



FIRST DATA TECHNOLOGIES  
6200 SOUTH QUEBEC STREET  
ENGLEWOOD, CO 80111



March 22, 2000

Secretary  
Federal Trade Commission  
Room H-159  
600 Pennsylvania Avenue, N.W.  
Washington, D.C. 20580

RE: Gramm-Leach-Bliley Act Privacy Rule: 16 CFR Part 313-Comment

Ladies and Gentlemen:

We are writing on behalf of First Data Corporation ("First Data") and its subsidiaries, including First Data Resources, Inc. ("FDR"), Western Union Financial Services, Inc. ("Western Union"), Integrated Payment Systems Inc. ("IPS") and Telecheck Services, Inc. ("Telecheck"). First Data employs over 30,000 people and is a global leader in payment services. It processes the information that allows millions of consumers to pay for goods and services by credit or debit card at the point of sale, over the Internet, by check or by money wire. Its primary subsidiaries are engaged in diverse businesses:

**FDR** is the world's largest third-party credit and debit card transaction processor, providing a comprehensive line of products and services to more than 1,400 credit, debit, commercial, private label and oil card issuers worldwide.

**Western Union** enables consumers and businesses to securely transfer money or make payments using money orders and other electronic systems. Western Union operates through approximately 82,000 agent locations in 176 countries.

**IPS** is a leading provider of official checks and money orders to banks and savings institutions. It issues millions of payment instruments for thousands of financial institutions across the country.

**Telecheck** is the world's largest check acceptance company. It provides a broad range of check guarantee, check verification and collection services to merchants and financial institutions. TeleCheck's annual check volume represents more than 2 billion transactions. TeleCheck has more than 200,000 customers worldwide.

Given the nature of First Data's businesses, we have serious concerns about the Privacy Rule and its impact on our ability to provide our services to consumers and our business customers at the lowest price. Our comments are as follows:

### **Comments Regarding the Definitions in Part 313.3:**

#### "Affiliate and Non-Affiliated Third Party".

First Data has over 30,000 employees and over 82,000 Western Union agent locations. Since business entities must operate through their employees and agents, we are concerned about the treatment of employees and agents under the Rule. Currently, the Rule defines "non-affiliated third party" to include natural persons, but to exclude affiliates and persons employed jointly by a business entity and a nonaffiliated third party. The Rule does not address how the employees and agents of a business entity itself are treated. We suggest that the definitions of "affiliate and non-affiliated third party" make clear that employees and agents are not "non-affiliated third parties". The Rule should also make clear that disclosure of information by consumers to employees and agents of a business entity constitutes disclosure of the information by the consumer to the business entity. In addition, the Rule should make clear that the disclosure of information by the corporation to its employees and agents does not constitute a disclosure of information to non-affiliated third parties.

#### "Clear and conspicuous"

In the past, federal agencies have provided samples of compliant disclosures (e.g. the Federal Reserve with respect to Regulation E). We would request that a similar procedure be followed here. Such samples would substantially reduce the confusion likely to be experienced by consumers who will otherwise be suddenly provided with dozens of privacy notices, all drafted in different ways. It would also be helpful to businesses that do not know exactly what disclosure is required to be made.

#### "Collect"

We believe that the information collected that is subject to correction by a consumer must be both organized in a database and retrievable on a personally identifiable basis. While most information held by financial institutions is organized, a substantial portion of such information is not placed in databases and is not retrievable on a personally identifiable basis. For example, most banks have in archives copies of millions of checks, most of which contain names and perhaps bank account numbers or driver's license numbers and other personal identification information supplied by the payee or indorser. This information, however, is not organized in a database that is retrievable on a basis personally identifiable with the payee. It is usually organized by the name of the account holder, date and number. Requiring financial institutions to give consumers access to information that is not retrievable by any means identifiable with such consumer would be extremely burdensome. It might cause financial institutions to create additional databases containing more specific consumer information. Such a result would be contrary to the underlying policy behind passage of the GLB Act, which is intended to limit, not expand, the collection and use of consumer information by financial institutions.

#### "Customer and Customer Relationship"

Understanding that the proposed Rule is intended to be, for the most part, uniform with the Rules proposed by the bank regulatory agencies, it would be helpful if the FTC deviated from its desired uniformity when examples are provided so that the examples illustrate the kinds of relationships created by non-bank financial service providers, such as money order sellers and money transmitters.

The commentary to Part 313.3 (h) implies that a financial institution that only performs isolated transactions for a consumer may have a customer relationship with the consumer. The commentary in the second paragraph states, "A consumer would not necessarily become a customer simply by repeatedly engaging in isolated transactions..." This statement contradicts the commentary to Part 313.3 (i) which states, "The Commission has interpreted the Act as requiring more than isolated transactions between a financial institution and a consumer to establish a customer relationship." We believe that the Rule should state that "a consumer *does not* become a customer simply by repeatedly engaging in isolated transactions." One would hardly expect a bank to provide a privacy notice to an individual whose account was at a different bank and who only used the bank's drive up ATM, though repeatedly, simply because it was on the way home. If a series of isolated transactions is not excluded, then great uncertainty is created as to whether or when the "continuing relationship" is created. The creation of a long-term relationship, such as the opening of an account or the purchase of an insurance policy should be required to create the customer relationship. We believe that isolated transactions should be defined as those transactions that require the consumer to start fresh or anew with the business entity each time a transaction occurs. The examples given in the regulation are illustrative of these types of transactions.

We believe the Rule should also state that when transactions are conducted anonymously, then no customer relationship is created. Anonymous transactions are those transactions in which insufficient information is collected by the financial institution to identify the consumer. This occurs when the consumer's name and/or address are not collected. These types of transactions are common, particularly with respect to the sale of money orders or prepaid phone cards.

#### "Financial Institution"

First Data believes that companies that have no "consumers" or "customers" should be excluded from the disclosure requirements of the Rule. The Rule's limitations on reuse of the nonpublic personal information that those companies possess is adequate to protect consumers from the use of their information without their knowledge. Requiring companies that only perform data processing for financial institutions to make separate disclosures to consumers with whom the data processors have no relationship would only confuse consumers. For example, if a data processor for a bank were required to provide disclosures to the consumers whose personal information is housed and processed on its computer system, the following anomalies would result:

- Those consumers would receive two separate notices governing the same information;
- One of the notices would be from an entity that the consumer has never heard of, and which has no authority to take independent action with respect to the consumer's information;
- If a consumer "opted out" in response to the data processor's notice, but not in response to the bank's notice, the data processor would have no contractual authority to take actions contrary to its bank client with respect to the information; and
- The data processor's actions would represent a needless intrusion into the important relationship between the bank and its customer.

## "Nonpublic Personal Information"

### 1. Alternative Definitions.

The Notice provides two alternative definitions of "nonpublic personal information" for comment. Both alternatives are based on a definition of "personally identifiable financial information" that includes virtually any information that a financial institution obtains about a consumer. We believe this interpretation of the GLB Act is unsupportable, and that these alternatives deviate significantly from the clear language and intent of the GLB Act.

Title V, Section 509(4) of the GLB Act defines "nonpublic personal information" as "personally identifiable **financial** information (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer. . . ; or (iii) otherwise obtained by the financial institution." Basic rules of construction dictate the conclusion that Congress would not have used the word "financial" in this phrase if it had intended the definition to encompass all information obtained by a financial institution. The statutory definition is carefully crafted to address information that is financial, uniquely in the hands of a financial institution, considered private by the consumer, and a proper subject of protection.

The Notice, on the other hand, proposes to define "nonpublic personal information" to include information that is not financial in nature, is not uniquely in the hands of a financial institution, and is not traditionally considered private information. This information, which includes the name and address information often referred to as "header information," is freely available to and by non-financial institutions. Some uses of this information are:

- Verification of name and address information on applications for financial or other services;
- Use by law enforcement to locate suspects and witnesses;
- Use by the IRS or other government agencies to redirect returned mail, or to verify social security numbers;
- Use by mutual funds to locate lost shareholders, or by banks and other financial institutions to return unclaimed funds; and
- Verification of identity required for the use of digital certification in e-commerce.

While the commentary suggests that trying to distinguish financial from nonfinancial information would be too difficult, this distinction has been made as a matter of course under the Fair Credit Reporting Act ("FCRA"). "Header information" is outside the scope of the FCRA primarily because it is **not** financial in nature. Furthermore, nothing in the proposed Rule will prevent or limit the ongoing compilation and availability of this information. Rather, the regulation as proposed would single out financial institutions as the only entities that are significantly restricted in their use and disclosure of this information. That result serves no consumer interest or public purpose. It is therefore difficult to ascertain a rational basis for the proposed Rule to deviate so significantly from the apparent intent of Congress in defining nonpublic personal information.

If the currently proposed alternatives are not withdrawn or revised, First Data would view Alternative B as the better alternative. The vast majority of publicly available information is obtained from entities other than a public source. To require financial institutions, as opposed to other entities, to obtain this information directly from the public source in order to use or disclose it is equivalent to a prohibition, since the cost and burden of obtaining information directly from a public source is prohibitive. By stating

its preference for Alternative B, First Data does not intend in any way to limit its strong objection to the proposed definition of nonpublic personal information in the proposed Rule.

We oppose any variation that requires a financial institution to undertake procedures to establish that information is, in fact, available from public sources before the institution may treat it as "publicly available information." Requiring a financial institution to undertake such procedures would generally be equivalent to Alternative A, since public availability cannot be confirmed without going directly to the relevant public source.

## 2. Compilation of Data Without Personal Identifiers

The term "nonpublic personal information" should not include information about a consumer that contains no indicators of a consumer's identity. Aggregate information about loans, payment history, income and similar factors is used to increase the validity and accuracy of credit scoring and other predictive products that are used by financial institutions to control risk and support fair lending practices. Without such aggregate information, third parties who provide these products would have great difficulty meeting the regulatory requirement that such products be "empirically derived, demonstrably and statistically sound." If this information were subject to consumer opt-out, the information base for these products arguably would not be representative or statistically sound. For these reasons, we believe aggregate information of this type should be explicitly excluded from the scope of the Rule.

### **Comments Regarding Other Provisions:**

#### Part 313.4: "When Initial Notice is Required."

We seek additional clarification with respect to when a company, such as Western Union or IPS, which transacts its business primarily in a series of isolated transactions, is required to provide the initial notice. As stated above, the commentary to Part 313.3 (i) correctly states the Commission's position: "The Commission has interpreted the Act as requiring more than isolated transactions between a financial institution and a consumer to establish a customer relationship." We believe that the Rule should state that "a consumer does not become a customer simply by repeatedly engaging in isolated transactions." If this modification to the Rule is made, then it is clear that no "initial notice" is required until some other relationship is created. However, if a "customer relationship" can be created as a result of a series of isolated transactions, then under the Rule as proposed one does not know when in the series the customer relationship is created for purposes of determining when to give the initial notice.

#### Part 313.4: "How to provide notice."

We believe that, whenever a customer chooses to transact business with a company electronically, electronic delivery of the notice should be an acceptable method of delivery, regardless of whether the customer agrees. Requiring written delivery in such a case is unduly burdensome and impedes the development of electronic commerce. In addition, requiring written delivery may require the collection of additional information from the consumer, such as a mailing address.

For telephone transactions, we believe that, if the consumer initiates the relationship over the telephone, the institution should not be required to obtain the separate agreement from the consumer to deliver the privacy notice at a later date. The consumer's consent to later delivery should be implied from the consumer's initiation of the transaction and delivery of the privacy notice after delivery of the product or

service should always be allowed. The notice could be mailed on the next business day and the consumer could be given a reasonable time period (30 days) to opt out before the information could be used for marketing purposes. Telephone transactions systems are extremely time sensitive. Each second added to the transaction time increases the cost and the price to the consumer. No consumer would reasonably expect a financial institution to provide written notice over the telephone. Therefore, asking for the consumer's agreement not to do so would be without benefit and would only increase the cost of the transaction.

For transactions initiated at automated machines, whether the traditional ATM or the newer multi-transactional machine ("ATMs"), which are not owned by the financial institution performing the transaction for the consumer, delivery of a privacy notice is also impractical. An ATM screen is simply not large enough to display several pages of text in a consumer-friendly and readable method. In addition, programming ATMs to display third party privacy notices is impractical and would likely result in a significant slowdown in transaction processing. These types of transactions should be treated in a manner similar to telephone-initiated transactions. The consumer's consent to later delivery should be implied from the consumer's initiation of the transaction and delivery of the privacy notice after delivery of the product or service should always be allowed. The notice could be mailed on the next business day and the consumer could be given a reasonable time period (30 days) to opt out before the information could be used for marketing purposes.

The commentary indicates that the initial notice may be provided at the same time a financial institution is required to give other disclosures required by law and regulation. The Rule should clarify whether notices, initial or annual, can be included in the same document or communication as other regulatory notices. Permitting combined notices would provide significant cost savings to financial institutions and, ultimately, to consumers.

Rules regarding delivery of the required notices should be consistent with rules concerning the delivery of other required disclosures under current regulations. Creating a separate set of rules is needlessly confusing. For example, current regulatory proposals regarding electronic delivery of disclosures should be the model for privacy disclosures as well. Similarly, existing rules provide guidance as to who should receive notices, including jointly liable parties. Inconsistent requirements may require reprogramming by processing systems that are configured to meet existing regulatory requirements.

#### Part 313.4 (d) (5): "Examples of Providing Notice"

We request that the following example be added to the current list of examples of how to provide the notice:

"You may reasonably expect that a consumer will receive actual notice of your privacy policy and practices if you: ...

(E) Make a written copy of your privacy policy and practices available in the same manner as other forms used to effect the financial transaction, such as providing the policy in the same display rack used for other forms or prominently displaying the policy on the counter used to transact business with the consumer in person or providing the policy on your website for consumers who transact business with you on your website."

Consumers are quite familiar with the form display racks commonly used by financial institutions to make forms and other important information available to consumers. For companies that only engage in isolated transactions, requiring delivery of the notice at the time of each transaction unnecessarily increases the cost. In the case of our company, unless this type of delivery is allowed, millions of duplicate forms may be delivered each year to consumers at a cost running into millions of dollars.

With respect to Part 313.5 (b), we also believe that a company should be allowed to meet the annual notice requirement for consumers who do business with it in person by making the policy available to all consumers at all times in a display rack at the point of sale. Similarly, posting of the privacy policies on a website should be deemed an adequate annual notice for those consumers who transacted business with you on your website. If such is not the case, companies that only engage in isolated transactions might need to develop customer mailing lists and perform annual mailings to people who do not receive mailings today. Such a result is inconsistent with the purpose of the GLB Act, which was adopted to limit, not expand, the collection and use of consumer information.

Part 313.5 (c): "Termination of Customer Relationship"

Many businesses have customer relationships that do not last one year. We believe that a customer relationship should be deemed ended if there has been no communication with the consumer for a period of 3 months. This shorter period will allow businesses with more transient customer bases to purge databases more frequently and avoid the cost of mailing annual notices.

Part 313.8: "Form and Method of Providing Opt Out Notice"

We believe that financial institutions should not be required to provide self-addressed stamped envelopes with the notice form in order to provide a reasonable means to opt out. This unduly increases the cost of providing the notice. It should be acceptable to allow the consumer to mail the opt out form to a central office for processing at the consumer's expense. This position is consistent with the telemarketing laws of many states in that those laws also require a small charge to be paid by the consumer to be placed on a "no call" list.

Part 313.8 (e): "Duration of consumer's opt out direction."

A time limit needs to be placed on how long companies must keep a consumer's opt out direction. Otherwise, these records would have to be kept forever. We believe that a reasonable time period would be created if the opt out direction expired one year after the customer relationship terminates. If such a time limit does not exist, matching common customer names and addresses becomes increasingly unreliable as many consumers move on a frequent basis.

Part 313.13: "Limits on Sharing of Account Number Information for Marketing Purposes"

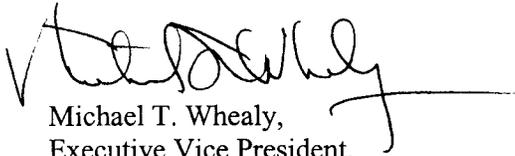
As the world's largest third-party credit and debit card transaction processor, we prepare and mail millions of card statements each month on behalf of card issuers. A common practice is to insert a marketing piece in the envelope containing the statement. We do not believe that Congress intended to prohibit this practice when it adopted Section 502 (d). We believe that an exception should be created for this practice. In addition, we believe that a consumer should be allowed to consent to disclosure of his or her account number for marketing purposes.

Part 313.16: "Effective Date"

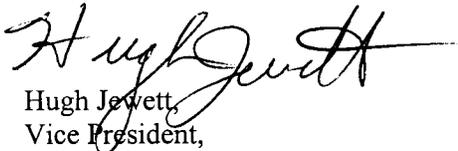
We believe that the regulations should not be effective for a time period of one year. The proposed 6-month time period for implementation would be extremely burdensome for companies like Western Union, which have thousands of locations and millions of consumers who use our services. In addition, the 6 month time period is not adequate for data processors, like FDR, which must obtain an appropriate understanding of its clients' requirements and then implement programming changes that are responsive to those needs. The additional 6-month time period would allow us to implement our privacy program in a more orderly and cost effective manner.

We appreciate the opportunity to comment on your proposed regulations. If you have any questions or need additional information, please contact either of us.

Respectfully submitted,



Michael T. Whealy,  
Executive Vice President,  
Chief Administrative Officer  
and General Counsel  
(770) 857-7103



Hugh Jewett,  
Vice President,  
Government Relations  
(303) 967-7691