controls the federal government's collection, use, and disclosure of information on individuals. It does not apply to state government agencies or the private sector.[90] A federal agency may collect "only such information about an individual as is relevant and necessary" to accomplish a required agency function and the agency must provide a Privacy Act statement to each individual asked to supply information.[91] The Privacy Act prohibits, with limited exceptions, a federal agency from disclosing any such record to any person or to another agency unless the individual to whom the record pertains has either requested the disclosure or consented to it in writing.[92]

The Right to Financial Privacy Act ("RFPA") prohibits the federal government from accessing or obtaining information in a customer's financial records from a financial institution, and prohibits a financial institution from disclosing such information to the federal government, except pursuant to the customer's authorization, an administrative subpoena or summons, a search warrant, a

---

consumer rights to access, and more generous error correction procedures, as well as permit information sharing with affiliates. Cal. Civ. Code 1785.3(c). State fair credit reporting laws generally impose requirements on users of consumer reports similar to the FCRA. However, the revised FCRA preempts most state laws or regulations governing information sharing and use among affiliated companies whether limited to credit reporting or not. Most federal preemption provisions sunset on January 1, 2004. 15 U.S.C. 1681t(b)(2). State laws that were preempted by the FCRA do not automatically return in force after the sunset date. Each state must enact new legislation. 15 U.S.C. 1681t (d).

[90] The Privacy Act established a Privacy Protection Study Commission to study the data systems of governmental, regional, and private organizations and to make recommendations for the protection of personal information. *See* Pub. L. No. 93-579, 5 (amended June 1, 1977). The Commission's report, issued in 1977, recommended protection of individual records maintained by private sector record keepers in its provision of telecommunication services, but Congress has never done so. Privacy Protection Study Commission, Personal Privacy in an Information Society (USGPO Stock No. 052-003-00395-3) (1977).

[91] 5 U.S.C. 552a(e)(1) and (3). The Privacy Act applies only to personal information within "records" contained in a "system of records," as these terms are defined by the Act. *Id*. 552a(a)(4) and (5).

[92] *Id.* 552a(b). An individual may access and copy any information pertaining to himself that is maintained in an agency's system of records. *Id.* 552a(d).

judicial subpoena, or a formal written request.[93] The RFPA defines a "financial institution" as any office of a bank, savings bank, credit card issuer, industrial loan company, trust company, savings association, building and loan, homestead association, credit union, or consumer finance institution.[94] The RFPA only covers "financial records," defined to include "information known to have been derived from" a record pertaining to a customer's relationship with a financial institution.[95]

It is uncertain whether the RFPA would apply to a consumer's e-money transaction information for several reasons. First, the scope of institutions subject to the RFPA is limited, although many current e-money issuers would most likely fall within the RFPA's definition of "financial institutions."[96] Second, a consumer's e-money transaction information may not, in all instances, be considered to be a "financial record" relating to an "account" for purposes of the RFPA.

Although the U.S. has various sectoral privacy laws protecting some consumer financial information, it is uncertain whether these protections would extend to e-money. Accordingly, existing laws may not address consumer concerns about the collection and use of their e-money information, require issuers to disclose how information will be collected and used, provide consumers with the ability to control whether unaffiliated third parties can obtain the information, or generally limit government access to the information. In sum, it is uncertain and untested whether consumer concerns about privacy in e-money transactions are addressed by existing law.

---

[93] 12 U.S.C. 3404 - 3408. The government generally must notify the customer of the nature of the law enforcement inquiry and give the customer an opportunity to challenge the access *prior* to accessing a customer's records. *Id.* 3405-3408. The government generally must notify the customer of the nature of the law enforcement inquiry and give the customer an opportunity to challenge the access *prior* to accessing a customer's records. *Id.* 3405-3408.

Many states also have financial privacy laws that impose similar restrictions to the federal RFPA, often only regulating disclosures to governmental agencies. Cal. Gov't Code 7460-7493 (1995 & 1997 Supp.); Nev. Rev. Stat. Ann. 239A.010-239A.190 (1996); N.H. Rev. Stat. Ann. ch. 359-C (1984 & 1996 Supp.); Or. Rev. Stat. 192.550-595 (1995). Other states have broader statutes that prohibit disclosures to "any person," which implies that private entities are also covered. *E.g.*, Conn. Gen. Stat. Ann. 36a-42 (1996); Me. Rev. Stat. Ann. tit. 9-B 162 (1997); Md. Ann. Code 1-302 (1996 Supp.). The types of financial institutions and records regulated by states also differs from the federal RFPA, ranging from only state-regulated financial institutions and financial records to any corporation organized under the state or federal law and any confidential information, financial or otherwise. *E.g.*, Nev. Rev. Stat. Ann. 239A.030 (1996) and Neb. Rev. Stat. 8-1401 (1996 Supp.). State laws, however, may more readily apply to e-money issuers and products. This is largely because some state financial privacy laws apply to both depository institutions and nonbanks and have more expansive financial definitions of "financial records." Overall, although a few states' laws may apply in this context, the majority may not.

[94] 12 U.S.C. 3401(1).

[95] *Id.* 3401(2).

[96] Issuers which do not otherwise fall within the definition of "financial institution," would probably not be considered a "financial institution" for the purposes of the RFPA based on their e-money activities alone. *See* 12 U.S.C. 3401(1).

Security of Consumers' Transaction Information

Federal laws prohibiting unauthorized access to electronic communications may be applicable to the security of e-money payment information.[97] The Electronic Communications Privacy Act ("ECPA") prohibits the unauthorized access or use of any facility through which an electronic communication service is provided or to intentionally exceed the authorization for accessing that facility.[98] "Electronic communications" is defined broadly and includes any transfer of signs, signals, writing, images, sounds, or intelligence of any nature transmitted by a wire, or electromagnetic or photo-electronic system, except electronic funds transfer information stored by a financial institution.[99] The ECPA also prohibits any person or entity from knowingly divulging to any person or entity the contents of an electronic communication while that communication is in transmission or in electronic storage.[100]

Again, it is unclear whether a consumer's e-money transaction information would fall within the ECPA's prohibition against disclosing electronic communications in transmission or storage.

Industry Responses

Information on consumers and their preferences has important economic value to businesses and consumers. It can help businesses better allocate their resources, improve product quality, and assist consumers in product and service choice. Information can aid firms in the design and delivery of products and services, in marketing, and in inventory control.

---

[97] Several states have also criminalized unauthorized access to electronic communications. *See, e.g.* N.J. S.A. 17:16K-2.

[98] 18 U.S.C. 2520. Although "electronic funds transfers" are exempt from the scope of the ECPA, it is unclear whether e-money products would be "electronic funds transfers."

[99] 18 U.S.C. 2510 (12). "Electronic communication system" is defined as any wire, electromagnetic, or photoelectric facilities for the transmission of electronic communications and any computer facilities or related electronic equipment for the electronic storage of such communications. 18 U.S.C. 2510(14).

[100] 18 U.S.C. 2701(a)(1). *Also see* S. Rep. No. 99 -541, 99th Cong., 2d Sess. 1, 37 (1986). "Electronic storage" means (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication. 18 U.S.C. 2510(17).

There are several exceptions to the ECPA's general prohibition on disclosure. These include: disclosure to the addressees or intended recipients of the communication or their authorized agents; in response to a court order; and with the lawful consent of the sender, addressee, or intended recipient of such communication. 18 U.S.C. 2702(b)(1)-(4). Information may also be released to law enforcement agencies if the contents were inadvertently obtained by the communication service provider and the information pertains to the commission of a crime. 18 U.S.C. 2702(b)(6). However, none of these provisions is intended to affect any other provision of federal law that prohibits disclosure of information on the basis of the content of that information, such as the FCRA.

Although some information, such as mailing lists or product purchase patterns, has always been used for marketing purposes, technological advances of recent years have made that information easier to develop and cheaper to replicate.[101] Consequently, firms are able to make better use of existing information and to lower the costs of developing new information sources. Information resources can also generate their own independent source of revenue when replicated, sorted, and sold. In some cases, the revenue from direct sale of information might make the provision of primary services profitable. The development and use of consumers' information, however, also raises important questions about consumers' privacy.

The heightened public debate in recent years about privacy and electronic technology has begun to make financial industry participants more sensitive to issues surrounding the collection and dissemination of customer information. As in the financial services sector more generally, industry responses that could be relevant to e-money are continuing to evolve. For example, many products can be purchased on an anonymous basis, such as through vending machines. Similarly, the development of more anonymous e-money products is, itself, one market response that has the potential to provide consumers with new ways to enhance their privacy in financial transactions. Industry responses based on new, more anonymous technologies may be constrained, however, by law enforcement concerns, which may constitute a significant barrier to the development of electronic money products with greater protections. Although it is too early to tell how many e-money products will ultimately develop, it is likely that more anonymous products will emerge if there is consumer demand for the products and law enforcement concerns can be accommodated. For example, consumer preferences might emerge for anonymous small dollar payments, which would not infringe on the important interests of government agencies to review suspicious large dollar transactions.

Current e-money technology is capable of delivering products with varying effects on privacy, ranging from fully anonymous, cash-like systems, in which no personally identifiable transaction records are created, to fully auditable systems that can identify and store every transaction conducted by every consumer. As the technology evolves, new products will be developed. The extent to which new products will incorporate privacy protections will be influenced by several factors, including consumer preferences, law enforcement needs, and industry perceptions of the value of information.

Consumers with a high degree of concern about the privacy of their transactions will likely favor cash or other cash-like payment products that preserve their anonymity. Other consumers are willing to surrender a degree of privacy in their consumer transactions in order to obtain consumer benefits available with auditable systems, such as convenience, error resolution,

[101] *See* Lawrence J. Redecki, John Wenninger and Daniel K. Orlow, *Industry Structure: Electronic Delivery's Potential Effects on Retail Banking*, 19 Journal of Retail Banking Services 57 (Winter 1997).

recovery of value for lost cards, purchase protection, and loyalty program awards.[102] The majority of stored value systems in existence today involve some trade-off between these types of consumer benefits and privacy. Some e-money issuers claim that it is possible to combine some consumer benefits of an auditable system with the anonymity of a cash-like system, decreasing the need for this trade-off.[103]

At the present time, whether consumers will demand e-money products that protect their privacy is uncertain. How widespread the existence of privacy protections will become may depend on the extent to which consumers tend to prefer products that offer these protections. Given the strong competing pressures from cash and other payment methods, issuers are more likely to face pressures to provide privacy protections, especially as consumer awareness over information collection and use rises and consumers increasingly seek such protections.[104] Issuers in such an environment might see offering privacy protection as a way to differentiate their product, competing for customers on the basis of the privacy protections offered.[105] Similarly, some issuers may then create a product for which consumers would, in effect, pay a premium in exchange for additional privacy protections. While there is reliable evidence that consumers are reluctant to commit to electronic commerce and e-money because of privacy concerns, a clear market demand for this "privacy premium" product has yet to emerge. Consumers that are not particularly concerned about the confidentiality of their purchases may not demand privacy protections or information about disclosure policies, as is currently the case for credit cards and similar payment vehicles.

Market developments may in some respects address consumer concerns about privacy. Moreover, even if individual consumers do not demand specific protections — due to lack of

---

[102] *See* Laufer, R.S. and M. Wolfe, *Privacy as a Concept and a Social Issue: A Multidimensional Development Theory*, Journal of Social Issues (33:3), Summer 1977, pp. 22-42. Note, however, that even if consumers recognize the benefits of surrendering some privacy, privacy concerns can still arise if consumers are not aware that information is being collected and if more information is gathered than the transaction and associated protections required.

Alan Westin demonstrated this point by constructing a "willingness to trade-off" index, which measures an individual's willingness to trade consumer benefits for a relaxation of privacy interests. Westin, A.F., *Domestic and International Data Protection Issues*, Testimony before the Subcommittee on Government Information, Justice, and Agriculture, Committee on Government Relations, U.S. House of Representatives, U.S. GPO, WDC: 1991, pp. 54-68.

[103] One product developer, DigiCash, claims already to have done this.

[104] In markets without such competition, the incentives to provide privacy protections may not be as great. Lack of consumer awareness that information collection is taking place, or the absence of viable substitutes available to consumers for the service provided, could dampen private incentives to respond to privacy concerns of individuals.

[105] Although issuers, who market their product based on its privacy protections will disclose their information practices or other privacy-enhancing features, many others may not. In the latter cases, consumers will have to make judgements about whether to use the product, as they do with other payment methods today.

knowledge or otherwise — implementation of privacy protections by individual firms could increase consumer confidence overall and thereby foster development of the e-money market.

In addition, many financial industry participants, either individually or as part of industry groups, are exploring self-regulatory responses to consumer privacy concerns in the financial services industry more generally. As described more fully below, several groups have voluntarily established privacy policies or codes of fair information practices. Also, several industry groups are considering developing "Acceptance" or "Privacy" marks.[106]

- The SmartCard Forum's[107] Privacy Guidelines encourage their members to: respect the privacy expectations of consumers; ensure that the data are as current, accurate, and complete as possible; promptly honor consumers' requests for information that a company has about them; enable consumers to correct inaccurate personally identifiable information; limit the use, collection, and retention of customer information; and apply appropriate security measures to protect consumer data. The SmartCard Forum principles also encourage their members to provide consumers the opportunity to opt-out before personally identifiable consumer information is to be provided to unaffiliated third parties for marketing or similar purposes. Third parties receiving the information from SmartCard members are encouraged to adhere to equivalent privacy standards with respect to that information. Similarly, the guidelines suggest that service providers should implement policies and procedures to limit employee access to personally identifiable consumer information on a need-to-know basis, educate employees about the privacy guidelines and their responsibilities under the guidelines, and monitor employee compliance, taking appropriate disciplinary action where appropriate.[108]

- In September 1997, the American Bankers Association ("ABA"), The Bankers Roundtable and its division, the Bank Information Technology Secretariat ("BITS"), the Consumer Bankers Association (CBA), and the Independent Bankers Association of America ("IBAA"), endorsed a common set of privacy principles ("Banking Industry Principles"). These principles provide that subscribing financial institutions should:

  > (1) recognize a consumer's expectation of privacy by making available privacy guidelines and/or providing a series of questions and answers about financial privacy to their customers;

---

[106] See Koehler Statement, *supra*.

[107] The Smart Card Forum was formed in 1993 to promote the widespread acceptance of smart cards that support multiple applications. Bringing together representatives from technology companies, the financial services industry and other interested parties from the public and private sector, the Forum participants focus on issues to advance interoperability across industries and applications. Currently, over 230 corporate and government entities from the U.S., Canada, South America and Europe are members of the Smart Card Forum.

[108] Smart Card Forum Privacy Guidelines.

(2) only collect, retain and use individual customer information where it would be useful (and allowed by law) to administer that organization's business and to provide products, services, and other opportunities to its customers;

(3) establish procedures to ensure customer information is accurate, current, and complete in accordance with reasonable commercial standards, including responding to requests to correct inaccuracies in a timely manner;

(4) limit employee access to personally identifiable information to those with a business reason for knowing such information, educate employees so that they will understand the importance of confidentiality and customer privacy, and take appropriate disciplinary measures to enforce employee privacy responsibilities;

(5) maintain appropriate security standards and procedures regarding unauthorized access to customer information;

(6) not reveal specific information about customer accounts or other personally identifiable information to unaffiliated third parties for their independent use, except for the exchange of information with reputable information reporting agencies to maximize the accuracy and security of such information or in the performance of bona fide corporate due diligence, unless 1) the information is provided to help complete a customer-initiated transaction, 2) the customer requests it, 3) the disclosure is required by/or allowed by law (*e.g.*, subpoena, investigation of fraudulent activity) or 4) the customer has been informed about the possibility of such disclosure for marketing or similar purposes through a prior communication and is given the opportunity to decline (*i.e.*, "opt-out");

(7) if personally identifiable information is given to a third party, the financial institution should insist that the third party adhere to similar privacy principles that provide for keeping such information confidential;

(8) devise methods of providing a customer with an understanding of their privacy principles.[109]

In conjunction with the privacy principles, BITS is in the process of developing a plan for implementing the principles. Thus far, the BITS Board of Directors, made up of the Chairs of the largest banks in the United States, as well as representatives of the ABA, IBAA, and Bankers Roundtable, have approved and endorsed the "Privacy Principles Implementation Plan." This plan states that: a plan for implementing the privacy principles will be approved at the level of the Board of Directors or the Office of the Chair of the bank; bank policies related to customer

[109] Banking Industry Principles.

privacy will be communicated to bank customers; employees will be informed and educated about the bank's plan to implement the privacy principles; banks will obtain agreements from third-party vendors on a case-by-case basis to comply with the bank's privacy principles; where a bank provides information to unaffiliated third parties for their independent use for marketing or similar purposes, the bank will notify customers of their right to opt-out from the information sharing; banks will establish and maintain procedures by which customers can correct inaccurate information, and banks will establish internal policies to ensure compliance with and to address breaches of a bank's privacy policy.[110]

These principles are more likely to address consumers' privacy concerns in a meaningful and effective manner if they involve a means to assure adherence by industry participants.

Certain industry self-regulatory initiatives include a compliance assurance mechanism. For example, the members of the Individual Reference Services Group ("IRSG") have agreed to self-regulatory principles that require an annual review by a "reasonably qualified independent professional service" to assess whether the reference service is in compliance with the IRSG's principles.[111] The results of this review must be made public. Also signatories to the principles have agreed only to sell information to reference service companies in compliance with the principles.[112]

Separately, a company's failure to honor its own stated privacy policy may also constitute a deceptive practice prohibited by the Federal Trade Commission Act ("FTCA") and state law. Section 5 of the Federal Trade Commission Act prohibits any person or corporation from engaging in unfair and deceptive acts or practices in or affecting commerce.[113]

Even if any industry self-regulatory policies are not implemented through a formal mechanism for enforcement, the interplay of these practices with existing law may result in certain remedies being available to consumers.

---

[110] *Id*.

[111] The FTC, in its Report on Individual Reference Services, discussed the pros and cons of the IRSG self-regulatory initiative. *Individual Reference Services: A Report to Congress*, December 1997.

[112] The FTC criticized the IRSG principles for not giving consumers access to the public information maintained about them and disseminated by the reference services. Under the IRSG principals, consumers thus would not be able to check for inaccuracies in information resulting from transcription or other errors that occur in the process of obtaining or compiling such information. *Id.*

[113] 15 U.S.C. 45(a)(i). Under Section 5 of the Federal Trade Commission Act, deception occurs if "there is a representation, omission or practice that is likely to mislead the consumer, acting reasonably in the circumstances, to the consumer's detriment." *Cliffdale Associates, Inc.*, 103 F.T.C. 110 (1994).

First, a court may find that the consumer's reliance on an issuer's stated privacy policy gave rise to a contractual relationship between the consumer and the issuer concerning the terms of the privacy policy. Thus, the issuer's failure to follow the terms of the policy statement could constitute a breach of contract.[114] Second, a consumer may argue that the issuer's failure to follow its privacy statement was a breach of warranty.[115] Third, consumers may have actions in tort for negligent misrepresentation.[116]

Review of Existing Self-Regulatory Policies

Both the SmartCard Forum guidelines and the Banking Industry Principles appear to generally address many consumer privacy concerns. It remains to be seen, however, whether they will be sufficient to address the concerns expressed to the Task Force. Each set of guidelines appears to encourage practices that address certain concerns about the collection and use of information. However, neither set has yet developed a formal means to assure adherence by participants or other members of industry. The lack of a means to assure adherence may limit the effectiveness of these guidelines.

Conclusion

---

[114] The general doctrine of implied contract may also offer some, albeit limited, protections through an implied contract of confidentiality. As applied to financial privacy, a depository institution can be said to have an implied contract with its customers to keep their financial affairs confidential. Although several state courts have found such an implied contract in a financial institution's relationship with its customers, there is no uniformity among state courts in the doctrine. *E.g., Peterson v. Idaho First Nat'l Bank*, 367 P.2d 284 (Idaho 1961) (Bank liable for unauthorized disclosure of customer's ledger record to customer's employer). Many cases upholding such an implied contract involved disclosure of information in connection with investigations of alleged violations of law, rather than in connection with marketing or other ordinary business transactions. Whether this theory provides any meaningful protection for consumers is uncertain as a financial institution may expressly negate any duty of confidentiality in its contract. Because consumers are told of the issuer's disclosure practices, the consumer may also be construed to have given implicit consent to any uses set forth in the agreement. This implicit consent may be converted to express consent if the issuer adds appropriate language to the EFT service contract and disclosure. Law of Electronic Funds Transfer, Donald I. Baker, Roland E. Brandel ¶ 19.02[2][a]. However, if the consumer relied on these privacy statements to the consumer's detriment the issuer may be estopped from withdrawing or altering the promise it made to the consumer.

[115] Warranties are assurances by one party to a contract of the existence of a fact upon which the other party may rely, which, if untrue, may give rise to an action for breach of contract and damages. In such instances, the consumer could argue that statements made by the issuer in the privacy statement were untrue.

The Magnuson Moss Warranty Act, 15 U.S.C. 2301 *et seq.* may also be applicable if e-money were found to be a product, rather than a service as it is generally viewed at present.

[116] Negligent misrepresentation usually requires a material misrepresentation made by a party who had a duty to provide accurate information to the party requesting the information, who suffered injury as a result of the misrepresentation. Parties who in the course of their business supply false information for the guidance of others in their business transactions may be subject to liability for pecuniary loss caused by justified reliance on the information if they did not use reasonable care when making the representation. Restatement (second) of Torts 552. In the case of e-money, a consumer could argue that an issuer misrepresented its privacy practices in order to cause the consumer to rely upon those practices and purchase the issuer's product.

Several privacy concerns were brought to the Task Force's attention during the course of its proceedings. Commenters stated that consumers were concerned that e-money technology would enable issuers and merchants to obtain large amounts of information about them. Similarly, many commenters stated that consumers were concerned that they would not receive adequate disclosure about an issuer's information practices, and that issuers would be able to share a consumer's e-money transaction information with third parties without the consumer's consent.

The Task Force recognizes that the increased efficiency of data collection methods associated with e-money may increase the potential for privacy intrusions. However, the Task Force also recognizes that technology provides opportunities for increased privacy, and that different privacy policies and product characteristics may be appropriate for different consumers depending on their disparate individual preferences relating to privacy. Moreover, e-money is in an early stage of development, and there is not yet any indication that anonymous payment methods (such as cash or anonymous e-money products) will not remain available.

Additionally, existing laws and market responses may address some consumer concerns. Industry participants appear to have significant incentives to develop an e-money market for consumers especially concerned about privacy. Similarly, industry self-regulatory principles have the potential to address other concerns expressed to the Task Force. Industry groups are currently working to develop privacy practices. The Task Force encourages issuers to adopt self-regulatory initiatives that are meaningful and effective in that they both respond to consumers' privacy concerns and involve some means to assure adherence by individual participants. These means can involve a variety of flexible approaches.

Privacy protections are essentially evolutionary in the United States, and there is little precedent for comprehensive government established privacy protections. Until e-money has had more time to develop, it is premature to assess whether and the degree to which it will present threats to privacy that would warrant government action.

As the e-money industry changes and matures, the extent to which industry participants have effectively addressed consumer privacy interests through self-regulatory initiatives should be carefully monitored. The need for government action regarding privacy standards for e-money then can be reassessed based on the growth of e-money as a payment media and the success of e-money providers in implementing effective privacy principles and policies.

FINANCIAL CONDITION OF ISSUERS

As e-money is generally a prepaid payment instrument, consumers and merchants bear some credit risk in holding it. Thus, the financial condition of issuers is an important consideration.

Summary of Comments

Many commenters informed the Task Force that consumers will be concerned about the financial condition of the issuer of e-money products. Specifically, commenters believed that consumers would be concerned that issuer insolvency or illiquidity resulting from poor investments, insufficient internal controls, or undetected counterfeiting could prevent their e-money issuer from honoring the value it issued.[117] For these reasons, several commenters suggested that only federally insured depository institutions should be permitted to issue e-money.[118] Similarly, several commenters were concerned that the market would stratify along socioeconomic grounds with lower-income consumers offered products issued by unregulated issuers. In response, some commenters suggested model legislation to ensure that LMI consumers enjoyed protections against issuer insolvency.[119]

Many commenters were concerned that consumers would not be aware of, or would be confused about, their rights in the event their e-money issuer became insolvent. According to some commenters, many consumers may incorrectly assume that the stored value is FDIC-insured and even if consumers realize that the stored value products are not insured, many may believe that the presence of depository institutions in the distribution chain indicates that their stored value would have some greater level of "protection."

Other commenters were concerned that even if issuers provided disclosures about an issuer's financial condition, consumers may not understand the risks of the particular types of issuers. They argued that consumers' lack of understanding of the complex structure and operations of stored value systems may cause consumers to misunderstand the risks inherent in these systems.

---

[117] Prof. Budnitz, in his remarks before the Task Force, noted that the pattern of failures currently occurring in the phone card industry, including those resulting from organized crime, may also arise with the advent of e-money. Remarks of Prof. Mark Budnitz, Professor of Law, Georgia State University College of Law, Task Force Public Meeting (June 9, 1997), Panel on Disclosures and Consumer Protections. *See also* FRB Report, at 34-35.

[118] Harshaw, Remarks and Statement, *supra*; Shields, Remarks, *supra*. These commenters also added that only insured depository institutions should be permitted to issue e-money in recognition of their obligations under the Community Reinvestment Act.

[119] These commenters maintained that legislation was necessary, because the market will not address the concerns of low- and moderate-income consumers. Budnitz, *supra*, and Margot Saunders, Remarks and Prepared Statement, Task Force Public Meeting (June 9, 1997), Panel on Disclosures and Consumer Protections.

They were further concerned that inadequate disclosures may serve to exacerbate consumer confusion concerning the protections in place for any specific stored value product.

An industry commenter stated that many states regulate payment instrument issuers and that these laws would likely apply to issuers in e-money systems.[120] This commenter added that although these laws differ markedly, the protections that result are in fact quite uniform because most issuers comply with the laws of the most stringent states. Other commenters questioned the adequacy of protections offered by the state-based money transmitter regime and whether those laws in fact apply to e-money.[121]

Another industry commenter noted that integrity of the e-money issuer is critical to ensuring a safe and reliable e-money payment system. This commenter felt that the failure of an issuer will have the potential to derail the settlement of thousands of transactions and leave consumers with devalued or worthless payment instruments, thus shaking public confidence in the payment system.[122] Therefore, this commenter believed that issuers should be required to meet high standards of financial soundness and responsibility.

Several industry commenters stated that they have significant market incentives to provide consumers disclosures about their financial soundness. First, they often provide detailed disclosures to help differentiate themselves from competitors. Second, they wish to set the standard of financial integrity in the industry.

Still another industry commenter stated that one issuer has committed to a federal banking agency that it will only invest consumers' funds represented by stored value in short term U.S. government securities.[123] This commenter further stated that every licensed sub-issuer in this issuer's system is contractually required to redeem at face value all value presented by system cardholders.

Many industry commenters argued against government-mandated disclosures for e-money systems. These commenters felt that mandated, uniform disclosure rules could not accommodate the many potential varieties of e-money systems. They believed that, at most, the government should list topics to be covered in disclosures, and not mandate the details. Finally, others

---

[120] Levine, *supra*.

[121] Budnitz, Remarks, *supra*; Plotkin, Panel on Financial Integrity.

[122] Statement and Remarks of John M. Lewis, President, Bank of Fayetteville, on behalf of the American Bankers Association, Task Force Public Meeting (June 9, 1997), Panel on Financial Integrity.

[123] Plotkin, Statement and Remarks, Panel on Financial Integrity, *supra*. This commenter further stated that this issuer has committed to engage only in activities deemed to be permissible for national banks and that it be subject to the examination, supervision, and regulation of a federal banking agency.

believed that industry self-regulatory disclosure initiatives would be developed by industry trade associations.

Protections in Law

Existing laws may help address consumer concerns about issuer default. However the nature of the risks will likely depend on the status of the e-money issuer.

Existing Protections for Depository Institution Issued Stored Value

If the issuer is a bank, thrift, or other federally supervised depository institution, it would be subject to supervision, examination, and regulation by the federal depository institution regulatory agencies.[124] Liquidity and solvency questions are addressed in current depository institution regulation through capital requirements, asset restrictions, and limitations on depository institution activities.[125] Federal depository institution regulatory agency supervision seeks to protect the safety and soundness of the depository institution through on-site examinations and the periodic review of submitted financial information. Depository institutions issuing e-money directly would be subject to those constraints. These protections are designed to reduce the risk that the institution will become insolvent.

Consumers holding depository institution issued e-money would face significant risk of loss should the depository institution become insolvent. The FDIC, in its General Counsel's Opinion No. 8, concluded that most stored value products are not considered "deposits" under 12 U.S.C. 1831(l) and thus are not covered by deposit insurance.[126] The FDIC further stated that it expects

---

[124] Similarly, if the issuer is a subsidiary of such an institution, or if insured institutions hold minority investment positions in the issuer, it could be subject to special oversight. *See, e.g.*, OCC Conditional Approval No. 220 (December 2, 1996).

[125] For a more complete discussion, *see* U.S. Department of the Treasury staff report, *An Introduction to Electronic Money Issues*, prepared for the United States Department of the Treasury Conference, Toward Electronic Money and Banking: The Role of Government, September 19-20, 1996, Appendix 4, (hereafter cited as *An Introduction to Electronic Money Issues*).

[126] Federal Deposit Insurance Corporation General Counsel's Opinion No. 8, 61 Fed. Reg. 40,490 (August 2, 1996). The FDIC in General Counsel's Opinion No. 8, classified all e-money systems into four categories based on the statutory definition of deposit in the Federal Deposit Insurance Act. The categories are:

> (1) Bank Primary-Customer Account Systems, in which funds underlying the e-money remain in an account until the value is transferred to a merchant, who, in turn, collect's the funds from the customer's bank;
> (2) Bank Primary-Reserve Systems, in which the funds are withdrawn from a customer's account (or paid directly by the customer) and paid into a reserve or general liability account held at the institution to pay merchants as they make claims for payments;
> (3) Bank Secondary-Advance Systems, in which the electronic value is created by a third party and is provided to the depository institution to make available to its customers. As customers exchange funds for e-money, the

insured depository institutions to clearly and conspicuously disclose to their customers the insured or non-insured status of their stored value products, as appropriate.[127] Moreover, depositor preference laws would result in e-money holders becoming general creditors of the bank, behind uninsured and insured depositors.

Although consumers purchasing depository institution issued stored value would still face insolvency risk, the level of protections produced by existing laws and regulatory practices may address many of the consumer concerns expressed to the Task Force.[128] For example, depository institution e-money issuers, as encouraged by the FDIC, would be expected to disclose the insured or uninsured status of their product.

Existing Laws Governing Nonbank Issued Stored Value

In the 43 states that have enacted money transmitter laws, the general requirements and the levels of prudential standards and enforcement vary significantly.[129] Most states require the

---

> funds are held for a short period of time and then forwarded to the third party; and,
> (4) Bank Secondary-Pre-Acquisition Systems: in which the e-money value is created by a third party and the depository institution exchanges its own funds for e-money from the third party, and in turn, exchanges e-money for value with its customers.

Id. at 40,490.

The FDIC also asked for public comment on whether the FDIC should propose regulations or seek legislative action to determine that e-money, like cashiers' checks and money orders and other analogous paper obligations issued by a bank, is entitled to deposit insurance. *Id.* The FDIC, by press release dated June 24, 1997, announced that it has decided not to seek to define e-money as deposits for purposes of insurance coverage.

[127] *Id.* at 40,494.

[128] *See* William Roberds, *What's Really New about the New Forms of Retail Payment?*, Federal Reserve Bank of Atlanta Economic Review, 32 (First Quarter 1997).

[129] *See* Remarks and Written Statement of Ezra Levine, Howrey & Simon, representing the Association of Money Transmitters, Task Force Public Meeting (June 9, 1997), Panel on Issuer Financial Condition and Reliability.

Federal regulation in this area to date is limited. The Treasury Department regulation in this area focuses on law enforcement money laundering concerns, such as extending currency and transaction reporting requirements to money transmitters and requiring money transmitters to register with Treasury. 31 U.S.C. 5330. Additionally, the Federal Trade Commission has enforcement authority over nonbanks pursuant to certain credit-related consumer protection statutes and trade regulation rules, including the EFTA and FCRA. In addition, Section 5 of the Federal Trade Commission Act prohibits unfair or deceptive acts or practices.

However, the Congress has recognized the lack of uniformity in the existing state regulatory system for money transmitters and has considered legislation providing comprehensive federal regulation in the past. *See, e.g.*, H.R. 1448, the "Check Cashing Act of 1993," which would have created a federal licensing requirement and would have prohibited a person other than a depository institution from engaging in the business of issuing, redeeming, or cashing checks, travelers' checks, money orders, or similar instruments, or from transmitting money without a license from the Federal Trade Commission (FTC). H.R. 1448 would have required the FTC, before issuing a license to review the business record and the capital adequacy of the applicant and the competence, experience, integrity, and financial ability

transmitter/issuer to have a specified minimum amount of assets and to purchase a surety or bond. A number of states require issuers to hold assets in permissible investments sufficient to cover all outstanding payment instruments (not only those issued in the particular state).[130] A few state statutes impose a constructive trust over these reserve assets to ensure that the reserves are protected from the claims of the money transmitter's general creditors.[131] Several states exempt closed systems from the scope of their money transmitter regulatory systems. Some states have the authority to conduct on-site examinations whereas other states conduct an off-site analysis of financial information submitted for state review.[132]

In addition to the safety and soundness requirements just discussed, several state money transmitter laws require payment instrument issuers to place their name on the face of the payment instrument, and display their license and/or the name and address of the state regulatory agency.[133]

---

of each applicant, controlling person, or supervisory employee. *See Check Cashing Stores: Necessary Service or Excessive Profit? Hearing before the Human Resources and Intergovernmental Relations Subcomm. on H.R. 1448*, 103d Cong. 1st Sess. 2 (1993).

Congress has also sought to encourage uniform state regulatory of money transmitters. In 1994, as part of the Money Laundering Suppression Act of 1994, Congress specifically requested that the states develop and adopt a model money transmitters act under the auspices of either the National Conference of Commissioners on Uniform State Laws ("NCCUSL") or the American Law Institute. *See* Sense of Congress Resolution, Section 407, Community Development and Regulatory Improvement Act of 1994, P.L. 103-325.

The NCCUSL is presently drafting such a model act addressing non-depository providers of financial services, including stored value issuers. An initial draft of this act was issued in February 1998

The Money Transmitter Regulatory Association ("MTRA"), an organization consisting of members of various state banking departments has also developed a model act addressing the need for uniform national licensing and regulation of money transmitters. This act imposes limited capitalization and bond/surety requirements, requires the payment instrument issuer to maintain highly liquid reserves equal to the amount of instruments outstanding, and provides for both on-site and off-site supervision by the appropriate state banking agencies, among many other requirements. To date, six states have adopted a version of this model act. Levine Remarks, *supra*.

[130] *See* Levine, *supra*, (stating that 20 states require that issuers maintain permissible investments reserves).

[131] Only Colorado, Georgia, and Illinois impose a constructive trust over the permissible investments, protecting them from levy or seizure by general unsecured creditors. *See* Colo. Rev. Stat. 12-52-107 (Supp. 1995), Ga. Code Ann 7-1-682(b) (Michie Supp. 1995), Ill. Rev. Stat. ch. 205, para 657/50. *But see*, Levine Remarks, *supra* (stating that three states that adopted the "Model Act", discussed *infra*, impose a constructive trust and that Massachusetts and New Jersey will be enacting similar requirements shortly).

Without such a trust, creditors of the money transmitters' other activities would be able attach the unprotected reserve funds to satisfy their obligations.

[132] However only a handful of states actually exercise this authority. Levine remarks, *supra*. In particular, California, New York, and Pennsylvania have long performed examinations of nonbank payment instrument issuers. Texas, Florida, and Delaware have only recently begun performing such exams. *Id.*

[133] For example, Arizona, Delaware, District of Columbia, Florida, Illinois, Kentucky, Louisiana, Mississippi, Nebraska, North Carolina, North Dakota, Oregon, Pennsylvania, Virginia, and Wisconsin require the name of the payment instrument issuer to appear on the instrument. *See* Ariz. Rev. Stat. Ann. 6-1215(a) (Supp. 1996), Del. Code

Although many states have laws regulating money transmitters and issuers of written payment instruments, such as money orders and travelers checks, it is unclear whether these laws will apply to nonbank e-money issuers. To come within this regime, e-money generally must meet existing state definitions of a "check" or "payment instrument." Several states have determined that e-money would fall within these laws. In addition, many major money transmitters have stated their view that these laws apply to electronic money.

If e-money were determined to be covered under some state money transmitter laws, consumers would have rights to the proceeds of the bond/surety pledged for the benefit of holders of the nonbank issuer's payment instruments and to the funds held in the pool of liquid assets. Should these remedies be insufficient to satisfy consumers' claims, consumers holding the issuer's stored value would become general unsecured creditors of the issuer's bankruptcy estate for the unsatisfied portion of their claims.[134] It is important to note, however, that recent experience of nonbank issuers of travelers checks and money orders does not provide conclusive evidence that e-money issued by nonbanks is likely to be inherently riskier than that issued by banks.

Industry Responses

Industry responses relevant to the financial condition of issuers may focus on measures to promote the financial reputation of issuers, or of entire electronic money systems, in order to encourage consumer and merchant acceptance of their products. In general, an issuer would likely have difficulty setting up a large scale system without taking steps to assure consumer and merchant confidence. Since this is an emerging market, it is likely that fears about the debilitating effect on the issuer's reputation that would result from issuer default will cause issuers to take steps to limit this risk wherever possible.

Merchants who accept e-money in payment for their goods and services would have strong incentives to monitor issuers or systems and their record of honoring electronic money transactions in a timely manner. Inadequate policies or fraudulent issuers are likely to become apparent in short order, particularly to merchants who would quickly cease to accept cards from suspect issuers that did not meet redemption demands. Monitoring of issuers by merchants, who will have a much stronger incentive than consumers, may also cause issuers to limit their default risks.

Consumers are also likely to be wary of entrusting their funds to an unknown entity with questionable reputation given the prepaid nature of electronic money products. If choices are

---

Ann. tit. 5, 2313, D.C. Code Ann. 47-3112, Fla. Stat. ch. 560.213, Ill. Rev. Stat. ch. 205, para. 657/65(a), Ky. Rev. Stat. Ann. 366.120, La. Rev. Stat. Ann. 1043, Miss. Code Ann. 75-15-23, Neb. Rev. Stat. 8-1011, N.C. Gen. Stat. 53-203.1, N.D. Cent. Code 51-17-13, Or. Rev. Stat. 717.140, Pa. Stat. Ann. tit. 7, 6111(b), Va. Code Ann. 6.1-378, Wis. Stat. 217.11.

[134] One state, however, provides a form of insurance by levying a one time assessment against all licensed money transmitters in the state to cover any such shortfall. *See* N.Y. Banking Law art. XII-C (McKinney 1996).

available, consumers will likely require some familiarity with issuers of stored value products since they are prepaying for value to be used at some future date. Thus, consumers choosing to use e-money will likely migrate to products with well-known sponsors or to paper currency and coins, payment media that carry no credit risk for the consumer or merchant.

Some nonbank issuers may be affiliated with depository institutions. In such instances, depository institutions entering into such arrangements may want to confirm the nonbank's financial stability, such as through independent audits, and to limit their liability, such as by requiring a third party bond/surety or the pledging of specific assets. Such affiliations may subject the nonbank issuer to additional federal supervisory oversight.[135]

As some commenters noted, specialized issuers of e-money are already instituting policies to invest their funds in highly liquid assets, such as cash and short-term government securities, to minimize market and liquidity risk of their portfolios.[136] E-money systems comprising numerous financial institutions, which the major electronic payments networks plan to operate, may also adopt financial integrity policies to protect consumers and merchants from losses due to the failure of any one institution in the system. Issuers, either individually or as part of a group, may establish protections against issuer default by purchasing insurance issued by a third party, self-insuring, or absorbing the increased costs rather than passing them on to consumers. In addition, groups of institutions could create a self certification system denoting issuers of strong financial condition or institute loss-sharing arrangements providing that members cover any shortfall caused by any one member's default.[137] The industry may also develop disclosure policies regarding consumer rights in the event of issuer default, insured/uninsured status of the e-money product and whether the institution is subject to regulatory oversight.

Some commenters have suggested that issuers will provide disclosures about their financial condition and the rights of consumers in the event of bankruptcy. The nature of a consumer's rights and claims against an issuer in bankruptcy or insolvency likely will involve highly complex legal issues and likely will differ depending on the structure of the particular electronic money system. It seems unlikely that most consumers will be able to comprehend information about detailed legal and financial issues. Issuers may, however, encourage consumer acceptance by disclosing the existence of financial guarantees, if any, that are available either within, or external

---

[135] The federal supervisory agency of the depository institution affiliating with the nonbank issuer could, in some cases, require the depository institution to implement controls to minimize its risk exposure from such an arrangement.

[136] *See* Plotkin Remarks *supra*.

[137] Such market-established protections against issuer default could increase the costs of e-money systems and possibly the prices consumers must pay for the products. Thus, some consumers could pay a premium to ensure the quality of the stored value they are holding, while others could elect a potentially riskier product for lower fees. The higher cost resulting from these protections may make the products' cost prohibitive for some or all consumers and issuers. *See also* G-10 Report at 9.

to, the system — such as federal deposit insurance coverage or commitments by institutions to honor e-money in the event one issuer fails.

Although some issuers may seek to distinguish themselves by publicly disclosing their investment policies and the assets backing their e-money instruments, this incentive may not exist for less financially-stable issuers. In such cases, consumers will have to use their judgment in determining whether to use the product.

Conclusion

Many commenters informed the Task Force that they were concerned that e-money issuers would become insolvent, and that consumers would not be informed of their rights in the event of such an insolvency.

Depository institutions that issue e-money will be subject to the supervision, regulation, and examination of the federal and state depository institution regulatory agencies. These issuers are expected to disclose the insured or non-insured status of the e-money products they issue. Nonbank issuers that are owned by or affiliated with banks also may be subject to oversight by the federal and state depository institution supervisors that supervise the depository institutions that own interests in the issuer and possibly other federal regulatory agencies.

Other nonbank issuers may be subject to state supervisory oversight; however, the extent of this supervision is unclear. Clarification by state regulators and legislatures of the applicability of their laws to e-money could be beneficial.

It is too early to tell whether market developments will adequately address these concerns in light of existing regulatory schemes. E-money is not currently, nor expected to become in the near future, a significant part of the payment system. Accordingly, regulatory action to set standards for e-money issuer financial integrity is premature at this time.

The level of consumer awareness of issues presented by e-money products will also affect the assessment of whether these and other self-regulatory responses are adequate given the state of the marketplace. At least in theory, informed consumers can safeguard themselves from risks arising from the financial condition of issuers by limiting the amount of funds they are willing to place with an issuer when the issuer’s reputation is questionable or its financial condition is not transparent. If, however, e-money issuers target segments of consumers, *e.g.*, low- and moderate-income individuals and the elderly, who may have for various reasons, more limited choices of e-money providers than other consumers and may have less ability to protect themselves by "shopping" for e-money providers, the financial condition of issuers that primarily serve those consumers may deserve careful monitoring.

The Task Force urges issuers of electronic money to establish policies and procedures to safeguard consumer funds and ensure that transactions can be honored as promised. The Task

Force also urges industry participants to explore means of improving the transparency of the financial structure to participants, including consumers and merchants.

Moreover, for all e-money issuers, the Task Force urges that issuers disclose to consumers information concerning whether they can recover funds held in stored value in the event of issuer insolvency and the insured or uninsured nature of e-money products. Effective disclosure of this information would be a useful self-regulatory step that could be undertaken at this early stage of e-money industry development.

CONSUMER DISCLOSURES AND PROTECTIONS

While e-money holds the potential to provide consumers with benefits not found in traditional payment mechanisms, it also presents new areas of consumer concern. These concerns must be addressed if e-money is to achieve widespread consumer acceptance.

Summary of Comments

Many commenters stated that consumers may not know or understand their rights and liabilities when using e-money systems. These commenters stated that the physical similarity between some types of e-money products and more familiar debit and credit cards might cause some consumers to assume that the same safeguards and regulatory requirements apply to each system.[138] Additionally, these commenters believed that this potential for confusion would be even greater for multi-function cards, such as a card that can perform debit, credit, and stored value functions. Several commenters noted that consumers may not fully appreciate that if they lose their e-money cards, they could lose all remaining value on the card.[139] Finally, several commenters were concerned that the market would stratify along socioeconomic grounds with lower-income consumers only being offered less costly products issued with fewer protections.[140]

Other commenters noted that advertisements may mislead consumers. For example, they noted that statements that e-money is "just like cash" could cause some consumers to incorrectly believe that e-money is legal tender and that all merchants must accept it.[141] Similarly, a commenter noted that consumers may face liability if merchants are unable to collect from the stored value issuer for goods purchased with stored value.[142]

Furthermore, many commenters stated that consumers will be concerned that they will not receive adequate disclosure of their rights and liabilities in e-money systems. Several commenters noted that consumers should receive disclosures that provide a description of what happens if a card is

---

[138] *See* Written Statement of the Consumer Federation of America, Consumers Union and U.S. PIRG, October 21, 1997.

[139] *Id. See* also, Shields Remarks and Creque Statement and Remarks, Panel on Security Issues.

[140] *See* Graves Remarks, *supra.*

[141] Budnitz Remarks and Joint Statement with Margot Saunders and Saunders Remarks, *supra*.

[142] *Id.*

lost or stolen, liability for unauthorized transactions, instructions on the use of the card, a description of the redemption process, and an itemization of fees and charges.[143]

Many commenters stated that disclosure alone is not an adequate substitute for substantive regulatory protections. They argued that the government should establish uniform minimum regulatory protections rather than adopt only disclosure requirements or rely on industry self-regulatory initiatives. These commenters urged that uniform protections should be established for all types of payment instruments, to avoid the consumer confusion that occurs when different rules apply to different payment mechanisms.[144]

Other commenters suggested that very low value e-money cards do not raise concerns that should necessitate regulatory or legal recourse in the event of loss or theft.[145] However, they believed that the absence of substantive protections should be clearly and prominently disclosed. These commenters further suggested that higher value stored value cards should benefit from the same types of substantive protections against loss or theft that apply to other noncash payment instruments, such as debit and credit cards.

Many industry commenters noted that it would be inadvisable to attempt to mandate a single set of consumer protection rules. Instead, they suggested that information should be tailored to particular products.[146] These commenters stressed that because e-money is designed to be a cash substitute, substantive regulatory protections such as those applicable to other card-based

---

[143] *See* Consumer Federation of America, Written Statement, *supra*. Some commenters also stated that the financial strength of the issuer should be disclosed to consumers to permit them to make an informed decision about the relative financial strength of the issuer prior to purchasing e-money. Several other commenters remarked that an issuer's privacy policy should also be disclosed.

[144] A few commenters urged the Task Force's support of a "Stored Value Protection Act" that would apply to all systems (whether open or closed) capable of storing value in excess of $25. Under this proposal, all issuers either would be regulated by the federal government or be bonded in the amount equal to twice the value of the sales of the stored value cards in one year. This proposal also provided, among other things, clarification that payment by e-money would represent full and final payment by the consumer and that issuers generally would be required to reimburse consumers for all losses resulting from an error attributable to the issuer or a merchant's defective device, fraud or mistake on the part of the issuer or merchant and damage to the e-money card. This draft act further provided that issuers must inform consumers of any change in terms affecting the e-money's validity and must allow consumers to redeem all remaining value on the card for cash for $1. The draft act also provided an error resolution mechanism and prohibited issuers from making false and misleading claims. Additionally, the draft act prohibited the issuer from disclosing consumer's personally identifiable information without the consumer's prior consent. Moreover, the draft act required the initial disclosure of all fees, error resolution procedures, rights of reimbursement, and the expiration date of the card. Finally, the draft act required issuers to provide transaction receipts, either written or electronic for all transactions over $5, reflecting fees, charges, and the amount remaining on the card. Budnitz and Saunders, Joint Prepared Written Statement.

[145] Consumer Federation of America, Written Statement, *supra*.

[146] Smith, Statement and Remarks, *supra*, Rinearson, Statement and Remarks, *supra*.

payment products may not be necessary for these products. They suggested that disclosures stressing the cash-like nature of the product (and differences with other products that have clearly established consumer protections associated with them) coupled with consumer education efforts such that consumers understand these products would be more appropriate.[147] A commenter added that if consumers want a product that can be replaced under any circumstances, including loss, then consumers must be prepared to accept reduced convenience and probably higher costs (due to higher prices for the authorization and telecommunications infrastructure required to provide the additional service).[148]

Several industry commenters added that issuers will respond to consumers' expectations and that products that do not satisfy these expectations will not survive in the marketplace. Similarly other industry commenters noted that there already is a substantial competitor to e-money in the marketplace — cash. Accordingly, issuers already face a large obstacle to design a product that is at least as attractive as cash.

These commenters further stated that because e-money products are still in an early phase of development, compliance with premature regulatory requirements may be technically infeasible and unaffordable for some of these products and the expense of compliance may result in other products no longer being economically justified.[149] Lastly, industry commenters added that development of these products should be driven by technological capability, economic viability and consumer demand, not government regulation. They suggested that government intervention should be limited solely to addressing the financial integrity of the issuer.[150]

All industry commenters currently operating pilot programs stated that they provide information to consumers at the time of purchase. This information is usually provided in a brochure or on the back of the purchase receipt for consumers who purchased stored value cards from unattended card issuing machines.[151] These disclosures usually provide information about how and where to use the cards, procedures for loss of card, card redemption and replacement, fees, applicable law governing disputes arising from the card, FDIC-insured status, and what happens to value remaining on a card when the card expires. In addition, some issuers print some information on the card itself, such as whether the funds will be replaced if the card is lost.
Several commenters added that they intend to set high standards for consumer disclosure that will be followed in the marketplace to generate trust and consumer confidence in these products.

---

[147] *See, e.g.*, Plotkin Statement and Remarks, Panel on Consumer Protections and Disclosure, *supra*.

[148] *Id.*

[149] *See, e.g.*, Smith Statement and Remarks, *supra*, Rinearson, Statement and Remarks, *supra*.

[150] *See*, Smith, *supra*, Plotkin Statement and Remarks, *supra*.

[151] *See, e.g.*, NationsBank Written Statement, First Union Written Statement; Smith, *supra*.

Existing Statutory and Regulatory Protections

The Electronic Fund Transfer Act and Regulation E

The Electronic Fund Transfer Act ("EFTA") covers a variety of electronic funds transfers involving consumers' checking, savings, or other consumer asset accounts. The EFTA and its implementing regulation, Federal Reserve Regulation E, establish certain rights, liabilities, and responsibilities of participants in electronic fund transfer ("EFT") systems. Under the EFTA, consumer liability for unauthorized use of a lost or stolen access device (*e.g.*, an ATM card) is generally limited to between $50 and $500.[152] The EFTA also provides procedures for resolving errors and disputes involving EFT services. For example, providers are required to investigate and respond to consumer complaints within 10 business days (or longer, if the provider provisionally re-credits the consumer's account in the amount of the alleged error pending further investigation). Finally, the EFTA makes the covered provider of EFT services generally liable to the consumer for all damages caused by the failure to make a correct and timely transfer of funds.[153]

Under Regulation E, financial institutions offering EFT services subject to the EFTA must provide extensive disclosures to consumers. They are required to provide consumers with initial disclosures covering: consumer liability for unauthorized use of an access device, procedures for reporting a suspected unauthorized transfer, any limitations on the type and frequency of transfers, the amount of charges for transfers, the consumer's right to detailed documentation of transfers, the consumer's right to stop payment on preauthorized transfers, the circumstances under which the financial institution will disclose information on the consumer's account to third parties, and a summary of the error resolution procedures. Additionally, financial institutions are required to provide consumers with a documentary record of EFT transactions, in some cases at the time the transfer is initiated at a terminal, and in periodic account statements.

The full range of EFTA and Regulation E consumer protections apply to consumer EFT by any financial institution that holds either a consumer's account or issues an access device and provides the consumer EFT services. Thus, the EFTA mandates uniform protections for consumers that engage in EFT. Further, these consumer rights cannot be abrogated by contract.

---

[152] Similar protections are also available for credit cards under the Truth in Lending Act and the Fair Credit Billing Act.

[153] Several states also have electronic funds transfer statutes that provide consumers with similar protections to the EFTA. Iowa Code Ann. 527 (1996); Mass. Gen. Laws Ann. ch. 167B 1 (1996); Mich. Comp. Laws Ann. 23.1137 (1995); Mont. Rev. Code Ann. 32-6-101 (1996). Although, these states' laws apply only to consumer asset accounts, several states define this term very broadly. Mass. Gen. Laws Ann. ch. 167B 1; Iowa Code Ann. 527.2. Ordinarily, state EFT laws would be preempted, if they are inconsistent with the EFTA, but not if the state law provides greater protections than the EFTA. The Federal Reserve Board has not determined that Reg E does not apply.

The Federal Reserve has not yet determined whether Regulation E applies to stored value cards or other e-money systems. Thus, consumers are generally required to receive extensive disclosures in EFT systems, but not in e-money systems except where the e-money product provides access to an account.[154] However, the Federal Reserve Board has proposed an amendment to Regulation E to provide limited coverage of certain stored value cards.[155]

Under this proposal, all stored value cards that do not allow more than $100 to be loaded on the card at any one time would be exempt. Moreover, even those systems that permit a maximum load of more than $100 would not be covered if they are "off-line unaccountable" stored value systems in which the record of individual transactions and the card balance is maintained on the card itself. "Off-line accountable" systems, stored value card systems that maintain a central record of individual transactions and card balances, would be subject to most of Regulation E's initial disclosure requirements, but not any other disclosure requirements or substantive consumer protections. Finally, under the proposal, most of Regulation E's provisions would be applied to those systems that maintain a central database where transactions are authorized on-line ("on-line accountable"). Such systems would not be required to provide a periodic statement (if an account balance and a summary of recent transactions is provided on request), the annual reminder of error resolution procedures, or change in terms notices.

In response to this proposal, Congress directed the Federal Reserve Board to conduct a study that evaluates whether provisions of the EFTA could be applied to e-money products without adversely affecting the cost, development, and operation of such products. In conducting this study, the Board was also asked to consider alternatives to regulation under the EFTA, including the option of allowing market forces to shape the development of e-money.[156]

The Federal Reserve Board submitted its Report to Congress in March of 1997. The report included a detailed analysis of the potential cost implications of applying a range of Regulation E requirements to e-money and concluded that:

> Any . . . approaches to selective application of Regulation E requirements would, depending on the details, probably impose significant operating costs for some electronic stored-value products and could generally give rise to opportunity costs as well. The approach to applying Regulation E to electronic stored-value products that would impose the smallest opportunity costs and be least likely to inhibit development of the new technology is the one that requires only initial disclosures. However, even this approach has the potential to distort market

---

[154] Regulation E does apply to the transaction when consumers download value from their transaction account to load onto a stored value card.

[155] 61 Fed. Reg. 19696 (May 2, 1996).

[156] *See* Section 2601 of the Economic Growth and Paperwork Reduction Act, Pub. L. No. 104-208, 110 Stat. 3009.

outcomes by differentially affecting the costs of alternative products. Given the limited experience with stored-value products to date, it is difficult to assess the extent to which the benefits to consumers from any particular Regulation E provision would outweigh the corresponding costs of compliance. Moreover, Regulation E does not cover some important risks faced by consumers using stored-value products, such as loss (where no unauthorized use occurs) or expiration of the instrument or insolvency of the issuer.

Early regulation of electronic stored-value products could cause higher regulatory costs than later regulation (if regulation ultimately is determined to be desirable) because of economies of scale, the cost of revising regulations, and possible opportunity costs. However, early regulation also has the potential to speed up development by promoting standardization and by removing uncertainty about the applicability of regulation to new products and technologies.

Even if regulation of electronic stored-value products is determined to be desirable, there may be legal constraints to regulating all stored-value products under the Electronic Fund Transfer Act. The Act's language and its legislative history clearly permit the application of Regulation E to some electronic stored-value products (i.e., those that involve a consumer's asset accounts), but may not cover others. To the extent that this legal distinction leads to differential regulatory treatment of similar products, it could significantly influence the evolution of electronic stored-value products as a payment option.[157]

The Congress directed that the Federal Reserve Board delay acting on the proposal for a nine-month period ending in June 1997. Final action by the Federal Reserve Board is still pending.

Other Federal and State Statutes

As discussed in the privacy section, the FTCA prohibits entities from engaging in unfair or deceptive practices in or affecting commerce. E-money issuers that represent that their e-money is just like cash or otherwise imply it is "legal tender" may be engaging in deceptive practices.[158] Similarly, e-money issuers that misrepresent the quality of assets backing their e-money or make other misrepresentations about the value or attributes of the e-money products that consumer rely upon to their detriment may also be engaging in fraudulent and deceptive practices.[159]

---

[157] FRB Report to Congress, *supra*, 4 (footnotes omitted).

[158] *See* 31 U.S.C. 5103 (defining U.S. legal tender).

[159] *Cf.* Press Release, *FTC Charges Seller of Prepaid Phone Cards with Deception*, August 6, 1997; Press Release, *Seller of Prepaid Phone Cards Settles with FTC*, March 18, 1998.

As discussed above, state money transmitter laws may also provide some consumer protection. These laws require disclosure of the money transmitter's name on the instrument,[160] limit the amount of fees money transmitters can charge,[161] and prohibit false or misleading advertising.[162] However, as discussed previously in the financial condition of issuer section of this report, it is unclear whether these laws apply to e-money.

State Uniform Commercial Codes governing negotiable instruments also may not apply to e-money for several reasons.[163] First, the promise to pay associated with an electronic stored value product is often subject to the conditions set forth in the product contract and may not be "unconditional." Second, even if the e-money promise to pay was found to be "unconditional," it may not qualify as a "writing" which generally must be reduced to tangible form.[164] Finally, most e-money products do not include a promise to pay a sum certain; rather, they permit many fractional payments until the value stored on the card is exhausted.

In sum, the application of existing statutory regimes to e-money is uncertain and may not by themselves specifically address consumers' concerns about receiving adequate information about their rights and liabilities in e-money systems, liability for unauthorized use or card malfunction, and the ability to correct e-money transaction errors.

Protections in Common Law

---

[160] Arizona, Delaware, District of Columbia, Florida, Illinois, Kentucky, Louisiana, Mississippi, Nebraska, North Carolina, North Dakota, Oregon, Pennsylvania, Virginia, and Wisconsin require the name of the payment instrument issuer to appear on the instrument. *See* Ariz. Rev. Stat. Ann. 6-1215(a) (Supp. 1996), Del. Code Ann. tit. 5, 2313, D.C. Code Ann. 47-3112, Fla. Stat. ch. 560.213, Ill. Rev. Stat. ch. 205, para. 657/65(a), Ky. Rev. Stat. Ann. 366.120, La. Rev. Stat. Ann. 1043, Miss. Code Ann. 75-15-23, Neb. Rev. Stat. 8-1011, N.C. Gen. Stat. 53-203.1, N.D. Cent. Code 51-17-13, Or. Rev. Stat. 717.140, Pa. Stat. Ann. tit. 7, 6111(b), Va. Code Ann. 6.1-378, Wis. Stat. 217.11.

[161] For example, the District of Columbia and Michigan limit the amount of fees that can be charged for the sale and/or cashing of checks. *See* D.C. Code Ann. 47-3113, Mich. Comp. Laws Ann. 487.910.

[162] Puerto Rico, Rhode Island, and Washington prohibit money transmitters from false and misleading advertising. *See* P.R. Laws. Ann. tit. 10, 2333(b), R.I. Gen. Laws 19-14-21 (Supp. 1995), Wash. Rev. Code 31.45.060 (West Supp. 1996).

[163] Although some initially thought that e-money might be a "good" under Article II, of the U.C.C. , many now believe that e-money will be exchanged for goods and services and that this exchange of value will constitute a payment, not barter. *See* ABA Task Force on Stored Value, *A Commercial Lawyers Take on the Electronic Purse*, 52 Business Lawyer 653 (February 1997). Similarly, it is likely that e-money would not be found to constitute fund transfers under article 4A, as most e-money transactions probably would not be initiated by an instruction by the payor to the payor's bank to pay the beneficiary.

[164] U.C.C. 3–103. However, this would not be the case in all states. At least three states have enacted statutes recognizing the validity of digital signatures in commercial settings. *See, e.g.*, Florida's Electronic Signature Act of 1996, Fla. Stat. Ann. 1.01(4), Utah's Digital Signature Act, Utah Code Ann. 46–3–102 et seq., and Washington's Electronic Authentication Act, Wash. Rev. Code title 19.

General common law contract and tort principles may also provide consumers some rights and protections with respect to e-money. Courts will not enforce an agreement between two parties if there was no "meeting of the minds." Consequently, undisclosed terms will not be considered part of the e-money contract and would be unenforceable. For example, a consumer may not be held liable for usage fees that were not disclosed to the consumer before he or she purchased the e-money product.[165]

Additionally, as discussed in the privacy section of this report, a consumer may bring an action for breach of warranty with respect to e-money, unless the issuer clearly and conspicuously disclaims any warranties. For example, e-money issuers that fail to provide clear and conspicuous warranty disclaimers may face liability for breach of warranty should the e-money malfunction.

Similarly, consumers may also have remedies in tort for negligent misrepresentation if an issuer supplies false information to consumers that they rely upon to their detriment if the issuer did not use reasonable care when making the representation about their e-money product.[166] To avoid liability, issuers may seek to disclaim this responsibility in consumer disclosures.

Finally, consumers may also have remedies under traditional common law fraud. Fraud usually is found to occur when a party obtains title to the property of another by an intentional or (knowing) false statement of past or existing fact with the intent to defraud the other. For example, a consumer may be able to bring an action under fraud should an issuer willfully misrepresent the value, attributes or costs of its e-money product and the consumer suffers pecuniary harm resulting from reliance on the representation.[167]

In summary, although e-money products may not fit neatly into existing federal or state legal regimes governing specific types of payment instruments, they may be covered by common law

---

[165] Other contract law principles may also help ensure that e-money issuers do not engage in unfair practices. Some contracts may be unenforceable if there is a wide disparity in bargaining power between the parties and the weaker party is forced to adhere to the terms set forth by the stronger party. Courts will often relieve parties from onerous provisions imposed by contracts that are contrary to public policy. Similarly, contracts that impose excessive fees or liability on a consumer may found to be unconscionable and will be voided by a court. Additionally, a court will refuse to allow a party to deny the existence of the contract when one party relies on the representation of the other to their detriment. In such instances, courts may also find that acceptance of the offer was manifested through performance. *See* Restatement (Second) of Contracts 45 & 90.

[166] Restatement (Second) of Torts 552.

[167] Existing federal and state laws addressing fraud that do not require a traditional depository institution account relationship or other special circumstances, will likely apply to e-money systems and may generally accord some protections, depending on the e-money system in question. In addition, state criminal statutes addressing debit or credit card theft may also apply to e-money. *See, e.g.*, Crimes involving Debit or Credit Cards, Ky. Rev. Stat. Ann., 434.550 *et seq.* (1993); Mich. Stat. Ann. 28.354 (13)(1995); Neb. Rev. Stat. Ann. 28.678 (1996); S. C. Financial Transaction Crime Act, S. C. Code Ann. 14-14-10 et seq. (1996).

principles. The applicability of these principles to e-money products creates incentives for issuers to establish reasonable rules regarding rights and responsibilities of the parties and to provide sufficient information to consumers concerning their policies. However, as discussed earlier, the efficacy of these protections is uncertain, as a consumer must affirmatively challenge the actions of an issuer under common law principles in a court proceeding.

Other Governmental Actions

Other governmental actions may address some of the consumer concerns expressed to the Task Force. Some of the federal banking agencies have issued guidance to banks that engage in e-money activities. These issuances encourage banks to provide adequate disclosure about their stored value products. For example, the FDIC, in its General Counsel's Opinion No. 8, states its expectation that all federally insured depository institution issuers disclose the insured or non-insured nature of their stored value. Also, the OCC, in its Stored Value Card Bulletin, encouraged national banks to provide the basic disclosures needed for stored value cards they distribute.[168] Among other things, the OCC suggested that banks consider the following topics when deciding how to adequately inform consumers:

- How to use the card.
- Where and how the consumer can increase the value on the card.
- Whether the electronic cash earns interest, dividends, or any other return.
- Where, how, and when the electronic cash can be redeemed.
- All fees charged in connection with obtaining or using the card or the electronic cash stored on it.
- The name of the entity that issues the electronic cash and its obligation to redeem it.
- Whether the consumer is protected in case of a lost or stolen card.
- Whether the amount of the electronic cash transferred to the card is insured by the FDIC.
- Where does liability lie if a transaction is not properly consummated.
- What happens to electronic cash that is abandoned or expires under the terms of the agreement.
- How consumers can resolve disputes involving electronic cash transactions.
- The circumstances under which information on a consumer's electronic cash transactions may be disclosed to third parties.

[168] OCC Bulletin No. 96-48. The OCC added that these disclosures should be adapted to the type of stored value sold.

Industry Responses

Issuers have many incentives to provide certain information to consumers. To promote use of their product, issuers will most likely need to provide consumers with information about how and where to use e-money, as well as instructions in its use. Issuers also need to ensure that merchants are properly trained in using the systems so as to prevent errors and malfunctions. If errors and malfunctions are widespread and cannot be easily resolved, consumers and merchants will have little incentive to accept these payment instruments.

The market also provides significant incentives for issuers to provide consumer disclosures and protections. Although consumer disclosures and protections are generally costly for issuers and other providers, issuers in the major U.S. pilot projects of stored-value cards have already provided written disclosures to consumers, through brochures or through information printed directly on the cards. These disclosures have generally covered basic information that consumers will need to address routine problems, such as a telephone number to call in the event of a problem and whether the card is replaceable if lost or stolen. Issuers are refining these disclosures based on the reactions of consumers and merchants and on changing technological capabilities to deliver these protections and disclosures. In addition, several issuers commented that they will seek to distinguish themselves in the marketplace by the quality of the disclosures that they provide. Issuers may also establish substantive protections not available for other payment methods to make e-money more attractive than other payment methods. Similarly, issuers may seek to distinguish themselves and their products by providing strong customer service for their e-money product.

In addition, some issuers may choose not to provide substantive protections for consumers using their e-money product. For example, some issuers argue that e-money is designed to be a cash-substitute, primarily for use in low dollar payments. Thus, they believe that consumers may not wish to pay significant fees for substantive protections and that, further, such protections are unnecessary in connection with product designed to be a cash substitute where users control the amount placed on a card or other device.

Similarly, if issuers of some e-money products prefer consumers to hold larger balances of e-money, they will likely have to provide protections against loss and theft to limit consumers' risks. Off-line stored-value card technology generally does not, at this time, provide a capability to reimburse consumers for lost or stolen cards, because the value remaining on the card generally cannot be determined and cards cannot be blocked at the point of sale in a cost-effective manner. However, in some cases, issuers have stated that, in order to maintain good customer relations, they intend to reimburse customers the first time that they lose a stored-value card, even if the disclosures indicate no such reimbursement will be made. Issuers of certain larger-value electronic money products have designed these systems with the technological capability to operate in an "on-line" manner such that the consumer more easily can be reimbursed for lost or stolen cards.

At the industry-level, at least one organization is in the process of developing consumer protection disclosure guidelines.[169] Voluntary industry-wide guidelines or codes of conduct establishing best practices for the industry may also evolve to the extent that e-money products become standardized. Issuers may also explore a self regulatory regime such as creating a voluntary "ombudsman" program for resolution of consumer complaints against issuers.[170]

Thus, issuers and other providers will likely determine over time, as more experience is gained with these new products, which of these protections are most valued by consumers. These disclosures and protections may well vary across products, depending on the type of product and its intended use. The Task Force believes experimentation with such programs may be useful and encourages the industry to continue to explore meaningful and effective self-regulatory practices.

Conclusion

Many commenters informed the Task Force that they were concerned that consumers would have neither substantive e-money protections nor information about their rights and liabilities when using e-money systems. In addition, since some stored value card products might closely resemble or be paired with traditional payment vehicles, such as credit cards, whose properties consumers understand, consumers, and perhaps some merchants, might assume that e-money is subject to the same safeguards and regulatory requirements that apply to the traditional vehicles. This potential for confusion concerns the Task Force.

In the United States, the e-money marketplace is still in a very early phase and it may be premature to establish broad substantive requirements regarding consumer disclosures and other protections. Market developments have the potential to address many consumer concerns, while some concerns may be addressed by existing legal requirements. Government action, such as supervisory guidelines that encourage issuers to provide disclosures, may help to ensure consumers receive certain disclosures, but such guidelines may not be responsive to the needs of a changing market. Accordingly, this is an excellent period for private sector initiatives to address potential consumer concerns.

The Task Force believes that it is possible at this time to identify certain disclosures that e-money issuers should provide to their customers. The Task Force recommends that industry groups and participants take steps to ensure that the features, costs, and risks are sufficiently transparent such that consumers can best make informed decisions about the relative merits of e-money products. Useful disclosures for consumers could also include information about significant user rights,

---

[169] The SmartCard Forum is currently developing disclosure guidelines. Koehler, *supra*. *See also*, Rinearson, Remarks, *supra*, discussing a possible seal of approval denoting the e-money products' consumer protections.

[170] *See* G-10 Report at 9.

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.[171]

The Task Force notes that the development of effective and meaningful industry self-regulatory initiatives may enhance the growth and development of e-money systems.

[171] *See* G-10 Report at 29. *See also* the *OCC's Stored Value Card Bulletin* for a more complete set of key consumer issues.

CONCLUSION

In this report, the Consumer Electronic Payments Task Force has both catalogued and analyzed perceived consumer concerns and explored whether they are likely to be adequately addressed by market incentives and by existing laws and practices. It is important that all participants in this emerging industry, whether in the market responses of individual firms or in collective self-regulatory efforts, recognize the legitimacy of consumer concerns — including concerns about individual privacy, the financial condition of issuers, the transparency of legal rules, and the accessibility of new payment systems — when designing, operating, monitoring, and establishing operating principles for these new products and systems. Of course, consumers also have a clear responsibility for choosing which products they are comfortable using and the amount of funds to place at risk due to potential loss or issuer failure.

The Task Force recognizes that the government possesses a broad array of instruments with which any perceived market failures might be remedied. For example, the federal government could mandate disclosures applicable to e-money products or establish substantive consumer protections to regulate this emerging, but potentially significant, means of commerce. As a less intrusive alternative, the federal government could promulgate policy statements or best practices guidelines that, without the force of law, would provide guidance to, and establish expectations for, industry participants. Government may play some role in consumer financial education, monitoring industry developments, and urging industry participants to take appropriate self-regulatory actions.

In evaluating what governmental action, if any, would be most appropriate in the context of e-money, the Task Force has carefully considered the salient features of this market. As discussed at the outset of this report, the e-money industry in the United States is at a very early stage of development. Indeed, many of the most promising products have been marketed only in pilot programs that have been limited both temporally and geographically. E-money is not now a significant factor in our economy or payments system. At the same time, the Task Force has recognized that this industry, and the underlying technology and consumer familiarity with that technology, are developing rapidly — facts which counsel both caution in government action and close attention in monitoring the market's progress. The Task Force also believes, based on the information exchanges, public meetings, and other information presented, that individuals are likely to display a diversity of values relating to the concerns considered in this report. This suggests that a flexible, rather than uniform, response to these concerns is desirable. Moreover, the Task Force believes that the firms that enter the e-money market will face considerable market pressure to acknowledge and address consumer concerns with their products. Accordingly, the Task Force believes that market mechanisms hold promise for responding effectively to many of the consumer concerns identified in this report regarding electronic money, where technological developments are making available a wide range of products.

The Task Force also has recognized the particular risks of governmental regulation of a market at this stage of development. In light of our limited current knowledge about the nature of the

market participants, the ways in which e-money products and systems will relate to their other businesses, the e-money products that will be developed and become successful, the manner in which consumers will use these products and value various features, and the extent and adequacy of self-regulatory efforts that may be undertaken on an industry-wide or firm-by-firm basis, comprehensive new regulation of e-money and/or its issuers could be counterproductive at this time. Such efforts, while premised on the best of intentions, could result in an inefficient scheme of rules with little relevance to the market that actually develops. Moreover, regulation at this stage risks quashing competition and innovation that could produce more effective operational rules. At worst, regulation could retard the development of a promising new industry that could introduce efficiencies to the nation's retail payments system. The Task Force also notes that regulation based on inadequate understanding of the relevant factors could increase the cost of new products unnecessarily. Such cost increases would impede access to these new products and systems.

While these factors lead the Task Force not to recommend specific governmental regulatory responses at this time, the Task Force does strongly recommend that market participants develop meaningful and effective policies and procedures to address specific, identifiable areas of consumer concern. The current early stage of development of e-money products is especially well suited for the flexibility of self-regulatory approaches. The Task Force also notes that market developments bear close monitoring. To date, there has been very limited practical experience with consumer usage of e-money products. Technological change can occur rapidly, however, and market developments with respect to e-money, such as product functions and features, the range of market participants, the scale of activity, and the types of consumers involved, could ultimately differ significantly from current expectations. Thus, it could become necessary in the future to reassess the need for government intervention to address significant consumer concerns that may arise. Regardless of technological and other developments, market incentives and effective self-regulatory techniques should be the first step for addressing consumer concerns.

For the foregoing reasons, the Consumer Electronic Payments Task Force recommends the following governmental and industry initiatives to address the consumer issues discussed in the report:

Recommendations

Governmental Action. The Task Force recommends that governmental action with respect to electronic money be limited at present to the following:

> *Providing Consumer Financial Education.* The Task Force believes that government may have a role in supplementing information provided by industry to help consumers become better educated and empowered to seek financial and payment products and features that will meet their individual needs. Moreover, as noted above, the Task Force believes that consumer education will foster industry efforts to address consumer concerns.

Monitoring Industry Developments. The Task Force recognizes that its knowledge and understanding of existing consumer concerns, product features, industry practices, and other relevant considerations are imperfect, and that the factors relevant in evaluating the proper role for government are subject to rapid change due to technological, commercial and other developments. Thus, it is appropriate for relevant government agencies to continue studying these aspects of e-money to protect the public interest. If self-regulatory or other efforts fail to address consumer concerns adequately, other alternatives may need to be explored.

Encouraging Appropriate Industry Action. The Task Force also believes that, through its monitoring efforts, government can act effectively as a clearinghouse for information relating to the electronic money industry, and as the industry continues to evolve can advise industry participants and groups as to the nature of consumer concerns and suggest possible avenues for addressing those concerns. Most significantly, government should encourage and foster meaningful and responsive self-regulatory efforts, where feasible, without hampering innovation and experimentation in the marketplace.

Specific Consumer Concerns. The Task Force also recommends that the following actions be taken in order to help address specific consumer concerns discussed in this report:

Access. The Task Force believes that, in considering access issues relating to e-money, it is important to evaluate the market incentives to serve all persons regardless of income level. The Task Force believe**s** that the issuers will have a strong incentive to serve all consumers particularly as the technology matures and the scalable costs decline.

The Task Force also recommends that the government address one subset of access issues — potential concerns about knowledge of how to use e-money products — through appropriate consumer education efforts, if necessary, that take into account the ongoing changes in these products and their intended markets.

Privacy. The Task Force recommends that industry groups continue to explore self-regulatory initiatives that are meaningful and effective in that they both respond to consumers' privacy concerns and include involve some means to assure adherence by individual participants. These means can involve a variety of flexible approaches.. The Task Force further recommends that industry groups explore mechanisms and technologies for providing consumers with greater control over the collection and use of information pertaining to them and their e-money transactions, consistent with the legitimate needs of law enforcement.

Financial Condition of Issuers. The Task Force recommends that the federal government continue to monitor the developments on issuer soundness. Should e-money begin to represent a substantial portion of the payments system or if particular issuers' failure begin to undermine public confidence, and should state and industry responses appear inadequate, federal government intervention could then become necessary. The Task

Force encourages all e-money issuers to disclose to consumers information relevant to issuer soundness and to inform consumers of their ability to recover funds in the event of issuer insolvency.

Consumer Disclosure and Protections. The Task Force recommends that industry groups and participants move toward adopting effective and meaningful approaches for other consumer protection and disclosure issues. These could include, for example, information about applicable fees, deposit insurance, and error resolution procedures, if any, and liability for lost or stolen e-money.[172] The Task Force further recommends that industry participants explore means to implement such policies through measures that could include product features, consumer education and marketing information, model disclosures, promotion of the policies among industry participants, and potentially the development of means to monitor, certify, and report the extent of their adoption. Policies should be designed to respond to consumer concerns in a specific and meaningful manner and be able to influence the practices of industry participants. Their effectiveness will be enhanced if they provide a mechanism for promoting conformance, such as providing effective incentives for conformance and remedies to consumers harmed by non-conformance. Such policies and their implementation must be designed so as not to lead to anti-competitive effects in the market or to preclude market participants from developing innovative methods of addressing consumer concerns.

Consumer Education and Technological Literacy. The Task Force believes that public education can play a significant role in addressing consumer concerns. In particular, the Task Force recommends that as the electronic money industry develops, appropriate governmental agencies take steps to inform the public of the basic characteristics of e-money in order to reduce the potential for misunderstanding and confusion. For example, e-money is designed to function as a substitute for cash, and in some cases may be marketed as having similar features. To the extent that marketing of this type leads to consumer confusion, the government could counter ensuing misimpressions by increasing public awareness that electronic money typically represents some form of liability of the e-money issuer; that the issuer may or may not be regulated and supervised for safety and soundness purposes; and that, even if e-money is purchased at a banking facility and issued by a bank, it is not likely to be insured by the government. The Task Force believes that such public education should compliment responses to these consumer concerns from industry groups and other participants over time as this new and dynamic industry continues to evolve.

The relevant government agencies should continue to monitor consumer concerns and industry initiatives in each of the four areas reviewed and consider whether alternative approaches are warranted in the future.

---

[172] *See* OCC Stored Value Card Bulletin, *infra*, for an example of possible disclosures.