ATTACHMENT

The Report of the Consumer Electronic Payments Task Force

April 1998

TABLE OF CONTENTS

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.[1] 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.[2] Similarly, several industry commenters noted that the use of encryption can enhance the technical security of products and provide greater privacy protection for consumers.[3]

---

[1] *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.

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

[3] 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.[4] 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.[5] 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.[6] These industry commenters also stated that they currently require their third party servicers or contractors to agree to provisions limiting their use

---

[4] 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).

[5] *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.

[6] *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.[7] Several commenters also noted that statutory and common law restricts third party access to many types of information.[8] Some commenters noted that they currently provide consumers with general information about what information is being collected and the use of that information.[9]

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.[10] 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.[11]

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).[12]

---

[7] *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.

[8] *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.

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

[10] 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.

[11] *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*.

[12] 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.[13] 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.[14]

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.[15] A consumer's right to *financial* privacy has not been established as a fundamental right by the United States Supreme Court.[16] 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.

[13] 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.

[14] 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).

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

[16] 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.[17]

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[18] at a financial institution and use electronic funds transfers ("EFTs") into or out of the account.[19] Among other things, Regulation E requires financial institutions to document EFTs in writing and to disclose certain information to their customers.[20] 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.[21] 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).

[17] 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.

[18] 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).

[19] 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).

[20] *Id.* 1693d.

[21] *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.[22] 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.[23]

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").[24]

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.[25]

---

[22] 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).

[23] 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).

[24] *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.

[25] *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.[26] 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.[27] 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.[28]

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).

[26] 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).

[27] 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).

[28] *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.[29] 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.[30] 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.[31]

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."[32] 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.

---

[29] 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.

[30] 12 U.S.C. 3401(1).

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

[32] 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.[33] 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.[34] "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.[35] 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.[36]

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.

---

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

[34] 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."

[35] 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).

[36] 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.[37] 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,

---

[37] *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.[38] 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.[39]

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.[40] 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.[41] 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 knowledge or otherwise — implementation of privacy protections by individual firms could increase consumer confidence overall and thereby foster development of the e-money market.

---

[38] *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.

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

[40] 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.

[41] 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.

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.[42]

- The SmartCard Forum's[43] 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.[44]

- 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;
  >
  > (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

---

[42] See Koehler Statement, *supra*.

[43] 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.

[44] Smart Card Forum Privacy Guidelines.

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.[45]

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 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

[45] Banking Industry Principles.

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.[46]

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.[47] 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.[48]

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.[49]

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.

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

---

[46] *Id.*

[47] 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.

[48] 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.*

[49] 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).

privacy policy. Thus, the issuer's failure to follow the terms of the policy statement could constitute a breach of contract.[50] Second, a consumer may argue that the issuer's failure to follow its privacy statement was a breach of warranty.[51] Third, consumers may have actions in tort for negligent misrepresentation.[52]

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

Several privacy concerns were brought to the Task Force's attention during the course of its

---

[50] 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.

[51] 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.

[52] 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.

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.