



March 31, 2000

National Fraud Center

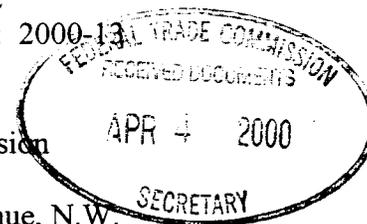
Communications Division
Office of the Comptroller of the Currency
250 E Street, S.W.
Washington, DC 20219
Attention: Docket No. 00-05

Ms. Jennifer J. Johnson
Secretary
Board of Governors of the Federal Reserve
System
20th and C Streets, N.W.
Washington, DC 20551
Re: Docket No. R-1058

Robert E. Feldman
Executive Secretary
Attention: Comments/OES
Federal Deposit Insurance Corporation
550 17th Street, N.W.
Washington, DC 20429

Manager, Dissemination Branch
Information Management & Services Division
Office of Thrift Supervision
1700 G Street, N.W.
Washington, DC 20552
Attention: Docket No.: 2000-13

Secretary
Federal Trade Commission
Room H-159
600 Pennsylvania Avenue, N.W.
Washington, DC 20580
Re: Gramm-Leach-Bliley Act
Privacy Rule, 16 CFR Part 313-Comment



Re: Comment to Privacy Rules

Dear Sirs and Madams:

Please accept this comment on the proposed rules promulgated pursuant to the Gramm-Leach-Bliley Act. ("GLB Act"). This letter is being sent to all the interested agencies as it concerns provisions that are common to both sets of proposed rules.

Initially, our interest in the proposed rules stems from our corporate mandate to provide solutions to the public and private sectors in the fight against fraud. Although National Fraud Center is a for profit entity with clients throughout the business world, we strive to provide assistance whenever we can to governmental entities that are also involved in fraud prevention. An example of National Fraud Center's involvement is our formation of the International Fraud Symposium, a non-profit organization comprised largely of law enforcement agencies designed to exchange information on organized fraud activities in the Pennsylvania, New Jersey, Maryland and Delaware region. We are also involved in the Internet Fraud Council, a public-private partnership formed to fight fraud on the Internet. I personally sit on the Board of Directors of the National White Collar Crime Center and the Economic Crime Investigation Institute. I, and other members of National Fraud Center, have provided countless hours and resources in assisting law enforcement in the fight against fraud. I truly believe that there are very few, if any, other private, for profit, entities that are as dedicated as we are to the understanding, preventing and investigating of fraud in the various forms that it may take.

Notwithstanding our dedication to fighting fraud, we appreciate the need to protect the privacy interests of law-abiding citizens. For this reason, we became one of the founding members of the Individual Reference Service Group (the "IRSG") and we are active in that organization's activities, designed to root out misuses of personal identifying information databases. We participated in the IRSG's comment to the proposed rules and we of course join in the position expressed in that comment.

We are writing because we fear that the agencies promulgating these rules may not be aware that by expanding the definitions contained in the GLB Act, beyond what we believe is the clear wording and intent of the Act, they are unwittingly stifling the efforts of both law enforcement and industry to fight fraud. Undoubtedly, any restriction on the data flow to databases containing names, addresses, telephone numbers, etc. will seriously retard fraud prevention.

We believe that the proposed definitions pertaining to the phrase "Non-Public Personal Information" go well beyond the definitions contained in the Act itself. The Act defines this phrase at § 509(4) as follows:

(4). Non-Public Personal Information

(A). The term "non-public personal information" means personally identifiable financial information --

(i). Provided by a consumer to a financial institution;

(ii). Resulting from any transaction with the consumer or any service performed for the consumer; or

(iii). Otherwise obtained by the financial institution.

(B). Such term does not include publicly available information, as such term is defined by the regulations described under § 504.

In the proposed rules, the promulgating agencies fail to properly account for the word "financial" in their definition of "personally identifiable financial information." (FTC Proposed Rule, § 313.3(o) and Joint Proposed Rule § ___3 (o)). Without properly accounting for the word "financial", the proposed rules appear to include within the privacy restrictive provisions of the Act, personally identifiable information such as names, addresses, telephone numbers, etc. This is not what the GLB Act states, and it is not what it intends to cover.

Moreover, if restrictions on dissemination of personally identifiable information were to be applied, it would conflict with the Act's clear fraud prevention exceptions. The GLB Act exempts from its application information that is used for such a purpose in at least two places; namely, § 502(e) and § 509(7)(C). Therefore, care must be taken that the public policy of fighting fraud, as clearly expressed by Congress, should not be unduly sacrificed in attempting to protect privacy.

It is essential to recognize the fraud detection and prevention roles that are served by personal identifying information. Many of these roles can be found in the December, 1997 Federal Trade Commission Report to Congress, "Individual Reference Services." These roles can be divided into two basic categories: fraud prevention and fraud investigation. Examples of purposes fitting into the fraud investigation category are: (1) identifying and locating suspects, witnesses and victims; and (2) enforcement of court orders, judgments and sentences, such as in locating assets of fraudulent perpetrators. These activities are often performed by government and law enforcement entities, such as the Federal Trade Commission, the Federal Bureau of Investigation, the United States Secret Service, the United States Department of Justice, the Internal Revenue Service, Health Care Financing Administration (HCFA) and various other federal, state and local agencies in the fight against fraud. Private industry also uses the databases for essentially the same purposes. Insurance companies, banks, credit card companies, etc. expend significant sums investigating suspicious and fraudulent transactions, particularly when law enforcement is either unwilling or unable to do so.

However, it is the other fraud-fighting role that is served by individual reference service products, i.e. fraud prevention, where private industry shoulders the burden virtually alone. Fraud prevention uses of personal identifying databases are in the validation and verification of individuals who apply for credit, insurance benefits, cell phones, etc. In this way, private industry serves as the first line of defense in the protection against identity theft.

Identity theft is a form of fraud that is now striking businesses at an increasing rate. With the dawning of electronic commerce, we can only expect this problem to exacerbate. National Fraud Center has prepared a report on identity theft, entitled "Identity Theft: Authentication as a Solution." This report can be found at our webpage, www.nationalfraud.com. As explained in the report, verification of the identities of consumer applicants, through the use of personal identifying databases, i.e. authentication, is an indispensable part of the identity theft solution. For, although biometrics and Public Key Infrastructure solutions might be available, any of these processes must still implement an authentication component to provide an adequate defense against identity theft.

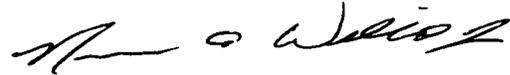
We hope that this comment is helpful in providing the proper framework for applying the GLB Act. We look forward to answering any questions that you may have.

March 31, 2000

Page 4

Thank you for your consideration.

Sincerely,

A handwritten signature in black ink, appearing to read "Norman A. Willox, Jr.", written in a cursive style.

Norman A. Willox, Jr.
Chief Executive Officer