April 21, 2000

MEMORANDUM

TO: NEC PRINCIPALS

FROM: FINANCIAL PRIVACY WORKING GROUP

RE: FOLLOW-UP ON FINANCIAL PRIVACY PROPOSALS

SUMMARY

During the NEC Principals meeting on April 3, 2000, you discussed the possibility of adding to our proposal another requirement: a financial institution must get affirmative consent (opt-in) before sharing any payee information with an affiliate or third party.[1] Before deciding whether to include this element, you asked the working group to explore several questions, which are discussed in detail below. We also advise you below (see issue 5) of a change we have made to our earlier recommendation on privacy in bankruptcy. We are also preparing a brief assessment of the Congressional outlook on opt-in proposals which will be sent separately.

1. What are the options for an opt-in requirement for especially sensitive financial information, and what information would be covered?

The working group wants to highlight three options in this area. **Option one** would be to exclude any opt-in requirement from the proposal. **Option two** would require an opt-in before a firm could share specific information about: (a) to whom the customer has made a payment by check, credit card, debit card, or other payment mechanism ("payee information"); (b) from whom the customer has received a payment or transfer of funds ("payor information"); and (c) for what purpose any of these payments were made. **Option three** would also cover the profiles derived from this specific transaction information under the same opt-in. These options are discussed in greater detail below.

Option 1: No Opt-In Requirement: Under this option, the core substantive proposal in our financial privacy legislation would be to provide opt-out choice for both affiliates and third-party information sharing. There would be no special protection for payor/payee information or for profiles derived from such information. This would match what the President has said would be included in the Administration's proposal, i.e., choice for affiliate-sharing, but would go no

[1] Interestingly, Senator Shelby introduced a new bill last week that would do effectively the same thing. Entitled the "Freedom from Behavioral Profiling Act of 2000," it would require an opt-in before any financial institution could share payee or payor information with an affiliate or a third party.

further.

Option 2: Payor/Payee Information: This option would provide consumers with opt-in choice before their transaction-level information could be shared by a financial institution. During the last Principals' discussion, the conversation focused on payee information. However, the working group believes that equally sensitive information could be contained in payor information (sources of income or deposits into your accounts). Imagine, for example, a consultant or an independent contractor whose bank account provides a complete record of her clients. We could articulate no justification for distinguishing between payee and payor information. If the decision is made to proceed with either option 2 or option 3 (the opt-in-based options), we believe that it should cover payor as well as payee information.

This option is consistent with the substance of the recent proposal of Senator Shelby, a leading proponent of financial privacy legislation. If the Administration's opt-in proposal covers only the payor/payee information, we should be careful not to oversell it as a limit on behavioral profiling. It is interesting to note that Senator Shelby billed his recent legislation as the "Freedom from Behavioral Profiling Act of 2000." He said, in introducing his legislation: "[F]inancial institutions would only be allowed to buy, sell, or otherwise share an individual's behavioral profile, if the institution had disclosed to the consumer that such information may be shared and the institution has received the consumer's affirmative consent to do so." Yet, as we read the bill, it would not require opt-in before profiles inferred from the information were shared or sold - only before specific transaction information itself is shared or sold.

Option 3: Payor/Payee Information and Profiles: A more difficult decision is posed by whether to require opt-in before sharing only specific transactional information or also to require opt-in before sharing the results of analytical models (i.e., profiles) derived from that transactional information. (See the Appendix for the modification to the legislative language that would accomplish this broader purpose.)

If the restrictions apply only to payor/payee information, we would prohibit a credit card company from sharing, for example, without your affirmative consent, the fact that you contributed to far-right wing political groups, purchased a book on gay marriage, or paid your ex-spouse only $100 a month in child support. However, they would be able to share, absent opt-out, profiles that describe you as right-wing extremist sympathizer, gay, or divorced. These examples are intentionally sensitive; many firms would be reticent to profile in these areas. Many people probably would have less objection to the profiling if firms were simply describing an individual as a Redskins fan, avid tennis player, frequent traveler, or aficionado of fine wines and cigars. However, it may be impossible legislate a workable distinction between "benign" and "non-benign" profiling categories. Note that under this option, we also include an anti-circumvention provision designed to preclude financial institutions from disclosing transaction-level information in the guise of a profile.

If the restriction also requires opt-in before sharing profiles, that would be a far bigger step than restraining the sharing of payor/payee information, as it would constrain existing industry practice. Credit card companies, for example, create profiles of individuals' purchasing behavior and use that information in target marketing (everything from bill inserts to phone solicitations). They share the profiles with affiliates and sometimes sell the profiles to third parties. A few

years ago, there was a firestorm when the press reported that American Express was considering selling the specific payor/payee information. The focus of the criticism was on sharing of "the raw data." American Express quickly retreated, and asserts they have no plans to share the more specific information. There has not been similar criticism of their continued practice of developing, using, and selling profiles based on consumer purchasing behavior.

If the Administration requires an opt-in for sharing payor/payee information without covering the profiles, some might argue that it would not adequately protect individuals against transfers of this sensitive information. Under the proposal, payment service providers would not be able to sell the fact that an individual made seventeen trips to Europe last year and stayed at particular hotels. They would, however, be able to "profile" that individual as a "frequent high-end European traveler," and sell that profile to others for marketing purposes.

2. Would the Administration be treating financial institutions differently than other firms, especially other on-line firms? Could we defend our policy as consistent?

Generally speaking, financial institutions and businesses whose activities are "financial in nature" are covered by the privacy restrictions in current law and under our new proposal. Thus, for the most part, comparable financial activities will be regulated similarly. However, there are some circumstances in which similar information could be collected by non-financial firms not covered by this statutory regime (as we would amend it). We also discuss below issues of consistency between the Administration's approach to privacy in the on-line world and the financial privacy proposal.

Covered Activities: The Gramm-Leach-Bliley Act (GLBA) and our new proposal cover all institutions engaged in financial activities, which are defined clearly in statute and regulation. Traditional financial institutions (banks, thrifts, securities firms, investment companies, insurance companies, and credit unions) engaging in activities "financial in nature"[2] are subject to enforcement by their respective financial regulator. In addition, other firms engaging in

---

[2] Activities that are "financial in nature" are defined as:

1. Activities specifically named in the statute, including lending and other banking activities; insurance underwriting, annuity, and agency activities; securities underwriting and dealing; merchant banking; and financial or economic advice or services.
2. Any activity that the Federal Reserve Board had determined to be "closely related to banking or a proper incident thereto" prior to the enactment of the GLBA. These activities include financial data processing, acting as a certification authority for digital signatures, and check cashing and wire transmission services.
3. Any activity that a bank holding company may engage in outside of the U.S., as authorized by the Federal Reserve, such as management consulting services; operating a travel agency; or organizing, sponsoring, and managing a mutual fund.

The Act also sets up a process under which the Federal Reserve and the Treasury may jointly determine that additional activities are "financial in nature" or "incidental to [a] financial activity" in order to accommodate future developments in financial products.

activities "financial in nature" are also subject to the privacy provisions.[3] Companies that engage in activities financial in nature, but are not traditional financial institutions, fall under the jurisdiction of the FTC.

The FTC's proposed rule states that it will view an entity engaged in an activity financial in nature as a financial institution only if it is "significantly" engaged in that activity. The FTC uses the following example: a retailer that directly issues its own credit cards to consumers will be considered a financial institution; one that merely establishes a deferred payment or layaway plan will not. The agency has sought comment on whether the term "significantly" should be more precisely defined. The FTC staff have indicated their intent to give consumers of like products like privacy protections. That is, the purchaser of a service that falls under the definition of "financial" should be protected to the same degree whether that service is obtained from a regulated bank or a non-traditional provider.

To help analyze the issue, we considered the case of AOL. AOL says that it does not collect information about the purchases that its customers make from merchants al the AOL site. They perceive that it would be seen as an invasion of privacy to keep track of their customers' purchases when using the service (of course they do keep track of their customers' browsing habits). They collect purchase information only for, products purchased from AOL itself, such as shirts bearing the AOL logo. However, if AOL were to collect that information, it is not clear whether they would be considered a financial institution under GLBA. AOL is now considering creating a "digital wallet" product. Customers could choose to put their credit card, home address, and other information into an AOL-maintained server to help speed transactions with e-merchants. In that case, AOL would expect to provide a log of such purchases to their customers, similar to a monthly credit card statement. These "digital wallets" may become a major payments system for e-commerce, and we believe that such services clearly should and would be "financial in nature" and therefore covered by the financial privacy rules.

Concerns have been raised that the payor/payee approach could create a situation in which credit card companies may have an advantage because they would possess more information than other market participants regarding a customer's transactions. If customers follow usual preferences and a low percentage of them opt-in to sharing of transaction-level financial data, credit card firms could have a competitive advantage in targeting communications to a single individual for marketing purposes.

However, credit card companies will face competition from other institutions that collect substantial amounts of transaction data. Competitors include other payment service providers, companies like Amazon.com that collect detailed information on a variety of online purchases, and internet "portals" that collect extensive browsing information. In addition, since our proposal would bar companies from selling payor/payee information without consent, any competitive advantage to payment service companies must be weighed against the assurances

[3] Exempt from coverage under the privacy title are: companies to the extent they engage in activities subject to the Commodity Futures Trading Commission's jurisdiction; the Farm Credit System institutions and Farmer Mac; and government-sponsored enterprises that engage in securitization or secondary market activities, as long as they do not sell or transfer nonpublic personal information to a nonaffiliated third party.

consumers will have that their payment information will not be distributed to those with whom they did not entrust such information.

Comparison with Non-Financial Privacy Policies: The Administration has generally taken the position that the more sensitive the information, the greater the privacy protection should be. We therefore supported legislation that requires an opt-in before sharing medical information or gathering information from children on-line. Current law also requires opt-in before sharing telephone numbers called, video rentals, release of student records, records of cable television viewing, government records, and release of drivers' records for marketing.

Regarding on-line privacy, while we have not proposed legislation for other on-line activity, we have urged self-regulation that provides for notice and opt-out choice for activity on Internet websites. In addition, the FTC and Commerce are in negotiations with the "Network Advertising Initiative" (NAI) about possible approaches to self-regulation of the practices of on-line profilers, who collect information about web surfers and select advertisements based on the surfers' behavior. They have taken the position that these practices raise special concerns (compared with data gathered at a merchant that the surfer chooses), because the surfers do not select the profiler and do not necessarily know of the profiler's activity. The agencies have made clear that, if the NAI does not agree voluntarily to practices that are sufficiently protective of privacy, they might support legislation.

While these negotiations are on-going, any code that results would likely require: (1) opt-in for any linking of a person's identity with on-line information that was gathered previously when surfers did not know of the profiler and could believe they were acting anonymously; (2) notice and opt-out (likely "robust" opt-out, with the option highly visible to surfers) for linking of surfing information in the future with the surfer's identity. In addition, a recent draft submitted by NAI contained a prohibition on profiling medical and financial information.

There are arguments that the Administration's policy on online privacy and options 2 and 3 of the financial privacy proposal -- each of which involve opt-in choice -- may not be comparable. Concerns have been raised that the opt-in provision in the financial proposal will make it more difficult to sustain our self-regulatory approach, which has generally called for notice and opt-out choice. This concern is stronger still if the opt-in covers profiling (option 3), and not just payor/payee information (option 2). Because the distinction between opt-out and opt-in is so significant, we would need to be able to explain the discrepancy in policy approaches. Another argument of inconsistency is based on the fact that the Administration's online privacy policy has been to support self-regulation, whereas here, we propose financial privacy Legislation.

There are also arguments that our online and financial privacy policies are consistent, as follows: Option 1 presents the strongest argument for comparability. It provides for opt-out choice in both industry sectors. For option 2, one argument is that there are no similar transactions in the online world as the payor/payee transactions that would be covered in the financial privacy proposal. Another argument is that the payor/payee information is most sensitive and merits greater protection, as evidenced by the special protection that American Express and AOL provide voluntarily for such information. For option 3, the argument would be that the Administration adopts a view that financial profiling information is most sensitive -- like

payor/payee information -- and therefore merits the greater, opt-in protection. Finally, for all options, current law and the Administration's proposal would treat a payment account or other "financial in nature" activity the same whether it is conducted on-line or on paper.

3. Would announcing this legislative proposal, or the addition of an opt-in for payee/payor information, harm our prospects for completing negotiations with the EU on the "safe harbor"?

At the first Principals' meeting, the Working Group was asked how the proposal overall, and a possible opt-in for payor/payee information, would affect the safe harbor talks with the European Union (EU). The Working Group has tentatively concluded that, while the privacy package as a whole could have an effect on negotiations with the EU, the addition of an opt-in for payee-payor information or for profiles probably will not change the course of those discussions, whatever they may be, significantly.

The most significant parts of the Administration's proposal from a safe harbor perspective are those dealing with affiliate sharing and access. Administration officials negotiating the safe harbor have envisioned for some time that financial services firms would need to comply with GLBA as well as affiliate sharing and access rules in order to have safe harbor benefits. With the release of this new privacy proposal, we would better align our position regarding the protections required domestically with the protections that we said were required for adequacy under the safe harbor. This is consistent with the position that U.S. officials took in EU negotiations in March. We should understand, however, that the industry will likely object to new requirements on affiliate sharing and access for both domestic legislation and safe harbor purposes.

Regarding the proposals to require opt-in before sharing payor/payee information and profiles, no similar opt-in is required in the EU. Under the EU Data Directive, opt-out is generally required before marketing uses. Opt-in is required for certain sensitive information, such as medical, ethnicity, and union membership data. But financial information is *not* considered sensitive under the Directive. We are not aware of any special privacy rules in the EU that are focused on the sorts of financial payments that may be covered by our opt-in proposal.

4. Would our privacy proposal prevent financial conglomerates from achieving the synergies which the Administration and others argued would flow from breaking down Glass-Steagall barriers between banking, securities, and insurance? Was information sharing a key element of those benefits?

While financial services firms may have sought modernization legislation, at least in part, in order to make it easier to benefit from information sharing within financial conglomerates, this was not their primary argument on its behalf. Nor was it a major focus of Administration arguments, where we emphasized *greater choice* for consumers, farmers, and small businesses. We also said that modernization should result in *lower costs* to consumers as more financial service providers compete for customers, and that it should *improver access* for under-served consumers by encouraging new competitors to find profitable opportunities in previously

overlooked markets.[4] However, in an October 5, 1999 speech Secretary Summers specifically mentioned the importance synergies and information sharing in financial modernization legislation in connection with the need for greater privacy protections. He said:

> "Financial privacy has gained much greater prominence as an issue since the last Congress. Much of the benefit of financial modernization is synergy, and part of that synergy is derived from the sharing of information from developing innovative products to relieving customers of the burden of reintroducing themselves to an institution each time they do business. Nonetheless, revelations about financial service industry practices have come as a shock to policy makers and many consumers, who thought that financial services firms preserve the confidentiality of personal customer information. Our challenge is to protect the privacy of consumers while preserving the benefits of competition and innovation."

Regardless of which option is selected, we believe that our plan strikes the right balance. While an opt-in requirement would provide greater protection for the most sensitive financial information, we would allow financial institutions to relieve their customers of the burden of needing to provide the same information to multiple affiliates. The Administration's proposal would expressly exempt sharing of information with affiliates "in order to facilitate customer service, such as maintenance and operation of consolidated customer call centers or the use of consolidated customer account statements, other than for marketing purposes."

5. **Privacy in Bankruptcy: Revised Recommendation**

We continue to recommend that the President announce that he has directed DOJ, Treasury, and OMB to complete a study of privacy and access issues in bankruptcy data before the end of the year. We also believe we should continue to work to eliminate provisions harmful to privacy in the current House and Senate bankruptcy bills. However, we are withdrawing the recommendation that we announce one substantive new provision now, as part of the broader financial privacy package. There are too many questions that we need the study to resolve before we can feel confident in the policy proposal.

[4] We checked the 1997 Rubin and Hawke testimony before House Banking and House Commerce (and the Exchequer speech and Key Points of the Treasury plan released in May '97), as well as 1998 and 1999 Senate and House testimony, and could find no reference to cross marketing or synergy benefits.

APPENDIX

SECTION 102. LIMITATION ON PAYOR AND PAYEE PROFILING

Section 502(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6802(b)) is amended to read as follows:

"(b) DISCLOSURE OF PAYEE AND PAYOR INFORMATION--

"(1) NOTICE AND OPT IN.—Notwithstanding subsection (a), if a financial institution provides a service to a consumer through which the consumer makes or receives payments or transfers by check, debit card, credit card, or other payment mechanism, the financial institution shall not disclose to an affiliate or a nonaffiliated third party—

(A) the identity of any person or entity to whom a consumer has made, or from whom a consumer has received, a payment or transfer by check, debit card, credit card, or other payment mechanism;

/(B) information about a consumer derived from the information described in paragraph (A);\ or

"(C) the goods or services for which such payment or transfer was made.

"(2) EXCEPTIONS.—

"(A) A financial institution may disclose the information described in paragraph (1) to an affiliate or a nonaffiliated third party if such financial institution —

"(i) has provided to the consumer a notice that complies with section 503; and

(ii) has obtained from the consumer affirmative consent to such

disclosure and such consent has not been withdrawn.

"(B) This subsection shall not prevent a financial institution from disclosing the information described in paragraph (1) to an affiliate or a nonaffiliated third party for the purposes described in subsections (f)(1), (2), (3), (5), (7), (8), (9), or (10)."