UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

September 22, 2000

BY E-MAIL
& HAND-DELIVERY

Leander D. Barnhill, Esq.
U.S. Department of Justice
Executive Office for United States Trustees
Office of the General Counsel
901 E Street, N.W., Suite 780
Washington, D.C. 20530

Comments on Study of Privacy Issues in Bankruptcy Data

Dear Mr. Barnhill:

The staff of the Federal Trade Commission's Bureau of Consumer Protection is pleased to offer comments in response to the request for public comment by the Department of Justice, the Department of Treasury, and the Office of Management and Budget (the Study Agencies).(1) The Study Agencies are conducting a study (the Study) of how the filing for bankruptcy relief affects the privacy of individual consumer information that becomes part of a bankruptcy case.(2)

This comment focuses on the privacy and identity theft issues raised by the collection and use of personal financial and other information in personal bankruptcy cases. As a threshold matter, the Study Agencies may wish to consider to what extent highly sensitive information, such as a consumer's social security number, must be included in public record data in light of the increased risk of identity theft and other illegal conduct. The comment also suggests that the Study Agencies consider prohibiting the commercial use by trustees of debtors' non-public data for purposes other than for which the information was collected (i.e., to administer the bankruptcy case). Finally, the comment suggests evaluating the interplay between consumers' privacy interests and the Bankruptcy Code, focusing for example, on issues where private customer information is protected by a company's privacy statement.

A. Interest and Expertise of the Federal Trade Commission

The Federal Trade Commission (Commission or FTC) is an independent law enforcement agency whose mission is to promote the efficient functioning of the marketplace by protecting consumers from unfair or deceptive acts or practices and to increase consumer choice by promoting vigorous competition. The Commission's primary legislative mandate is to enforce the Federal Trade Commission Act (FTCA), which prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.(3) With the exception of certain industries, the FTCA provides the Commission with broad law enforcement authority over entities engaged in or whose business affects commerce.(4) Pursuant to these responsibilities, the Commission has acquired considerable experience in addressing privacy issues in both the online and offline worlds,(5) and has long had particular interest in, and gained extensive experience dealing with, privacy and consumer protection issues.(6)

Beginning in April 1995, the Commission held a series of public workshops on online privacy and related issues. It also has examined: Web site practices in the collection, use, and transfer of consumers' personal information; self-regulatory efforts and technological developments to enhance consumer privacy; consumer and business education

efforts; the role of government in protecting online information privacy; and special issues raised by the online collection and use of information from and about children.(7) The Commission also has issued a series of reports to Congress regarding privacy online: *Privacy Online: Fair Information Practices in the Electronic Marketplace* (May 2000) (2000 Report); *Self-Regulation and Privacy Online: A Report to Congress* (July 1999); *Privacy Online: A Report to Congress* (June 1998) (1998 Report). In its 2000 Report, a majority of the Commission recommended to Congress that consumer-oriented commercial Web sites that collect personal identifying information from or about consumers online be required to comply with fair information practices.(8)

Concurrent with its online privacy activities, the Commission has implemented the Identity Theft and Assumption Deterrence Act of 1998.(9) That Act directed the FTC to establish the federal government's centralized repository for identity theft complaints and victim assistance. Indeed, the Commission's toll free hotline, which was established so that consumers could report identity theft and obtain counseling to resolve identity theft issues, averaged over 1,000 calls per week during the months of July and August, 2000.

Identity theft occurs when a person's identifying information -- name, social security number, mother's maiden name, or other personal information -- has been used by another to commit fraud or engage in other unlawful activities. Common forms of identity theft include taking over an existing credit card account and making unauthorized charges on it; taking out loans in another person's name; writing fraudulent checks using another person's name and/or account number; and opening a telephone or wireless service account in another person's name. In extreme cases, the identity thief may completely take over his or her victim's identity -- opening a bank account, obtaining multiple credit cards, buying a car, getting a home mortgage and even working, or being arrested under the victim's name.

Although statistics from the Commission's Identity Theft Data Clearinghouse show that about 80 percent of identity theft victims who have filed a complaint with the Commission report finance-related fraud, such as the opening of fraudulent credit, loan, bank, or telecommunications accounts,(10) the Commission also has received hundreds of complaints involving an identity thief obtaining employment, compiling an arrest record, or receiving government benefits in the victim's name. Most of the consumers filing these complaints did not know how their personal information had been compromised. However, the victim's social security number, coupled with date of birth, are key pieces of information for identity thieves. These key pieces of information are of course contained in bankruptcy filings.

B. Privacy and Identity Theft Issues Raised By the Collection and Handling of Sensitive Information in Bankruptcy

The Study Agencies may wish to consider crafting future policies and procedures regarding the collection, use, and dissemination of personal information in light of the highly sensitive nature of the data collected and the new technological ease by which it can be used to facilitate identity theft and other illegal activities. Personal bankruptcy cases may involve the collection of highly sensitive personal information, such as social security numbers, financial information, credit information, income, and details about routine living expenses.

As a threshold matter, the Study Agencies may wish to consider whether certain items of highly sensitive personal information, such as an individual social security number, needs to be included in "public record" data. It may not be necessary for those creditors, and other persons who need notice of the filing and access to relevant information about the debtor, to gain access to such sensitive data through a public record. This concern is heightened by the increasing availability on the Internet of courts' public record data as well as data compiled offline from these same records that is subsequently made available on the Internet. As noted above, a social security number is currently the key piece of identifying information used to commit identity theft. Internet publication of social security numbers through the bankruptcy process is one way for identity thieves to ply their trade in a manner that is completely invisible to their victims and impossible for consumers to avoid or mitigate. For example, the identity thief can use a victim's social security number to open fraudulent credit, loan, bank, or utility accounts in the victim's name. A valid social security number is also essential to the thief's ability to obtain a driver's license or other official identification in a victim's name, and to obtain employment in a victim's name.(11)

Additionally, to the extent the Study Agencies determine that certain personal information should be kept on the public record as part of the bankruptcy case, they may wish to consider the feasibility of restricting, in an appropriately tailored manner, the commercial use of such public record data for certain purposes unrelated to the bankruptcy.

As a related point, the Study Agencies have asked commenters to address "[p]rinciples for the responsible handling of information in bankruptcy records" and describe "[b]usiness or governmental models that can provide access to, and protect debtors' privacy interests in, bankruptcy records."(12) Recognizing that certain information necessarily must be placed on the public record during a bankruptcy case, the Study Agencies should consider ensuring that debtors are given notice as soon as possible in the bankruptcy process as to how their information will be used and whether and how it will be disclosed. Consumers cannot fully consider the implications of pursuing relief from their debts in bankruptcy unless they are informed of the consequences and the extent and means by which their personal and financial information will be divulged to parties in interest and the larger public. The Study Agencies may wish to consider a requirement that potential debtors receive clear and conspicuous notice of this information before any filing is made to begin the bankruptcy process. For example, if the Study Agencies require that putative debtors receive notice of the potential dissemination of bankruptcy information before filing, the burden of disclosure will rest on debtors' counsel in the pre-filing consultation process. In this scenario, counsel would be required to certify that they have notified debtors of the consequences of providing their personal and financial information. Currently, counsel are required to certify that they have discussed with individuals whose debts are primarily consumer debts the types of relief available to them through the various chapters of the Code (see Bankruptcy Official Form 1). A certification of disclosures regarding dissemination of private information could be accomplished in the same manner. Alternatively, such disclosures could be made post-filing at the first meeting of creditors conducted pursuant to Section 341 of the Bankruptcy Code. The disclosures could be made in the informational sheets that the United States Trustees or their designees presently distribute at Section 341 meetings.(13)

C. Future Practices for Collecting, Analyzing and Disseminating Information in Personal Bankruptcy Cases

The Study Agencies have noted that "some trustees and creditors are considering compiling information contained in bankruptcy records electronically for easier administration of bankruptcy cases in which they have a claim. They may also envision some possible commercial use."(14) The Study Agencies have asked for comment on an appropriate commercial use of such information.

"Non-public" data, described in the Federal Register Notice as "additional data gathered by bankruptcy trustees in the course of administering the cases assigned to them," can include tax returns, and additional documentation or information regarding the value of assets and amounts of liabilities. Commercial use of such highly personal and sensitive non-public data raises several problematic issues and should be prohibited. In addition to privacy concerns, the non-public data should not be used for purposes other than those for which the information was collected (i.e., to administer the bankruptcy cases) for four reasons.(15) First, as discussed above in connection with certain items of public record data, disclosure of such non-public data may facilitate identity theft and other illegal conduct.

Second, trustees - whether appointed from a panel to a particular case or appointed by virtue of their position as a standing trustee -- serve as trustees as a result of governmental action and receive sensitive private information from debtors as a direct result of their appointment as trustees. Trustees use this information to scrutinize and marshal the debtors' assets, determine the universe of existing creditors, and ensure that all available assets are liquidated for the benefit of those creditors. The use of such non-public information for commercial purposes appears to fall outside the scope of the trustee's responsibilities.

Third, it is well-established that bankruptcy trustees are fiduciaries and thus owe a fiduciary's duty of loyalty to the bankruptcy estate and all participants in the system.(16) These common law duties and principles remain viable today.(17) It is difficult to reconcile the common law prohibition against self-dealing with the commercial use of information that trustees obtain in their fiduciary capacity. It is also difficult to reconcile the commercial use of

information obtained in a fiduciary capacity with the Department of Justice's recent rulemaking prohibiting standing trustees from using estate funds for their personal benefit.(18)

Finally, the commercial sale of such information by a trustee may implicate concerns under the Fair Credit Reporting Act (FCRA).(19) Generally, the FCRA limits the disclosure by "consumer reporting agencies" of "consumer reports," information that is used or expected to be used as a factor in determining a consumer's eligibility for credit, insurance, or employment. Applicability of the FCRA would turn on several factors including examination of the purposes for disclosing the information as well as the actual uses of the information.(20)

Notwithstanding these considerations, if the bankruptcy trustees begin to use debtors' non-public information for commercial purposes or any purpose other than the administration of the debtor's bankruptcy estate, the debtor should receive notice of this use and be given some opportunity to choose whether to have their information used in such a manner.

D. Related Issues

Finally, the Study Agencies may wish to consider the interplay between consumers' privacy interests and the Bankruptcy Code in the context of evaluating possible additional statutory changes. Traditionally, the Code vests a case trustee or a debtor in possession with sweeping powers to sell assets free and clear of liens and claims.(21) It is also well-settled, however, that a debtor or trustee in bankruptcy cannot take action in violation of extant law.(22) Recently, the Commission and various States have asserted that the sale of private customer information in direct violation of a company's privacy statement contravenes applicable law.(23) (We note that any governmental actions to exercise or enforce police and regulatory powers are exempt from the automatic stay pursuant to 11 U.S.C. § 362(b)(4).)

The interplay between these various interests is unsettled and involves competing considerations. For example, the more valuable the customer information is perceived to be, the greater the pressure on a bankruptcy estate to sell private information despite explicit pre-petition company promises to the contrary. The Bureau believes that the interplay of the Bankruptcy Code and law enforcement efforts to protect consumer privacy merit further in-depth analysis.

Conclusion

We are pleased to submit these comments. Please contact Jeanne M. Crouse, the Commission's Counsel for Bankruptcy and Redress, at (202) 326-3312, if there are questions about our comments or additional information that we may provide to assist your efforts in this important matter.

Respectfully submitted,

_____

Joan Z. Bernstein
Bureau of Consumer Protection, Director
Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580

1. These comments are the views of the staff of the Bureau of Consumer Protection of the Federal Trade Commission. They do not necessarily represent the views of the Commission or any individual Commissioner.

2. *See* Federal Register Notice Requesting Public Comment on Financial Privacy and Bankruptcy, 65 Fed. Reg. 46735 (July 31, 2000) (the Federal Register Notice).

3. 15 U.S.C. § 45(a).

4. The Commission does not have criminal law enforcement authority. Further, certain entities, such as banks, savings and loan associations, and common carriers, as well as the business of insurance, are wholly or partially exempt from Commission jurisdiction. See Section 5(a)(2) of the FTC Act, 15 U.S.C. § 45(a)(2), and the McCarran-Ferguson Act, 15 U.S.C. § 1012(b).

5. The FTC Act and most other statutes enforced by the Commission apply equally in the offline and online worlds. Thus, the agency has brought law enforcement actions to protect privacy online pursuant to its general mandate to fight unfair and deceptive practices, *see, e.g., FTC v. ReverseAuction.com, Inc.*, No. 00-0032 (D.D.C. Jan. 6, 2000) (settling charges that an online auction site obtained consumers' personal identifying information from a competitor site and then sent deceptive, unsolicited e-mail messages to those consumers seeking their business); and it also has pursued law enforcement, where appropriate, to address offline privacy concerns. *See, e.g., In re Trans Union*, Docket No. 9255 (Feb. 10, 2000), appeal docketed, No. 00-1141 (D.C. Cir. Apr. 4, 2000)(alleging that defendants' sale of individual credit information to target marketers was a violation of the Fair Credit Reporting Act).

6. In particular, the Commission has law enforcement responsibilities under the Fair Credit Reporting Act, which, among other things, limits disclosure of "consumer reports" by consumer reporting agencies, 15 U.S.C. §§ 1681 *et seq*., and under the Gramm-Leach-Bliley Act which restricts the disclosure of consumers' personal financial information by certain financial institutions, 15 U.S.C. §§ 6801-6809 (Subtitle A).

7. The Commission and its staff have issued reports describing various privacy concerns in the electronic marketplace. *See, e.g., Online Profiling: A Report to Congress* (June 2000); *Online Profiling: A Report to Congress, Part 2* (July 2000); *Individual Reference Services: A Federal Trade Commission Report to Congress* (Dec. 1997); *FTC Staff Report: Public Workshop on Consumer Privacy on the Global Information Infrastructure* (Dec. 1996); *FTC Staff Report: Anticipating the 21st Century: Consumer Protection Policy in the New High-Tech, Global Marketplace* (May 1996). The Commission has also recently issued a rule implementing the privacy provisions of the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801 *et seq*. *See* 16 C.F.R. Part 313, available at <http://www.ftc.gov/os/2000/05/glb000512.pdf>.

8. These fair information practice principles include: (1) notice (data collectors must disclose their information practices before collecting personal information from consumers); (2) choice (consumers must be allowed to choose whether and how personal information may be used for purposes beyond those for which the information was provided); (3) access (consumers should be able to view and contest the accuracy and completeness of data collected about them); and (4) security (data collectors must take reasonable steps to assure that information collected from consumers is accurate and secure from unauthorized use).

9. For a description of the FTC's identity theft activities, see Statement of the Federal Trade Commission on Identity Theft, United States House of Representatives, Committee on Banking and Financial Services (Sept. 13, 2000) <http://www.ftc.gov/os/2000/09/idthefttest.htm>.

10. The data analysis applies to the period from November 1999 through August 2000.

11. Importantly, although social security numbers serve as the critical piece of information needed to facilitate identity theft, other personal information routinely provided as part of public record data in bankruptcy cases also can assist criminals. Such personal information can include an individual's credit card information and bank account numbers. Easy access to this information on the Internet through the bankruptcy process could further facilitate identity theft as well as increase the risk of unauthorized debiting of accounts. That the individuals had filed for and obtained relief in bankruptcy likely would not deter such wrongdoing.

12. 65 Fed. Reg. 46736.

13. 11 U.S.C. § 341(d) (requiring United States Trustees to "orally examine the debtor" in chapter 7 cases to ensure that the debtor is aware of certain consequences of seeking bankruptcy relief).

14. 65 Fed. Reg. 46736.

15. Some of the discussion pertains only to trustees who serve in a unique role in the bankruptcy context. To the extent, however, creditors and others involved in the bankruptcy process may gain otherwise unrestricted access to non-public data, they too should not be permitted to use it for purposes other than for which it was collected.

16. *See, e.g., Woods v. City Nat'l Bank & Trust Co.*, 312 U.S. 262, 278, *reh'g denied*, 312 U.S. 716 (1941). The common law duty of loyalty prohibits any self dealing. Mosser v. Darrow, 341 U.S. 26 (1951).

17. *United States Trustee v. Bloom (In re Palm Coast, Matanza Shores Ltd. Partnership)*, 101 F.3d 253, 257-58 (2d Cir. 1996); *Walsh v. Northwestern Nat'l Ins. Co. (In re Ferrante)*, 51 F.3d 1473, 1479-80 (9th Cir. 1995).

18. *See* 62 Fed. Reg. 30171 (Final Rule Establishing Qualifications and Standards for Standing Trustees), codified at 28 CFR § 58.4. Given the common law prohibitions against self-dealing, one approach could be to require the trustees to certify in writing that (1) this sensitive information will be distributed on the same terms and conditions to all persons or entities and (2) that the trustees will not benefit from the dissemination of this information in any way, either directly or indirectly (including through any related or non-profit organizations). Such certifications would be consistent with those required by the Department of Justice when standing trustees submit their annual budgets or when standing trustees seek limited waivers regarding certain related party transactions. *See, e.g.*, 28 CFR § 58.4.

19. 15 U.S.C. §§ 1681-1681u.

20. 15 U.S.C. § 1681a. It is also worth considering whether the Gramm-Leach Bliley Act, 15 U.S.C. §§ 6801-6809 (Subtitle A), which generally limits the disclosure of consumers' personal financial information by a "financial institution," might bear upon subsequent uses of such information.

21. *See* 11 U.S.C. § 363.

22. 28 U.S.C. § 959.

23. *See, e.g., Federal Trade Commission v. Toysmart.com, LLC, et al.*, Civil Action No. 00-11341-RGS (D. Mass. filed July 10, 2000).