UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

PREPARED STATEMENT OF THE
FEDERAL TRADE COMMISSION

before the

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT
COMMITTEE ON BANKING AND FINANCIAL SERVICES

on the

Implications of Emerging Electronic Payment
Systems on Individual Privacy

September 18, 1997

I. INTRODUCTION

Chairwoman Roukema and members of the Subcommittee, I am David Medine, Associate Director for Credit Practices of the Federal Trade Commission's Bureau of Consumer Protection. I am pleased to appear on behalf of the Federal Trade Commission ("FTC" or "Commission") at this extremely timely hearing on the implications of emerging electronic payment systems on an individual's privacy and, more generally, on the level of privacy a consumer is afforded in financial transactions.(1)

One year ago tomorrow FTC Chairman Robert Pitofsky addressed the United States Department of the Treasury Conference: *Toward Electronic Money & Banking: the Role of Government* on consumer protection, privacy, access, and competition issues. He stated that government should give industry an opportunity to self regulate as these new technologies develop -- a view the Commission continues to hold. As an outgrowth of that conference, Treasury Secretary Rubin established the Consumer Electronic Payments Task Force ("Task Force") under the leadership of Comptroller of the Currency Ludwig.(2) As a member of the Task Force, the Federal Trade Commission on July 17, 1997 hosted a Task Force public workshop to address the privacy and security of electronic payments -- the same issues that this Subcommittee will be addressing. Attached is a transcript of the July 17 public workshop ("Transcript"). The Task Force plans to issue a public report on its effort by year end.

About two years ago, the Federal Trade Commission convened a series of hearings on changes in competition and consumer protection policy in response to growing global competition and developing new technology. Among the many things learned was that the old paradigms for how goods are marketed are changing, as companies begin to take advantage of dramatic innovations in communication technologies. In the next 5 to 25

years, many consumers may be making purchases on interactive television or their computer or through payment devices not yet even invented.

These new forms of marketing may be exceptionally beneficial to consumers and to competition. Consumers may have more options and greater convenience shopping on interactive television than in a shopping mall. They are virtually certain to have more relevant information -- including a wider variety of price data -- than is the case today. Tailored offerings could enable niche markets to be served more efficiently.

Changes in electronic payment systems will facilitate this marketing revolution. Great demands will be put on new payment systems to make sure they provide consumers with both convenience and security. Privacy and consumer protection issues will present an overarching policy question: What is the appropriate role of government in the development and deployment of new electronic payment systems?

On the one hand, it can be argued that without effective government regulation, there will not be sufficient public confidence in the security, effectiveness and fairness of these new electronic payment systems to permit their development. On the other hand, premature government regulation could chill or prevent the market from developing optimal solutions. Particularly at the early stages of new technologies -- where new issues will take shape gradually over time -- there is a good case for government restraint. The regulatory decisions that are made in the near future will have an enormous impact not just on electronic payment systems but on the whole marketing revolution that is occurring in the new high technology, global marketplace. For now, government should continue to monitor the development of the marketplace for electronic payment systems to ensure that consumers are getting the information they need to make informed choices about protecting the privacy of their financial transactions.

II. CONSUMER PROTECTION

The Commission has wide ranging jurisdiction over credit-related consumer protection matters pursuant to numerous statutes and trade regulation rules. In addition, Section 5 of the Federal Trade Commission Act prohibits unfair or deceptive acts or practices. One limitation on the Commission's jurisdiction involves banks and other depository institutions which are otherwise regulated by a federal banking regulatory agency.

There are three specific federal statutes the Commission enforces that are relevant to today's hearing -- the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681 *et seq*., Truth in Lending Act ("TILA"), 15 U.S.C. § 1601 *et seq*., and Electronic Fund Transfer Act ("EFTA"), 15 U.S.C. § 1693 *et seq*. The FCRA, which is concerned with the privacy and accuracy of information maintained by credit bureaus, underwent extensive revisions last year and those amendments become effective September 30.(3) The TILA and its implementing Regulation Z provide numerous protections for consumers in credit card transactions, including a $50 limitation on consumer liability for lost or stolen credit cards and the ability for consumers to dispute charges on their bill in certain situations. The EFTA and its implementing Regulation E cover a variety of electronic fund transfers

involving consumers, such as those with ATM(4) and other debit cards(5); it does not apply to transactions that do not involve a consumer's deposit account. Under the EFTA, consumer liability for unauthorized use of a lost or stolen card is generally limited to between $50 and $500, depending on when the consumer reports the loss or theft.(6)

In addition to using a credit card online, there are a number of emerging electronic payment systems referred to as electronic money. These include stored-value cards on which cash value can be stored for use by consumers at vending machines, on mass transportation systems, or other locations. Some stored value cards contain computer chips making them "smart cards," which are capable of performing numerous functions, including acting like a credit card, containing stored value, performing debit transactions, storing medical and other information, and keeping track of frequent flyer mileage. Internet-based payment systems allow value to be transmitted through computers, sometimes involving extremely small payments for bits of information or images obtained through the Internet. Stored-value cards, smart cards, Internet-based payment systems -- and new systems not yet developed -- hold tremendous potential for consumers.(7) In order to become a part of consumers' everyday lives, however, electronic money must be widely accepted, convenient, and secure. Our consumer protection experience has shown that payment systems will be accepted by consumers only when they are confident that those systems offer a sufficient level of privacy and security.(8) Electronic money presents a wide array of consumer protection issues, including liability for unauthorized use and dispute resolution procedures. While the focus of this hearing is on privacy, it is also important to address consumer protection issues. In some situations, there may be a tradeoff between consumer protection and privacy, and each must be fully understood to evaluate potential tradeoffs.

While the TILA covers credit card transactions and the EFTA covers electronic fund transfers, these statutes do not address many of the issues posed by the use of emerging electronic payment systems and associated liabilities for disputed transactions or misuse of such systems. This is especially true in the case of stored value cards which do not involve credit transactions and thus are not covered by the TILA, nor do some types of these cards involve transfers from deposit accounts that would be covered under the EFTA.

There are a number of different models on which to draw in considering what liability protections, if any, should attach to electronic money. These models include credit cards, ATM or other debit cards, and cash. It may be most instructive to examine the evolution of the credit card market. Credit cards began as mostly local, proprietary merchant cards. While there was an effort to create widely held, general purpose credit cards, that effort did not succeed, due in part to consumer concerns about liability, until Congress in 1968 and 1970, respectively, enacted federal billing dispute and unauthorized charge protections in the TILA, enforced by the FTC as to nonbanks. With these protections, credit cards instantly became more valuable than cash, especially for large transactions. Consumers who lost their credit cards or had them stolen were no longer liable (at least beyond $50) for unauthorized charges. The TILA also provides consumers with the ability to dispute charges on their bills in a number of situations, including when a

merchant did not deliver the goods. This gave consumers the confidence to deal with unknown merchants because they had recourse against their credit card issuer. Of course, these protections come at a cost to issuers and merchants, and ultimately to consumers. The question is whether the cost is worth it. In the credit card industry, the answer appears to be “yes.”

Another model for regulation of electronic money is the EFTA, which covers electronic fund transfers to and from a consumer’s deposit account. As noted above, under the EFTA, consumer liability for unauthorized use of a lost or stolen card is generally limited to between $50 and $500. However, it may be sensible in some situations to exempt from various EFTA requirements, as the Federal Reserve Board has suggested, certain types of stored value cards, particularly those acting as a substitute for handling relatively small amounts of cash.(9) Such cards are functionally similar to, but far more sophisticated and potentially more widely usable than, the subway fare cards used here in Washington. But that exception may work only so long as those cards are used for relatively small transactions, as has been initially proposed. If their use includes larger dollar transactions, consumers may want greater protections. Yet, some protections now afforded under EFTA, such as the requirement that written receipts be provided, may not make sense in a small payment context.

One question is whether consumers will demand the transaction-related protections similar to those afforded credit cards before they are willing to venture into the electronic marketplace. Consumers now feel comfortable making remote credit card purchases over the telephone or by mail. Will they demand credit-card type protections when shopping with electronic money on the Internet? More broadly, will consumers use new forms of electronic money (such as stored-value cards) online or offline for which neither the TILA or EFTA affords liability protection?

Concerns have been expressed that enhanced protections may inhibit the development of new technologies by adding regulatory compliance costs and limiting flexibility. The reverse may be true as well. Insufficient consumer protections may inhibit consumer confidence in new systems, and those systems may never reach a critical mass of acceptance.(10)

In addressing whether to expand or contract existing liability protections for various forms of electronic money to enhance consumer confidence, we observe that encryption has the potential to solve some consumer protection problems, including consumer concerns about lost or stolen cards and online transactions. Under certain encryption schemes, theft of electronic money could be useless because the encoded digital information needed to use that money would be unavailable to the thief who would not have the code or the "key" needed to access the information. A merchant’s failure to give a customer a receipt may not matter if the payment system provides proof that the electronic money was deposited. The ongoing problem of forged and bounced checks could disappear with the use of digital signatures, online verification, and other authentication devices. Thus, even without added legal protections, systems could be

designed to make electronic money better protected than cash.(11)

III. PRIVACY

Consumers may not know that the potential exists to monitor not just their ultimate purchases, but the whole online shopping process that led to their purchases. In the online environment, it will be possible for merchants not only to know what a consumer purchased, but also what other items he or she examined, for how long, and at what point this took place during the store visit. Privacy concerns also arise with the use of electronic payments in the online and offline context.

There are currently few, if any, controls on the use to which consumer transaction information is put.(12) Merchants are generally free to gather and use such information for their own purposes and to sell or rent it to third parties -- without notice to consumers. This information can then be combined with demographic information and data from other merchants to create detailed profiles of individual consumers which can enable merchants to more successfully market their goods or services. The Commission has learned from its privacy workshops that some consumers might not care whether that information is captured, especially if it results in their getting better service or individually tailored offers in the future; others might be highly offended. Shopping for some products -- books, magazines, videos(13) -- may raise more sensitive privacy concerns.

From the Commission's workshops on privacy and online transactions, it has learned that privacy is an important issue for consumers engaging in electronic transactions.(14) The Commission expects privacy to be relevant to consumers' willingness to use electronic money in making payments whether on the Internet or at the corner drugstore. Consumers' privacy can be protected in two major ways when using electronic payment systems. First, electronic transactions can be anonymous, so no personal information about the consumer is gathered. Second, consumers can be given notice of what information will be gathered about their transactions and how it will be used, some choice about such use, access to their transaction information, and assurances about the security of such information from improper access.

Anonymity protects consumers' privacy, but it also has drawbacks. It is important to recognize that the dominant method of payment in this country, both in terms of number of transactions and dollar amount transacted, is paper currency -- cash and checks.(15) Cash, of course, is a fully anonymous payment system.(16) There is no way to tie information about a transaction to a particular consumer if cash is used, which offers substantial benefits and detriments to consumers. On the benefits side, consumers can purchase items they may not want others to know they have purchased -- either due to the sensitivity of the item or a general desire not to be observed when making purchases. A major detriment, however, is that cash payments may inhibit consumers' ability to take advantage of certain consumer protections, such as those provided by the TILA and EFTA. This may sometimes be ameliorated by a receipt, if offered by the merchant, which can offer proof of purchase when a refund or adjustment is later sought. The

greater concern is that if cash is lost, it cannot be replaced. The same risk would apply to electronic payment systems that do not offer an audit trail. If those payment devices are lost, so is the value of the payments stored on them.(17)

One response to consumers' privacy concerns may be that purveyors of certain forms of electronic money will offer to ensure that transactions are anonymous.(18) Consumers will want to know that there are tradeoffs that accompany anonymity. For instance, without an audit trail, it may be impossible to replace lost or stolen cards or other payment devices. Armed with this information, consumers can then decide whether a card value replacement feature outweighs the loss of anonymity. Another concern is that scam artists may be more likely to prey upon those using anonymous payment systems. When the scam artist is caught, law enforcement authorities will be hard pressed to determine the identities of the scammer's customers, both for purposes of developing a case and for providing consumer redress. On the other hand, one important benefit of anonymity is that it could significantly reduce the incidence of identity theft. Identity theft involves a criminal takeover of a consumer's existing credit accounts or the opening of new accounts in a consumer's name.(19) Clearly it is much harder to assume someone's identity when their payment identity is anonymous.

One alternative to anonymous payment systems are systems that audit or keep track of the consumers' expenditures on the merchant end. If such a record exists, a lost or stolen stored value card could have its remaining value replaced because the issuer would be able to determine how much had been unspent on the card and might, if an online system were being used, prevent subsequent use of the stolen card. It could also give the consumer access to the array of consumer protections discussed above. The drawback of this system is that it would allow an individual's expenditures to be tracked. Given that stored value cards will often be a substitute for cash, it will mean that many everyday expenditures, which were previously anonymous, will now be recorded.

If confronted by this dichotomy of anonymity versus accountability, the market should decide which approach is preferable. In fact, a marketplace approach to this issue could well mean that both systems could thrive. Some consumers will place greater value on anonymity, others on accountability.(20) There is no reason in theory why both systems could not coexist. The key to making this marketplace work is consumer education and disclosure of important terms and information about electronic payment products.

No matter what happens, the Commission and others face the challenge of better educating consumers about emerging payment systems. There will be such a great variety of options; numerous models are already under consideration; even sophisticated consumers will find it difficult to have all the information needed to make informed choices. In particular, it will be important for consumers to understand clearly what types of information about their transactions can be captured, depending on the payment system they choose. Only when consumers have been armed with this basic information can they intelligently decide what degree of privacy they will seek for their transactions.

As noted above, the second major way to protect consumers' privacy using electronic

payment systems involves providing notice and choice to consumers. Thus, the choice between anonymity and accountability should not be the end of the privacy discussion. Even if non- anonymous smart cards are preferred by consumers because of their liability protections, that does not mean that privacy issues should be ignored. And, as noted above, privacy concerns arise even for consumers who use anonymous forms of electronic payment in the online medium.

Broadly, the Commission has learned through its public workshops that consumers are very concerned about privacy and electronic commerce. Privacy concerns can determine whether consumers enter a given marketplace. Therefore, even if consumers prefer transactions that can be examined and recorded, consumers' privacy concerns should be addressed. This can be done through notice, choice, access and security. First, it will be important to give consumers notice of what information is being collected about them and their transactions, how that information will be used, and who will have access to it. Second, consumers will want some degree of choice over the use and distribution of their transaction information. Third, consumers are interested in obtaining access to data on themselves to determine whether it is accurate and to take steps to correct inaccurate information. Finally, consumers are looking for some assurance that their data will be secure from improper, unauthorized access. Ideally, firms will even compete to offer the best privacy protections for consumers. They might also choose to offer incentives to consumers to reveal personal information.

Technology may, to some degree, allow us to transcend the dichotomy of anonymity versus accountability by making both available to consumers.(21) For example, at the July 17 Task Force public workshop, David Chaum, founder and Chief Technology Office of DigiCash, one of the many new electronic payment systems, pointed out that DigiCash offers an encrypted payment product that protects consumers' privacy while providing for some accountability.(22)

Self-regulation should be given a chance to operate, especially in this high technology arena where dramatic changes occur every few months. The Task Force heard testimony at its July 17 workshop about privacy policies that had been adopted or were under development, either by trade associations or individual firms.(23) It is somewhat premature to evaluate these policies because so few electronic payment systems have yet been made available to the public.(24) In the past, the government regulatory process has generally not been able to keep up with fast changing technological developments. The question may ultimately be whether there is any alternative to government intervention if self-regulation does not fill the void.

In any event, government can join industry in educating consumers about the legal protections available under each of the numerous payment systems that have or will enter the marketplace. Consumers will need to understand that with credit cards they get certain protections; debit cards other protections; and that some stored value cards may offer no protections at all. At some point, there may be a need to mandate uniform disclosures so that consumers can quickly and easily compare payment products and

determine which product best suits their needs.

IV. FAIR CREDIT REPORTING ACT

One federal statutory scheme governing the use of consumers' transaction information can be found in the FCRA, which is concerned with the privacy and accuracy of information maintained by credit bureaus. However, the FCRA has a significant exclusion: information about an entity's direct transactions with the consumer can be transmitted to anyone without making the source a consumer reporting agency or credit bureau.(25) Merchants are free to distribute without limitation information about their own experiences with a consumer. The FCRA applies when merchants submit information about their experiences with a consumer to a database that is created, used, or expected to be used by entities other than the owner of the database or its affiliates, to evaluate primarily consumer-initiated transactions, such as applications for credit, employment or insurance.

The Subcommittee may want to examine the impact of technological developments on the degree of protection the FCRA will afford financial information in the future. The FCRA is premised on the notion that financial information will be pooled into large databases, such as those operated by the major credit bureaus in the United States. However, developments in cyberbanking and computer networking technology suggest that the past efficiencies of large databases may not be nearly as great in the future. In the event that large numbers of individual merchants choose to report information on their transactions with consumers directly to other merchants, it will be possible to create detailed financial profiles on consumers that escape any protection under the FCRA.

In addition, in last year's amendments to the FCRA, a provision was included without the benefit of consideration in any Congressional hearing that permits affiliated companies to share consumer information, even credit reports, free from most of the FCRA's restrictions. 15 U.S.C. § 1681a(d)(2)(A) (effective Sept. 30, 1997). The Subcommittee may wish to examine whether these lessened protections for affiliated companies sharing information raise special concerns in the cyberbanking or electronic payments context, where detailed and sometimes sensitive information about consumers is gathered. The Commission will monitor the FCRA amendments when they become effective for other problems that may arise.

V. CONCLUSION

While privacy and consumer protection issues with respect to electronic money arise in a novel factual context, the issues themselves are not entirely unprecedented. Regulation of dispute resolution and privacy with respect to credit cards has generated a relevant body of experience that can apply to electronic money. It makes sense to err on the side of under rather than overregulation with respect to these new payment systems. Market-created solutions, voluntary self-regulation, and technological fixes may be sufficient. If private solutions prove inadequate, government should be ready to act. The utility of efficient, decentralized marketing on interactive television, the Internet and future

technologies is too valuable to be allowed to evaporate because an effective payment system does not develop.

Attachment:

Transcript of July 17 workshop

[Transcript attached to paper copies of testimony, but not available in electronic form.]

(1)The oral testimony and any answers to questions are my own and are not necessarily the views of the Commission or any individual Commissioner.

(2)The mission of the Task Force is "to identify and explore issues affecting consumers raised by emerging electronic money technologies (such as stored value and smart card and Internet based payment systems) and to identify innovative responses to those issues, consistent with the needs of a developing market." 62 Fed. Reg. 19173, 19174 (1997).

(3)See discussion of the FCRA in Section IV, *infra*.

(4)ATM cards, used at automated teller machines, allow consumers to obtain cash from their deposit accounts, transfer funds, obtain account balances, and, in some cases, purchase stamps or other products.

(5) Debit cards allow a consumer to authorize a merchant to electronically debit the consumer's deposit account to pay for purchases. Debit cards are accepted by a growing number of merchants.

(6)Thus, in some cases, consumer liability for electronic fund transfers covered by EFTA may exceed the absolute $50 cap found in the TILA for unauthorized credit card transactions.

Over the past few months, we have witnessed a market-driven, self-regulatory approach on the issue of consumers' liability for unauthorized debit card transactions. First MasterCard, then Visa, voluntarily agreed to provide protections greater than those required by EFTA by capping consumers' maximum liability for unauthorized use of debit cards at $50 or less (in fact, Visa has gone one step further and promised consumers no liability if the lost card is reported in the first two days).

(7)Initially, as such systems develop, industry and government will be faced with the major challenge of educating consumers about all of the various payment system options and the pros and cons of each. There will be a challenge in educating consumers about the features of multi-function chip cards, because such cards may have a similar appearance and perhaps the same corporate logos but very different functions. Consumers will need to be informed of their potential liability for the use of new types of electronic money, so that they can understand how each one differs from cash, credit cards and ATM and other debit cards. Consumers will also want to know about fees, charges, expiration dates, funds float, and the many additional competing features of payment systems, so they can better decide which payment method to use in which circumstance.

(8)The Task Force learned that recent research by Yankelovich and Associates echoes the growing concerns on the part of consumers about information and payment security and privacy on the Internet. Women, even more than men (85% versus 50%), who regularly go online say they will not do much shopping or banking over the Web until more safeguards are in place for security (surety that a credit card or bank account is not breached) and privacy (knowledge of what information is captured and how it is used). Testimony and written statement of Catherine A. Allen, CEO, Banking Industry Technology Secretariat. See Transcript at pp. 107-08.

(9)Last year, the Federal Reserve Board ("FRB") proposed amendments to Regulation E, which implements the EFTA, that would largely exempt stored-value cards from coverage, largely because they are a substitute for cash which is not accorded EFTA-type protections. 61 Fed. Reg. 37229 (1996). These amendments have not been made final based on a subsequent Congressional mandate. *See* Section 2601 of the Economic Growth and Regulatory Paperwork Reduction Act, Pub. L. No. 104-208, 110 Stat. 3009. In a March 1997 Report to Congress regarding application of the EFTA to electronic stored-value products, the FRB suggested that government regulation could be premature in this rapidly evolving market and that non-regulatory approaches, such as consumer education and industry guidelines, may be appropriate. Board of Governors of the Federal Reserve System, Report to the Congress on the Application of the Electronic Fund Transfer Act to Electronic Stored-Value Products (1997).

(10)One has only to look at the history of “900" numbers to see what happens when consumers lose confidence in a payment system. 900 numbers had a huge potential as a consumer payment system because every telephone could essentially be used as a credit card and more people have telephones than credit cards. The industry had a strong start, achieving $6 billion in sales in 1991. However, the industry was soon beset by fraud, included phony “gold card” credit cards and fake job listings. *See, e.g.*, FTC v. Interactive Communications Technology, Inc., Case No. CVF91018 REC (E.D. Cal., filed Jan. 18, 1991) ("gold" credit cards usable only for limited catalogue shopping); FTC v. Transworld Courier Services, Inc., Case No. 1:90-CV-1635-JOF (N.D. Ga., filed July 26, 1990) (phoney "job lines"). Efforts at providing protections to consumers were resisted by the industry. Consumers soon lost confidence in 900 numbers as a payment system and annual sales dropped dramatically to $300 million. Only after Congress directed the Federal Trade Commission and Federal Communications Commission to regulate the industry did consumer confidence begin to return, with sales in 1995 rising to $450 million. Consumers now are entitled to price information and to dispute charges without having their basic phone service terminated. *See* Telephone Disclosure and Dispute Resolution Act, 15 U.S.C. § 5711 *et seq*. (1992) and the Federal Trade Commission’s Trade Regulation Rule Pursuant to the Telephone Disclosure and Dispute Resolution Act of 1992, 16 C.F.R. Part 308 (1993).

(11)Another major issue is international jurisdiction. In the United States we are accustomed to controlling payment systems domestically. In the future, we may have to confront electronic money that is issued abroad, not easily traced, lacks consumer protections, and may be beyond the ability of domestic law enforcement agencies to challenge. In the conventional consumer protection field, it is becoming increasingly clear that international coordination and cooperation -- bilateral and multilateral -- is essential if consumers are to be protected. There is every reason to expect that regulation of electronic money will require attention to the international dimension.

(12)*See* discussion of the FCRA in Section IV, *infra*.

(13)Information about video rentals is protected under the Video Privacy Protection Act, 18 U.S.C. § 2710. However, this law does not protect information about which videos a consumer considered during the shopping process, and such information could be captured while shopping online.

(14)See Staff Report: Public Workshop on Consumer Privacy on the Global Information Infrastructure (December 1996), pp.12-15.

(15)Remarks by Chairman Alan Greenspan at the Conference on Privacy in the Information Age, Salt Lake City, Utah, March 7, 1997. Chairman Greenspan noted that checks, unlike cash, leave a paper trail which can compromise privacy, but it is a less efficient and accessible trail than when available newer technologies are used.

(16)According to Chairman Greenspan:

Paper currency is, of course, the ultimate protector of anonymity, for making ordinary payments at the retail level. It is, thus, a measure of how valued is privacy in our system that inroads into the use of

currency have been slow, and halting, in the face of technologies one would assume would have quickly buried the presumed inefficiency of paper transactions.

Remarks by Chairman Alan Greenspan at the Conference on Privacy in the Information Age, Salt Lake City, Utah, March 7, 1997.

(17)Of course, consumers may still find the systems' benefits are worth this risk. For example, there may be no other way to make micropayments of fractions of a cent to purchase information on the Internet without using electronic payments. There is also the convenience of not having to worry about exact change when making purchases.

(18)Testimony at the Task Force's workshop suggests that in some instances consumers should be wary of claims of anonymity. For instance, David Chaum of DigiCash testified that prepaid telephone cards, while seemingly anonymous, may not be. It might be possible to examine the record of calls made from a given card to identify the individual caller, possibly through repeated calls to home or to the office. Therefore, consumers and consumer protection agencies will have to assess critically claims of anonymity.

A separately important concern with anonymous payment systems is the possibility they will facilitate criminal activity, including money laundering and improper money transfers. As a law enforcement agency, the Federal Trade Commission is particularly sensitive to those concerns. There are some safeguards that could be built into payment systems, such as limiting the amount of money that could be stored on a card, that would at least make it more difficult to use the system to violate the law. The Subcommittee may want to consult with the Treasury and Justice Departments about the criminal law enforcement aspects of this issue.

(19)Credit identity theft was the subject of two workshops held at the Commission in 1996. From those workshops, we are aware of only some but by no means all of the steps financial institutions have taken to protect themselves and consumers from fraudulent transactions. One example would be software that monitors consumers' transactions to detect unusual account activity. This can result in a call to the consumer to verify that particular transactions were initiated by the consumer. While this certainly has the potential for invading a consumers' privacy, or the privacy of certain family members vis-a-vis each other regarding particular purchases, it has generally been accepted as a reasonable means of protecting both consumers and credit card issuers from fraudulent use of a credit card account. Clearly, any fraud detection methods employed by financial institutions have to be weighed against consumers' privacy interests. In some cases, it may be a matter of educating consumers about what steps are being taken and why they are in the consumers' interest.

(20)The 7th Annual Survey conducted in 1997 by the Graphics, Visualization, & Usability Center, College of Computing, Georgia Institute of Technology, reveals that when asked to rate their agreement/disagreement on a 5-point scale, with '5' representing strong agreement, most people surveyed preferred anonymous payment systems on the Internet over more accountable payment systems (3.93). The survey was conducted on the World Wide Web by eliciting respondents from popular Web sites, and is therefore non-random.

(21)Technology may help to resolve the issue of online collection of information from consumers and the attendant privacy concerns. At the FTC's workshop on online privacy this past June, there were many demonstrations of innovative software that can potentially empower consumers to protect their own privacy online (as well as their family members' exposure to undesirable materials). For example, consumers may soon be able to load software onto their computers that can filter out Web sites that are not rated privacy protective, either by the site itself, or more likely, by third party rating services. The next step will be software that allows consumers to engage in an electronic dialogue with Web sites over how their personal information should be handled. Time will tell whether this technology is adequate to protect consumers' privacy both now and as new technological developments emerge.

(22)Under the DigiCash model, consumers obtain "payment packets" from DigiCash. Merchants who accept these DigiCash payment packets cannot identify the payor. Instead, merchants forward encrypted payment packets to a bank that verifies and authorizes payment. However, the bank does keep a record of which demands for payments of particular packets have been submitted and by whom. If the consumer identifies to the bank which payment packets were his or hers, the bank can then determine whether they had been presented for payment or not. If no payments had been made of those specified packets, the bank could cancel payment rights for those packets and reimburse the funds to the consumer. In addition, the bank has the equivalent of a receipt for each transaction, indicating the entity that sought payment for a particular packet. If this system works as promised, it offers the opportunity for consumers to shop anonymously with payment packets, but still have some recourse if, for example, their computer that stored the payment packets fails.

(23)Through its workshops, the Commission is aware of efforts by financial services firms and trade associations to develop policies concerning the collection and dissemination of consumer information. Firms or trade associations in other sectors, such as direct marketing, have also been working to develop such policies. It is difficult to compare the progress made by the financial services industry with other industries because the Commission has not conducted a comprehensive survey.

(24)The government can, however, play an effective role in support of self regulation. Once firms voluntarily offer consumers privacy protections for their electronic payments, and consumers rely on those representations in choosing which electronic payment system they want to employ, a firm’s failure to honor those offers would almost certainly violate the Federal Trade Commission Act’s prohibition on unfair or deceptive trade practices. In other words, if firms act responsibly and voluntarily offer privacy protections to consumers, the FTC already has the legal tools needed to enforce adherence to those stated policies.

(25)Section 603(d) of the FCRA, 15 U.S.C. § 1681a(d) ("The term "consumer report" . . . does not include (A) any report containing information solely as to transactions or experiences between the consumer and the person making the report.").