

March 17, 2000

**TO: NEC PRINCIPALS**

**FROM: FINANCIAL PRIVACY WORKING GROUP**

**RE: PROPOSED FINANCIAL PRIVACY LEGISLATION**

## **I. SUMMARY**

Last year's financial services legislation (the "Gramm-Leach-Bliley Act" or "GLBA") includes important provisions to protect the privacy of sensitive consumer financial information. For the first time, consumers will receive notice about companies' policies for sharing information with affiliates and third parties, and have the right to "opt-out" of having their information shared with third parties (but not affiliates) for marketing and other purposes. However, the President promised at the GLBA signing ceremony, and again in the State of the Union, to propose legislation to provide individual choice before personal financial information can be shared with affiliated firms.<sup>1</sup>

The working group has developed a proposed legislative package on financial privacy. In addition to providing consumers with the right to opt-out of having their personal financial information shared with affiliated firms, the package would:

- Grant customers access to financial information that institutions collect about them and the right to have that information corrected, if it is inaccurate or incomplete;
- Restrict the use of medical information obtained from a financial institution's affiliate;
- Eliminate an exception in GLBA that allows banks to engage in joint marketing agreements for financial products without providing customer choice; and
- Make other minor improvements to GLBA, drawing on lessons learned through the rulemaking process.

Finally, in transmitting the package, the Administration would indicate that the Treasury Department will complete a GLBA-mandated study of financial privacy before the end of

---

<sup>1</sup> "Without restraining the economic potential of new business arrangements, I want to make sure every family has meaningful choices about how their personal information will be shared within corporate conglomerates. We can't allow new opportunities to erode old and fundamental rights." President Clinton, GLBA Signing Ceremony, November 12, 1999.

the year. In that study, Treasury will consider whether additional protections are necessary to address emerging technologies and information practices. (This leaves us a opening to propose further protections if we end up supporting either legislation or self-regulatory efforts imposing higher standards for on-line companies and want to ensure equivalent protections for financial information.)

The appendix provides a short summary of the views of various interested parties.

## II. SUMMARY OF LEGISLATIVE PACKAGE

### A. Offer Consumers Choice Regarding Information Sharing Among Affiliates.

Under current law, there are two major sets of restrictions on information sharing by financial institutions: the Fair Credit Reporting Act (FCRA) and the recently enacted provisions of GLBA.

The FCRA categorizes information into two types: (1) **application information**, which is information that a consumer provides on an application for credit or employment; and (2) **transaction and experience information**, which includes account balances, deposit and withdrawal amounts, the identity of payees and sources of deposits, information on what payments are made for, and summaries of any of the foregoing).

FCRA requires notice and opt-out before **application information** can be shared with affiliates. If application information is shared with a third party, the entity sharing the information becomes a credit bureau subject to a series of regulatory requirements.

Under GLBA, financial institutions' customers must be given the ability to opt-out before their **transaction and experience information** can be shared with third parties, subject to a long list of exceptions.<sup>2</sup> However, only notice must be given before such information can be shared with affiliated companies; consumers have no "choice" other than to take their business elsewhere.

Current law coverage is summarized in the chart below. In signing GLBA, the President pledged to revisit the chart's shaded box, implying that we might want to require notice and opt-out (as we had proposed the previous May) in this context as well.

---

<sup>2</sup> Exceptions include sharing: under "joint marketing" agreements; necessary to effect a transaction, for fraud prevention and risk management; to resolve consumer inquiries; with rating agencies, accountants, and auditors; with law enforcement; in connection with mergers and acquisitions, and to comply with other laws or court orders.

	Transaction and Experience Information (Covered by GLBA)	Application Information (Covered by FCRA)
Shared with an Affiliate	Notice and Opt-out	Notice and Opt-out
Shared with a Third Party	Notice and Opt-out (with exceptions)	Institution sharing becomes a credit bureau subject to various requirements

Our new proposal would extend the opt-out choice available for third party sharing to the sharing of transaction and experience information among affiliated firms. As a rule, affiliated companies would not be able to share without offering an opt-out. However, the proposal would contain the same exceptions applicable to third party information sharing under GLBA (but not the joint marketing exception, as discussed below). Sharing with affiliates for law enforcement, data processing, and similar purposes would be exempt from the opt-out.

In addition, we propose to clarify a existing exception to ensure that sharing of information for risk management and customer service purposes are permitted without opt-out, as long as notice is provided. This would allow a credit card company, evaluating a credit limit increase, to consider that the customer has just defaulted on a small business loan to the company's bank affiliate. It also would allow an institution to produce and send consolidated account statements, covering insurance, securities, and other accounts in a single document.

We considered other options including: (1) requiring opt-out before sharing with affiliates only for certain activities (marketing and profiling) or only for the most sensitive information; (2) requiring opt-in before sharing with third parties, but not affiliates; or (3) requiring opt-in before sharing with third parties and affiliates. As a policy matter, the working group does not see a compelling need for opt-in before most information can be shared within financial holding companies. Many uses of such information can provide customer benefits, but inertia will lead only a fraction of customers to affirmatively opt-in. Some of us believe that sharing some types of information, or sharing for certain uses, might justify stronger protections like opt-in. However, given the largely rhetorical nature of this debate this year, we did not think it worth offering a complex proposal with various degrees of protection (both more and less protective) for different categories of information or uses. However, we do propose to indicate that Treasury will continue to study emerging technologies, leaving us an opening to argue for greater protections at a later time.

**B. Improve Consumers' Ability to Access and Correct Financial Information.**

Consumer groups and the EU have pushed us to grant consumers an unequivocal right of access to their financial information. In practice, consumers already have substantial access rights – financial firms are legally required to provide monthly account statements

and make corrections where appropriate, and financial firms routinely honor requests for copies of historical records.

We propose to strengthen federal access rules by explicitly providing consumers the right to access personal financial information that institutions collect about them, and to have that information corrected if it is inaccurate or incomplete. The customer would have to cover the reasonable cost of the search, and there would be an exception for proprietary information such as credit scoring models.

**C. Prevent Unauthorized Use of Medical Information Obtained from an Financial Institution's Affiliate.**

In May 1999, the President called for limitations on sharing medical records within financial holding companies. We sought to ensure that a financial institution would not make credit decisions based on medical information about the customer obtained from an affiliate without the customer's permission. In response, House Republicans attached a deeply flawed medical privacy amendment to the Financial Modernization bill. It actually would have *reduced* the protections provided by current law and HHS regulations on medical privacy. We were concerned that this would give the Congress a chance to say they had addressed medical privacy without tackling the more comprehensive medical privacy legislation that we supported. In the House, we sought and won an instruction to conferees that the medical provision be stripped; and it was removed in conference.

Some Banking Committee Democrats and Republicans criticized us for stripping the provision. They argued correctly that HHS regulations cover only certain insurance providers, and would not protect medical information held by life, auto, some disability, and property & casualty insurers affiliated with banks.

This year, we wanted to close this gap with a limited provision that would not reopen debate on medical privacy more broadly. We propose to say that a financial institution or subsidiary may not receive, obtain, or consider medical information from an affiliate, unless it requires the submission of and considers the same specific medical information about *every* applicant for a financial product or service. In addition, in order to receive even this limited range of information, the institution would have to obtain the customer's opt-in consent before any sharing could occur. Finally, the proposal will clearly state that nothing in this law or in the GLBA supercedes the provisions of the Health Insurance Portability and Accountability Act or regulations promulgated under it.

This provision will likely be popular, as consumers particularly fear misuse of this type of data, and it is easy to explain the risks. It also would close a genuine loophole in existing law. And it would please Democrats like Reps. LaFalce and Vento, who acceded reluctantly to Administration wishes that medical privacy be dropped from GLBA. HHS and some Democrats, while generally supportive of the proposal, have lingering concerns about our ability to limit the way Congress addresses the issue and fear that the standards that apply generally to medical data might be lowered. They are

also concerned that “fixing” life insurance or other records in the financial bill would reduce the chances of including those entities in future medical privacy legislation.

**D. Remove Joint Marketing Exemption.**

The third-party opt-out provisions of GLBA provide an exemption for financial institutions that join forces in “joint agreements” for purposes of marketing financial products and other services through third party marketers. This exception was intended to level the playing field, allowing small financial institutions (without affiliates) to take advantage of information-sharing opportunities that larger financial conglomerates could do, without opt-out, by sharing amongst their affiliates. However, in fact, it is badly written and broad enough to allow large and small institutions to avoid GLBA’s protections in many cases.

Since we propose to require an opt-out before inter-affiliate sharing – leveling the playing field between larger and smaller institutions – there is little justification for retention of the joint marketing exemption. When Congress takes up this issue, however, we may be pressed to consider some alternative relief for small banks.

**E. State Preemption.**

GLBA includes a Sarbanes amendment providing that nothing in that law shall preempt state privacy laws that go further. However, the FCRA contains an explicit preemption of state regulation of information sharing within a “corporate family” – i.e., affiliate sharing – until 2004. This does not prevent states from providing access or limiting third-party marketing. Even for affiliate sharing, states can still enact restrictions provided they do not take affect until 2004.

As a result, the financial services industry’s greatest anxieties about privacy restrictions currently focus on the States. They are concerned not only about *strict* regulation, but also *inconsistent* regulation – the possibility that a nationally active bank would have to process data under 50 different state regimes. If additional federal privacy protections are ever adopted, industry will demand state preemption. Many Hill Democrats and consumer groups recognize that this deal probably would be part of additional federal privacy legislation, but none believe we should concede the point now.

Our proposal would be silent on preemption, thus leaving the Sarbanes amendment’s general preemption, and the FCRA exceptions, in place. This is consistent with our general policy that we want to leave in place the ability of states to provide greater protections, but would not preclude us from accepting an agreement at a later time that included some form of federal preemption. We considered whether to close the FCRA exception loophole, but no privacy advocates were urging us to do so and doing so might open the debate on broader preemption prematurely.

**F. Prevent Abuses of Bankruptcy Trustees Financial Information Databases.**

Bankruptcy trustees collect and hold a great deal of sensitive financial information regarding those with whom they have trustee relationship. Much of this information is required to be made public by law, in court records and elsewhere, to assist interested parties in pursuit of legitimate claims against debtors in bankruptcy proceedings. Other information, such as payment schedules for debtors to creditors in a bankruptcy workout, is not part of the public record.

Private bankruptcy trustees are considering proposals to aggregate and sell this information to third parties ostensibly to facilitate creditor monitoring of repayment under Chapter 13 plans. While the trustees appear to want to be responsible, the commercial distribution of large databases of non-public information to those without a direct interest in a particular bankruptcy claim raise privacy and other policy issues. Other bankruptcy records contain detailed financial information. Making even these public records available over the Internet has significant privacy and security implications. Appropriate protections should be put in place before any such information is available electronically. We are proposing a study to be conducted by the Executive Office of the U.S. Trustees (DoJ), OMB, and Treasury.

**G. Make Financial Institutions Responsible for Misrepresentations of Their Privacy Policies.**

The initiative will clarify that an institution will be considered in violation of the law and subject to sanctions if it fails to honor *any* aspect of its stated privacy policy as disclosed to consumers under GLBA, whether or not that particular aspect of the privacy policy is required by GLBA or any other federal law. Under current law, banks are not covered by the Federal Trade Commission Act's general prohibition on unfair and deceptive trade practices.

We also are still considering whether additional enforcement mechanisms should be included in our proposal. Options include heightened oversight by regulatory authorities, enforcement authority for State Attorneys General, and a private right of action. The last would be highly controversial, but we have insisted on it to protect medical privacy.

**H. Ensure That Consumers Can Use Privacy Policy Notices for Comparison Shopping.**

Our proposal would clarify that privacy notices must be provided to individuals upon request, and as part of any application for a financial service, to enable consumers to make informed decisions based on comparisons of those policies before the time a customer relationship has been established. The GLBA is unclear as to the timing of initial notices, and does not mandate that they be included with application materials.

**I. Clarify the Definition of Non-Public Personal Information.**

Our proposal would clarify that *all* information collected by an institution in connection with the provision of a financial product or service, including Social Security numbers, is to be covered by notice and opt-out requirements for *both* affiliate and third-party information sharing.

**J. Ensure That Secondary Market Institutions Cannot Transfer Sensitive Data.**

Our proposal would repeal the blanket exception in GLBA for Fannie Mae and Freddie Mac, while retaining specific exceptions to allow sharing as part of secondary market activities, e.g., securitizations. Thus, Fannie and Freddie would not be permitted to construct profiles of homeowners and sell that information to third parties such as home equity lenders.

**K. Provide Better Enforcement for Pretext Calling.**

GLBA prohibits the practice of "pretext calling," -- obtaining of information about individuals through the use of false statements and other deceptive tactics. It also authorizes criminal penalties for offenders, but grants enforcement authority only to the FTC. Our proposal would extend enforcement authority to State Attorneys General.

**L. Close Loophole in Re-Use Provision.**

The re-use provision in GLBA is supposed to hold a recipient company to the same standards as the company that transfers the data. A drafting error appears, however, to allow a loophole if a company first transfers the data to an affiliate. The data might then be transferable without the re-use restrictions. We would close the loophole.

**APPENDIX A**  
**VIEWS OF INTERESTED PARTIES ON FINANCIAL PRIVACY**  
**LEGISLATION**

**Rep. Markey/Senator Shelby.** Markey and Shelby formed an unlikely left-right alliance over privacy issues in the S. 900 conference, and are still working together on the issue. Last year they introduced the "Consumers' Right to Financial Privacy Act," which provides notice and *opt-in* for all information sharing, requires institutions to give consumers access to all information about them, and prohibits institutions from denying services to customers that opt out of information sharing.

Upon passage of last year's bill, Markey said, "*The White House really pulled the rug out from under consumers by agreeing to weak privacy protections in the banking bill.*" Shelby's comments were similarly negative, and there are no indications that either will back away from their public stands. Indeed, the two recently founded a bipartisan, bicameral "Congressional Privacy Caucus" to push their legislation. Shelby has a few Republican allies in this effort, including Rep. Joe Barton (TX).

**Other Democrats.** Minority Leader Daschle announced the formation of another privacy group, the Senate Democratic Privacy Task Force, February 9. The group is chaired by Sen. Leahy, and is designed to be more of an educational effort than a legislative task force. Leading pro-privacy Democrats in the Senate include Bryan, Sarbanes, and Leahy. Bryan is the most vocal of these, and is the sole co-sponsor of the Shelby bill. Sarbanes has introduced privacy legislation before, but has been hesitant about pressing the issue – his interest is significantly staff-driven. House pro-privacy Democrats include Dingell, Waxman, and Hinchey.

**Senator Gramm.** Gramm strongly opposes Congressional efforts to legislate privacy policy. He opposed the provisions in S. 900, and in a February 3 interview said, "*This is an issue that is being driven by polls and politics. I am not going to let the Information Age be killed off before it is ever born.*" Gramm has the support of all of his Committee Republicans except Shelby on the issue.

**Industry.** Financial services firms have generally opposed legislative privacy protections, and fought to dilute the provisions contained in the GLBA. They can be expected to oppose any new privacy bill. However, two factors may make them more amenable to legislation than they have been in the past.

- Thirty or more states may consider financial privacy legislation this year. The prospect of having to comply with 50 different state requirements is far more daunting to most firms than a federal rule, and many may be willing to trade tougher federal protections for preemption of state laws.
- Some major firms are already providing at least notice and opt-out for affiliate marketing already (Citigroup under an agreement with the Federal Reserve, Chase Manhattan under a settlement with the New York Attorney General, Washington

Mutual and other Washington State thrifts voluntarily). They may thus be able to accept a federal rule that codifies practices similar to those they already have in place.

**Consumer/Privacy Advocacy Groups.** Advocates generally favor much stronger privacy protections, and complained loudly that the GLBA provisions did not go far enough. The Treasury and the White House were accused by some of settling for too little. Their strongest criticisms focused on the omission of affiliate restrictions, the exception for joint marketing agreements, and the failure to grant consumers a right of access.