(17)

Deborah Pierce, Staff Attorney
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110

December 4, 2000

Jennifer J. Johnson
Secretary, Board of Governors of the Federal Reserve System
20th Street and C Streets, NW
Washington, DC 20551

Sent Via Electronic Mail

Re: **Proposed Fair Credit Reporting Regulations rule – opt out**

Regulation V; Docket No. R-1082

Dear Ms. Johnson:

I am writing today on behalf of the Electronic Frontier Foundation (EFF), a nonprofit, public interest organization working to protect rights and promote responsibility in the electronic world. EFF is the leading global organization linking technical architectures and legal frameworks to support the rights of individuals in an open society.

As a civil liberties organization concerned with the accelerating erosion of consumer privacy, particularly in regard to financial privacy, EFF has serious concerns about the joint proposal put forth by Federal Reserve Board, the FDIC, the OCC and OTS that allows financial institutions to share personal consumer information with affiliated institutions without incurring the obligations of consumer reporting agencies. Privacy concerns that customers might have with regard to their information and how it is used are barely given any consideration at all in this proposed rule. Instead, the focus is on how to make sharing personal information easier for the affiliated institutions.

EFF is concerned that this rule change will further damage customer financial privacy for several key reasons. First, opt-out provisions provide consumers with the most minimal amount of privacy protection and so must be worded carefully to provide consumers with the maximum amount of privacy protection. Existing threats to consumer privacy such as the fact that more information is likely to be gathered about a customer by affiliated institutions than is necessary for a particular transaction will be exacerbated by opt-out rather than opt-in. In addition, it is likely that extensive consumer profiles will be created without the knowledge or consent of the consumer. Finally, it is highly likely that this information will find its way into other databases

controlled by the government, thus further expanding the amount of information kept in other governmental databases about individuals.

Opt-in would have been the best choice for consent for consumers because it requires data-collectors to get affirmative consent before information about the consumer is shared with others. EFF supports opt-in requirements particularly when the information is as sensitive as financial or medical records. The **Gramm-Leach-Bliley Act (GLBA) only requires opt-out and is a major advantage to financial institutions and their affiliates; the burden to prevent sharing now falls on the consumer. Because of this imbalance of power, the opt-out mechanism must be as consumer friendly as possible.** In these comments I will therefore focus on the dangers from the potential privacy invasions that consumers face from the lack of an opt-in requirement and advocate for the strongest opt-out notice possible.

A. Dangers to Consumers from Potential Privacy Invasions

Inappropriate Data Gathering/Profiling

The inability of consumers to prevent extensive profiles from being created about them is a primary concern to consumers who wish to protect their privacy. The (GLBA) allows affiliated institutions to share personal consumer information among themselves with no ability for consumers to restrict the sharing of that information, except for an opt-out provision that places the onus on the individual. Thus, if a consumer doesn't recognize the opt-out form, or realize what opt-out is, and then take affirmative action, their information may shared and merged into a single database that the affiliated institutions can access. Since each of these institutions (financial, securities, and insurance) each amass a treasure trove of personal information, including wealth, spending habits, and health matters from transactional data, the ability of these institutions to create extensive profiles is enormous. The sharing of these profiles with affiliates has the potential to cause great harm to consumers in the form of denial of insurance, credit, and other forms of discrimination.

Merger of Consumer Information into Other Governmental Databases

Collected information is likely to find its way into other databases controlled by governmental agencies, again taking control of personal information from the individual and giving it to the government. This compulsion for tracking the activities of every individual is a threat to our open society. Data sharing between financial, insurance and securities institutions has the potential to make more products available to consumers and thus be a boon to business, but this boon should not come at the expense of consumer privacy. Last year the public outcry against the proposed mandatory "Know Your Customer" rule was so great that the proposed rules were withdrawn. An attempt by the government to turn the driver's license into a national identification card was also thwarted by a huge public outcry (the law authorizing the national identification card was repealed). Weak provisions such as opt-out versus the stronger opt-in fly in the face of the public's desire to protect their privacy.

Banks now collect a vast amount of personal information on their account holders through voluntary "Know Your Customer" programs. If an account holder also applies for life or health insurance or securities products through their bank, banks could then add that information to a customer's "normal and expected" transactions. That information, whether supplied by the customer, or through sharing with affiliated partner institutions, could then be added to the customers' profile. There is nothing in the proposed rule or the current rule that would prohibit

this practice. This information can then be shared with other governmental agencies, as well as with the FinCen database, likely for IRS or law enforcement purposes.

B. Inherently Weak Opt-Out Provisions Must be as Consumer Privacy Friendly as Possible

Keeping the concerns noted above in mind, the agencies have asked for comment on the following questions:

1. Should financial institutions disclose in their FCRA notices how long a consumer has to respond to the opt out notice before the financial institution may begin sharing the consumer's information to its affiliates? Should the financial institution allow consumers to opt out at any time?

Yes, and yes. Consumers must be given a reasonable opportunity to opt-out. Disclosure of an institution's data dissemination plans is therefore a vital first step for consumers. Notice of the time period that a consumer has in order to take advantage of an opt-out provision also falls under the first prong of fair information principles. The Federal Trade Commission has stated that notice and consent are fundamental principles that are needed in order to protect consumer privacy. We believe that institutions must disclose the time frames for opting-out for consumers.

2. Do the benefits of the additional disclosures outweigh the burdens, and if so, should the regulation require the disclosures to state that the financial institution will wait 30 days in every instance before sharing consumer information with affiliates?

Yes, and yes. The threats to consumer privacy are so great that consumers must be given the opportunity, and the maximum amount of time, in which to opt-out. The time to opt-out should be at least 30 days. Even if it is more burdensome for the institutions to administer, the longest amount of time should be given to consumers in order to let them opt-out.

3. Should opt out notices be sent out separately?

Before answering this question, a short digression on the language of the opt-out form is in order. EFF agrees that the language of the opt-out form must be clear and conspicuous. Language can be placed prominently on a page, in large type, but the language itself must convey the possible threats to consumer privacy. Recently the Network Advertising Initiative (NAI) proposed self-regulatory guidelines that would require "clear and conspicuous" notice to be placed on web sites that would alert consumers to that particular data collector's privacy practices. The NAI proposals have to do with the sharing of clickstream and other data gleaned from a web surfer's web browsing habits. Financial information that is unique to a particular individual, particularly financial information that is being shared with affiliates, is much more sensitive than clickstream data collected at a web site. This is true since with clickstream data, many people in a household can share the same computer (profiling is of limited use in this case). But, the language recommended by the NAI is itself so bland and phrased in euphemisms that it is difficult for the reader to realize that data-sharing of their personal information across web sites might not be in their best interests.

Given the sensitivity of financial data with regard to the GLBA, care must be taken with the language of the opt-out notice to ensure that a consumer is alerted to the fact that financial information will be shared with other affiliated institutions unless that consumer opts-out. Stronger guidelines, in addition to requiring that the notice be "clear and conspicuous" are thus needed. There should be required language in the opt-out form that alerts a consumer to the

privacy risks if the consumer doesn't opt-out. Unless a consumer is savvy enough with regard to privacy issues, the language proposed by the NAI would not alert a consumer that they might wish to opt-out of the web site's data collection practices. The same could be true with notices devised by financial institutions and their affiliates.

To answer the question about separate notices for the opt-out form, the answer must be "yes." In order for a consumer to be able to have a meaningful opportunity to opt-out, a consumer needs to be able to see and recognize the opt-out form to begin with. The opt-out form itself should therefore be made obvious to the consumer. The best way to achieve this would be to send the opt-out form separately from other forms. Most consumers do not always read the inserts to their bills, particularly if there are many inserts and they are written in small type. Mailing the opt-out form separately would therefore segregate the notice from other notices that the consumer receives in the mail or electronically and be more likely to be read and acted upon by the consumer.

Conclusion

As with the "Know Your Customer" regulations that were proposed last year, along with other proposals and laws that are invasive of privacy, such as driver's licenses as national identification cards, individuals have consistently voiced their desires that their privacy be protected. Congress and the current Administration have also shown that they believe privacy is given short shrift in this country today. The weak opt-out provisions in the agencies joint proposal flies in the face of this almost universal concern.

EFF would welcome the opportunity to work with you to help craft a rule that would not further dismantle the already precarious privacy rights that individuals have with regard to their financial information.

Thank you again for giving us the opportunity to comment on this proposed rule. Please contact me at 415-436-9333, ext. 106 if I can be of any further assistance.

Sincerely,

Deborah Pierce
Staff Attorney