years, many consumers may be making purchases on interactive television or the 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 emerging 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

involving consumers, such as those with ATM (4) and other debit cards (5); it does not

merchant did not deliver the goods. This gave consumers the confidence to deal w 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 l to between $50 and $500. However, it may be sensible in some situations to exe exempt various EFTA requirements, as the Federal Reserve Board has suggested, certain 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

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 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) 0.003 offended. Shopping-fllt mafendeoher tdcjrdua itivTc
info1rCS1 c..003 Tc 0.003 Tw 17.19 0fhoppingMch can eT-4
le ix2(l)-pe* [(i)-2(nf)(y)20( )-10(w)2(or)3(ks)-1(hops)-(u)-10(

greater concern is that if cash is lost, it cannot be replaced. The same risk would a 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

payment systems involves providing notice and choice to consumers. Thus, the ch 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

determine which product best suits their needs.

## IV. FAIR CREDIT REPORTING ACT

(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 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 appropri 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 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) ("gol cards usable only for limited catalogue shopping); FTC v. Transworld Courier Services, Inc., Case No. 1:90-CV-1635-

currency have been slow, and halting, in the face of technologies one would assume would have q
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 wa a

(22)Under the DigiCash model, consumers obtain "payment packets" from DigiCash. Merchants w
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 sent to 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,
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 s
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 andpdient8(i)-65.831001 Tw 21.-12(ut)-2(a)-28(s)9( 2(w)na(a