

Testimony of Ralph Shalom, Associate General Counsel, First Data Corporation
Before the House Energy and Commerce Subcommittee on Oversight and Investigations
Thursday, September 21, 2006

Good morning, Mr. Chairman and members of the Committee. My name is Ralph Shalom, and I am Associate General Counsel at First Data Corporation. I am pleased to be here today to discuss First Data's role in the payments industry, specifically merchant processing, as the Committee continues its hearings into Internet child pornography.

Let me begin my testimony by describing First Data, and the unique role we play helping millions of consumers, businesses, and governmental entities buy products and services on a daily basis. Most people don't realize it, but First Data's products and services touch people's lives every day. We make buying and selling easier. It is that simple. Many of you do business with First Data everyday - whether you are using an ATM/debit card to pay for gas at the gas station, writing a check to pay for groceries, buying a book online, getting cash from an ATM, paying for dinner with a credit card or using a gift card - there is a good chance that First Data is moving that transaction at least part of the way between the merchant and the consumer.

Although we have many interesting products and services that provide some type of payment processing, I will focus my testimony on merchant processing. Our merchant services business segment facilitates the ability of merchants to accept consumer transactions at the point of sale, whether the merchant operates a physical store (brick and mortar) or whether the merchant has a virtual - or online - presence. Our services enable businesses of all sizes to accept various forms of payments from consumers, including

credit and debit cards. The term “processing” can be described as those functions associated with authorizing, capturing, and settling merchants’ credit, debit, stored value and loyalty card transactions. We provide merchant processing services for some 3.5 million merchants in the U.S.

At First Data, a majority of these services are offered through alliance relationships with financial institutions. These arrangements are established as either revenue sharing alliances or equity alliances. We have revenue sharing alliances with financial institutions like SunTrust, CitiGroup, and Huntington Bank. We have equity alliances with major financial institutions like Wells Fargo, PNC, and JPMorgan Chase. Our equity alliances are run as independent companies and compete against one another and against our Revenue Sharing Alliances in the market place.

Understanding How New Merchants Are Acquired

When we sign up, or acquire, merchants for processing services, we make great efforts to understand (1) who are our clients and (2) what type of products or services do they sell? The answers to these questions not only drive certain technical aspects of how the accounts are set up, but these questions also inform us of the risk that the merchant might present to us and, indeed, whether we are willing to accept the merchant at all. When merchants apply for services, they are asked questions to help us understand who they are, including obtaining their taxpayer identification number or their Social Security number. If the sale is made face-to-face, sales representatives are trained to make notations about the physical aspects of the merchant. If the merchant is an online vendor,

we require the merchant to provide us with its Web site address which is then reviewed by our credit department.

There are many businesses that we simply refuse to accept under the credit policies in which we operate. Each of the alliances has its own credit policy that was developed jointly with First Data. None of these policies allow for adult online video content.

Merchants whose businesses are involved in what we understand to be illegal dealings, including the sexual exploitation of children, are automatically excluded. Several years ago we also made the determination to avoid businesses providing sexually oriented on-line video content. When a merchant applies for an account with us, as part of the initial underwriting reviews, we pull a credit report, review the materials provided with the application, check the industry High Risk files, and check the Web site if the business is described as being online. We might disqualify a merchant from receiving an account from us if the merchant is involved in online gambling, online cigarette sales, online firearms sales, or if they are involved in sexually oriented online video content, to name a few reasons. In addition, we conduct additional policing on non face-to-face prescription drug sellers.

Understanding How Merchants Are Monitored for Fraud or Other Illegal or Unacceptable Practices

Merchants don't always tell us the truth when they describe what they are going to sell. Even if they have provided a processor like us with a Web site that describes their

business, a merchant can easily operate other Web sites that present a different business proposition to the consumer. There is nothing in the credit card transaction record that would prevent a merchant from taking transactions obtained on one Web site and submitting them through an account that, in our records, we have associated with a legitimate Web site. Also, sometimes legitimate merchants will get co-opted into running transactions for another business.

As a result, our review of merchant activity continues beyond the initial underwriting of the account. We review the transaction activity for our merchants to determine if their processing materially changes in ways that suggest the merchant is not who they claimed to be. Further, we continually evaluate new software and technology solutions to help us identify when a merchant has associated itself with illegal activity. Equally important, we maintain a liaison with law enforcement so that we can be notified when they are targeting specific merchants for illegal behavior.

From a merchant processing perspective, we see the financial piece of the transaction, which for most transactions is simply the date, time, amount of sale and card number, as well as industry specific criteria necessary for assisting bank card issuers in making authorization decisions and for qualifying a transaction through the card associations (e.g. VISA and MasterCard) to obtain certain interchange rates. In other words, we don't know what the cardholder saw or what the cardholder was told when he or she presented their bank card account information to complete the sale. Nor do we know what the merchant presented to the cardholder that generated the sale.

With billions of transactions running through our systems, individual transactions cannot be investigated. However, we do review merchant deposits for patterns that, in our experience, suggest the merchant may be of a different type than we originally understood. For example, we might look at significant increases in transaction volume, in excess of what we might expect as normal growth; patterns of transaction amounts larger than would be expected for the type of business described; an abnormally high number of transactions which are questioned by the cardholders or charged back; among others. We also run bank card transactions through more than 100 pattern filters to identify which merchants merit an additional review.

We have a fraud prevention department that is tasked with reviewing accounts that have tripped some of our suspicious activity patterns to determine whether there is anything that suggests we can or should stop providing processing services. As a result of the work of this department, we have terminated nearly 4,000 merchant accounts in the past five years. In preparation for this hearing, I have surveyed our managers in these areas and it appears that we have not seen incidents of child pornography in these reviews. However, we have identified instances where merchants submitted transactions for others, or we have found that some merchants were involved in sexually explicit materials. In these cases, we immediately shut down the merchant's accounts. It may very well be that some of these accounts that we shut down could have carried transactions originating with sexually explicit material.

Let me be very clear: We take this issue very seriously and have cooperated extensively with law enforcement. For instance, we have kept accounts open for a limited time when we have been told that is necessary to facilitate an ongoing investigation and have provided information and access to funds which have resulted in criminal convictions and significant seizures of funds associated with criminal activity.

First Data Participates in the Financial Coalition Against Child Pornography

At First Data, we have no tolerance for the sexual exploitation of children. Although identifying online merchants engaged in child pornography can be challenging, we are committed to taking additional steps to help identify these entities and prevent them from using our systems to fund their illicit activities. First, we are participating in a pilot project with MasterCard to identify illegal or unacceptable merchant activity by searching the Internet for Web sites that engage in the sexual exploitation of children. Second, we participate in the Financial Coalition Against Child Pornography. As you know, the goals of the Coalition are to: (1) establish a global clearinghouse on child pornography; (2) create a proactive system to enable the financial services industry to deal with illegal uses of its systems to disseminate child pornography; (3) create a system for reporting suspected child pornography; and (4) implement monitoring and due diligence checks. Two of the key components of the Coalition are the creation of the clearinghouse, which will facilitate the sharing of information among the payments industry. We believe this will be a valuable tool to help eradicate such illicit activity from the payments system. In addition, the Coalition's efforts to determine the best way to perform test transactions on targeted Web sites will help us more quickly and

accurately identify who is processing those particular payment transactions, so that we can work effectively with law enforcement to shut them down.

Conclusion

In summary, First Data takes seriously its role in protecting the payments system from activities that are illegal or against our policies and the card association rules. We employ effective, front-end due diligence procedures to help us identify unqualified merchants, and we impose checks on existing merchants when they trip any one of our existing suspicious activity patterns. Finally, the measures being undertaken by the Financial Coalition Against Child Pornography will help all of us in the payments system identify and deter the funding for the online exploitation of children.

Thank you.