For Release Upon Delivery
10:00 a.m., July 21, 1999

TESTIMONY OF

JOHN D. HAWKE, JR.

COMPTROLLER OF THE CURRENCY

before the

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

of the

COMMITTEE ON BANKING AND FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

July 21, 1999

Statement required by 12 U.S.C. 250:

The views expressed herein are those of the Office of the Comptroller of the Currency and do not necessarily represent the views of the President.

Introduction

Madam Chairwoman, Congressman Vento, and Members of the Subcommittee, thank you for the opportunity to testify about an issue that has enormous ramifications for the banking industry and the customers they serve -- financial privacy. I commend you, Madam Chairwoman, for holding this timely hearing on an issue that is generating increasing public attention and concern.

Fundamental to the relationship between banks and their customers is the trust that customers place in their banks to uphold the confidentiality of that relationship. In fact, the banking industry has had a long history of safeguarding customer confidentiality. A 1961 court case aptly described this tradition stating, AIt is inconceivable that a bank would at any time consider itself at liberty to disclose the intimate details of its depositors= accounts. Inviolate secrecy is one of the inherent and fundamental precepts of the relationship of the bank and its customers or depositors.≅[1]

Today, however, this tradition is under pressure from technological advances and from the demands of a competitive marketplace that have placed a premium on the availability of personal information -- often at the expense of personal privacy. Resistance to this pressure is of enormous importance, for if banks fail to honor customer expectations that personal information will be kept private and confidential, they will impair the most priceless asset of their banking franchise -- their customers= trust. Thus, privacy is not just an important consumer issue; it is an issue with implications for the long term vitality and stability of the banking system.

Banking is an information-driven industry. Bankers have always relied on access to personal financial information to make fundamental judgments about consumers= qualifications for financial products and services. Information exchanges thus serve a useful and critical market function that benefits consumers and financial institutions alike, in facilitating credit, investment, insurance and other financial transactions.

Recent advances in technology that permit the efficient collection, storage, analysis and dissemination of vast stores of information, coupled with the changing structure of the financial services industry and the development of efficient new delivery systems, have increased the market value of customer information. Passage of financial modernization legislation will further change the financial services landscape, permitting diverse financial companies to affiliate and to pool their customers= personal information. While financial conglomerates may profit from the cross marketing opportunities occasioned by an expansion of powers and the Awarehousing≅ and Amining≅ of personal data, and while consumers may benefit from the availability of a broader array of custom-tailored products and services, there is a serious risk that these developments may come at a price to individual privacy.

Until very recently, consumers knew little about the information-sharing practices of the companies that they patronized. As these practices become more widely known, however, the public appears ready to react against real or perceived abuses in the treatment of their personal information. When that information relates to financial or medical circumstances, customers are

---

[1] Peterson v. Idaho First National Bank, 367 P.2d 284,290 (Idaho 1961).

even less tolerant of perceived violations of privacy. Bank customers in particular, expect their banks to protect the confidentiality of their transactions.

A review of existing privacy laws and banking practices reveals that more can be done to assure the public about the responsible uses of financial information. H.R. 10, as passed by the House, adopts a measured approach that provides consumers with notice and choice about the information-sharing practices of financial institutions, without impeding the flow of information essential to doing business. This common sense approach is a positive step in assuring consumers that their information will be handled appropriately and in providing consumers with increased control over their personal information. Customers are likely to expect more, however, and the challenge is how best to meet their reasonable expectations of privacy without defeating the potential benefits available from advances in technology and the new corporate affiliations that would be made possible by H.R. 10.

My testimony today will expand upon these concepts and address the questions posed by the Chairwoman=s letter of invitation.

Privacy Laws

The letter of invitation asked about existing laws and regulations that protect financial privacy. Although the United States does not have a comprehensive, universal privacy law, there are a number of legal provisions that help to ensure that consumer financial information will be treated as confidential.

On the federal level, the most significant of these laws is the Fair Credit Reporting Act (AFCRA≅), which prohibits Aconsumer reporting agencies≅ from sharing information about consumers with third parties unless the third party has a Apermissible purpose.≅ The Act enumerates with some precision just what these permissible purposes are: they include using customer information (1) in connection with a credit transaction or insurance underwriting involving the consumer, (2) in other situations in which the third party has a legitimate business need for the information in connection with a business transaction that is initiated by the consumer, (3) for employment purposes, such as hiring, (4) in connection with Aprescreened≅ transactions involving a Afirm offer of credit or insurance,≅ assuming the consumer has not elected to be excluded from such offers, and (5) where the consumer has given written permission for the information to be shared.

These restrictions sharply curtail the circumstances in which the major credit bureaus and other central repositories can share the consumer financial information in their databases. They cannot, to note one important example, generally give out confidential information to telemarketing companies prospecting for sales.

Perhaps just as important as these limits on credit bureaus, from the standpoint of consumer financial privacy, are the limits that FCRA places on other business entities, such as banks, securities firms, and insurance companies. Roughly speaking, FCRA defines Aconsumer reporting agency≅ as any person or entity that furnishes Aconsumer reports.≅[2] Consumer reporting agencies are subject to a number of significant requirements under the Act -- including the information-sharing restrictions described above and related procedural requirements, accuracy standards, consumer access requirements, and dispute resolution procedures.

As a practical matter, unless they wish to become consumer reporting agencies subject to the requirements described above, banks and other financial firms may only share information that is not Aconsumer report≅ information, such as (1) information that relates solely to the institution=s own transactions or experiences with the consumer, and (2) any other information shared with affiliates, provided that the consumer is first given notice of the proposed affiliate information-sharing and an opportunity to Aopt out≅ -- that is, to object to the sharing of individual information.

Thus, FCRA does *not* provide consumers with the ability to object to or prevent the sharing of so-called Atransaction and experience information,≅ which includes a wide range of sensitive information about individuals -- not only loan repayment patterns, but also, for example, information from an insurance affiliate about one=s medical insurance claim history. Moreover, this information may be shared with affiliates or with unrelated third parties, regardless of their intended use of the information. In this light, it is not at all surprising that much of the current debate about financial privacy revolves around these provisions relating to Atransaction and experience information.≅

Other federal laws concerning financial privacy are much more limited in scope, involving either disclosure of information-sharing practices or governmental access to information. In particular, the Electronic Fund Transfer Act and its implementing regulation, the

---

[2]The term Aconsumer report≅ means any communication of information by a consumer reporting agency that bears on a consumer=s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, which is used or collected for a permissible purpose under FCRA.

Federal Reserve Board=s Regulation E, require financial institutions to provide deposit account customers a general disclosure about when, in the ordinary course of business, the institution will share information about the consumer=s account with affiliates or other third parties. These provisions require only disclosures, however, and do not impose any substantive limits on the actual sharing of information or enable consumers to opt out of such sharing.

The letter of invitation also inquired specifically about the Privacy Act of 1974 (APrivacy Act≅) and the Right to Financial Privacy Act (ARFPA≅). These laws provide controls over the federal government=s collection, use, and disclosure of consumer financial information. Among other requirements, the Privacy Act permits a federal agency to maintain in its records Aonly such information about an individual as is relevant and necessary≅ to accomplish a required agency purpose, and, with certain exceptions, prohibits the agency from sharing that information with another agency or person without the consent of the individual in question. Thus, unless an exception applies, the federal government may share this information only if the individual Aopts in.≅

In May 1998, the President issued an executive order directing all federal agencies to review their records and information systems to ensure compliance with the Privacy Act. The OCC promptly took appropriate actions to fulfill this mandate, including an inquiry to all employees to identify new or modified systems of records that might be covered by the Act. We will ensure both that new and existing records systems are fully compliant with the Privacy Act.

RFPA deals specifically with federal government access to customer financial records at a financial institution. RFPA limits such access -- as well as any further sharing of the information within the federal government -- to specifically enumerated situations. As is the case with the Privacy Act, these exceptions generally represent a careful balancing of privacy interests with important bank supervisory, law enforcement, and other governmental functions. In response to your question, Madam Chairwoman, although I have no evidence that these laws are not effectively accomplishing their limited purposes, they deal with potential privacy intrusions by the federal government, and do not cover the private sector or even state governmental units.

State laws also provide some measure of protection for consumer financial information. As an initial matter, many states have enacted counterparts to the FCRA and EFTA, the primary federal laws discussed above relating to private sector financial privacy. The federal laws in question generally provide that state laws on the same subject matter will not be preempted unless inconsistent with the federal provisions -- and then only to the extent of the inconsistency. Thus, the state and federal laws often comfortably coexist. There are important exceptions to this principle, however, the most important of which may be that any state law regarding the sharing of information with affiliates -- whether Atransaction and experience information≅ or

other information -- is specifically preempted by the FCRA until 2004. Thus, state law cannot provide *greater* protections for consumers than the FCRA in this regard.

In discussing state law, it also should be noted that common law principles -- particularly a fiduciary duty of confidentiality owed by banks to their customers -- may provide additional protections. As with state statutory law, however, these judicially recognized protections vary widely by jurisdiction, and do not provide equal protections to all U.S. consumers.

The letter also specifically asked about the OCC=s regulatory authority with respect to financial privacy. While we cannot promulgate regulations or issue authoritative interpretations for any of the laws discussed above, the OCC, like the other federal banking agencies, has the authority to remedy violations of any federal or state law or regulation with respect to the entities we supervise. This authority is granted in section 8 of the Federal Deposit Insurance Act, and includes both the authority to order that the bank cease and desist from violating any such law or regulation and, in certain circumstances, to order reimbursement for harms.

I must note, however, that with respect to the FCRA -- perhaps the most important federal law relating to financial privacy -- our enforcement authority has been severely hampered by 1996 amendments that curtailed our ability to examine national banks for compliance with the Act. In particular, we may examine a bank only in response to a complaint or if we Aotherwise have knowledge≅ of a violation. No other consumer protection statute we enforce similarly limits our ability to examine banks for compliance.

OCC Privacy Initiatives and Bank Practices

Over the past year, the OCC has issued three advisory letters to national banks focussing on different elements of privacy -- security of confidential customer information, compliance with existing legal requirements for consumer notice and choice regarding information sharing, and measures to address customer concerns about national banks= privacy practices in the Internet environment. Attached to my testimony are copies of these advisory letters.

Pretext Calling. The first advisory letter, issued in August 1998, alerted banks to a deceptive practice that victimizes both the banks and their customers. The subject of that advisory was Apretext phone calling,≅ a practice whereby account information brokers, posing as bank customers, gain improper access to confidential account information. In addition to warning banks about this practice, the advisory letter encourages them to establish clear guidelines, procedures, and internal controls to reduce the chances of unwitting and unauthorized disclosures of customer information by bank employees.

The OCC was initially alerted to pretext calling through its participation in an

interagency bank fraud working group. In response, the OCC jointly prepared the advisory with the other banking and law enforcement agencies in the working group. Additionally, the OCC has previously testified before this Committee in support of legislation aimed at curbing pretext calling. We generally support those provisions in H.R. 10, although we do have concerns about the enforcement authority.

FCRA Affiliate Information Sharing. The second advisory letter issued in March 1999 addressed banks= obligations under the FCRA to notify customers about affiliate information sharing and to provide customers with an opportunity to opt out of that sharing. The advisory letter discusses the most effective practices for meeting these requirements that the OCC observed among national banks. In doing so, the advisory features examples of notices that make bank information handling practices more readily understandable and transparent to customers and procedures that provide convenient opt-out mechanisms.

This advisory was the product of the OCC=s Privacy Working Group, an interdisciplinary team that includes senior level OCC officials, which was established to inform the Comptroller about financial privacy issues and to coordinate agency policy and initiatives. In assessing general industry privacy practices, working group members discovered that some bank FCRA affiliate sharing notices were often buried in fine print in multipage agreements and provided customers with little useful information about the bank=s information sharing practices. Other notices, however, were clear, simple, and precise and provided information sufficient to allow bank customers to make informed choices about the sharing of their information. It is those notices we highlight in the guidance.

Internet Privacy Policies. Our third advisory, issued in May 1999, informed banks about effective practices for developing privacy policies, in general, and prominently posting those policies on bank Web sites. The advisory letter provides examples of the various mechanisms banks have employed to make their privacy policies easy to spot and easy to understand by Web site visitors. Additionally, the advisory discusses effective procedures used by large and small banks to establish privacy policies, encourage employee understanding of and compliance with stated policies, and address privacy-related inquiries and complaints from customers.

The OCC issued this guidance in response to a comprehensive survey conducted by the FTC last year that found a general failure of Web sites, including those operated by financial institutions, to post any disclosures about their information handling practices. The OCC believes it is especially important for banks to reassure customers about the safeguarding of their personal information when information is communicated in an online environment. The advisory is intended to sensitize banks to some of the challenges posed by the Internet to consumer privacy and to give constructive examples for meeting these challenges.

OCC Privacy Policy

The OCC takes privacy issues seriously in its own operations. Last year we adopted a comprehensive new privacy policy, which was posted on our Web site in October 1998. The OCC=s privacy policy is conspicuously listed on the opening page of our Web site.

Pursuant to our privacy policy, we do not collect or store information about members of the public who call or write the agency or visit our Web site, unless they identify themselves and ask for a response to an inquiry or request. We do, however, collect and store certain non-personal information about visitors to our Internet site when they log on to read or download information, such as OCC bulletins, alerts or press releases, and this is disclosed in our privacy policy. We use this information simply to help us stay abreast of technical upgrades that can make our site more accessible to visitors, and to record the date and time of all visits to our site.[3] We do not attach Acookies≅ to the browsers of our visitors.

If visitors identify themselves when they contact us, appropriate agency employees may see this information. We adhere to the following principles in handling information provided by members of the general public:

X We use personally identifying information only for the purpose for which it is originally collected.

X We maintain personally identifying information in secure computer systems and we limit employee access to those with a business reason to see it.

X We do not disclose personally identifying information to anyone outside the OCC, except where compelled by law or in connection with a criminal investigation.

---

[3]Specifically, we record: The name of the domain from which a visitor accesses the Internet (for example, aol.com or princeton.edu); the Internet address of the Web site from which the visitor linked directly to our site, if any (for example, www.fdic.gov, if the visitor linked to the OCC from the FDIC Web site, or www.yahoo.com, if the OCC Web site was located using the Yahoo search engine); the type of Web browsing software used to view our site; and the date and time the visitor accessed our site.

Public Policy Responses

Maintaining the public=s confidence in the banking system has long been a critically important national policy objective. In furtherance of that objective, we have a program of federal deposit insurance and a comprehensive system of bank licensing, supervision, and regulation. Another critical factor in upholding public confidence in the banking system has been the assurance that banks will honor customers= expectations that information provided or maintained in connection with their financial transactions will be kept in confidence. Traditionally, national banks have earned the public=s trust in this regard by honoring those expectations.

However, developments in the marketplace are affecting the public=s concerns about privacy in ways that were not contemplated until fairly recently. Indeed, these concerns have evolved since the enactment of the laws dealing with the collection and use of financial information that I previously mentioned. These developments, and the consequent evolution of public concerns, explain why we are engaged in this public policy debate on privacy.

One reason for the increased public concern about privacy is the explosion of information technology. Today, personal information about individuals can be accessed, reviewed, combined, rearranged, and transferred with just a few key strokes. Information about a person=s financial or medical condition, buying habits, and other characteristics -- down to the most personal level -- can be used to create profiles for marketing or for developing new products. As a result of changes in technology, information is an increasingly valuable commodity.

Financial institutions have generally safeguarded customer information -- not only to preserve the trust and goodwill of their customers -- but also to protect what the institutions consider to be proprietary information. However, it is now possible to create huge databases that can be easily shared among affiliates due to improvements in technology. And with the development of speedy electronic marketing and delivery systems, institutions are using customer information for purposes other than those for which it was originally provided or maintained. Centralized customer databases within new financial conglomerates offer the promise of increased business opportunities, lower costs, and improved financial products and services for consumers. Information technology now enables combined financial services companies to offer one-stop shopping to customers and to adapt products to their customers= changing financial needs over the course of a lifetime.

At the same time, however, the commoditization of information, and the pace and magnitude of mergers and affiliations in the financial services industry -- which will be accelerated with financial modernization legislation -- have sharpened privacy concerns.

Obviously, affiliations among diverse sectors of the financial services industry offer tremendous opportunities for these companies to operate in complementary ways, achieve efficiencies, and expand through cross-marketing of products to customers. However, these new combinations also fuel both the perception and reality that individuals are losing control over their personal information. When the information is highly sensitive, such as medical and financial information, consumer concern over who has control over its disposition is magnified.

The banking industry has recognized the need to respond to consumer privacy concerns. Banking trade groups are to be commended for developing a common set of privacy principles that explicitly recognize a customer=s expectation of privacy, and it appears that an increasing number of banks are adopting this model. Financial institutions clearly have the capacity to react swiftly to concerns about abusive practices, as we have seen recently when several major banks discontinued their practice of selling customer account information to third-party telemarketers. I applaud these banks for their prompt responses when this privacy issue became known.

Let me now turn to the current legislation. The privacy provisions in H.R. 10 embody the important elements of notice and choice -- a concept already contained in the Fair Credit Reporting Act, and one with which financial institutions are very familiar. When administered properly, notice and choice enable consumers to make informed decisions about the disposition of their personal information and maintain control over their information. We have learned through our research as part of the Consumer Electronic Payments Task Force, and survey data bear this out, that consumers have different levels of sensitivity to privacy. Notice and choice allow those consumers who place a premium on privacy to protect that privacy at the expense of forgoing certain marketing opportunities or even beneficial treatment from their financial institutions in the form of cost savings. On the other hand, consumers without the same desire for privacy, may choose to relax confidentiality in exchange for the benefits that they perceive will result from information sharing. The bottom line is that it is the consumer=s choice to give up or retain personal privacy -- not the institution=s.

The privacy provisions in H.R. 10 will enhance the notice and choice requirements already existent under FCRA. The existing law limits the sharing of certain information among affiliated companies unless consumers are provided with notice about the sharing and an opportunity to opt out of that sharing. However, as I noted above, the banking agencies are presently hamstrung in their ability to enforce these provisions. H.R. 10 will restore the agencies= examination authority.

Additionally, and equally significant, H.R. 10 will give the banking agencies the authority to implement FCRA by regulation. As previously mentioned, the OCC has seen a number of affiliate sharing opt out notices that are virtually invisible to the consumer and

meaningless in their content. Regulatory authority should allow the banking agencies to prescribe meaningful and uniform standards for these notices. Also, since we published the advisory about affiliate information sharing requirements in May, we have received a number of inquiries from banks and their attorneys about the meaning of various ambiguous provisions of the FCRA. The rulemaking authority in H.R. 10 will enable the agencies to deal with the complex -- and evolving -- nature of the issues presented, pursuant to a public notice and comment process, that will permit adjustments to be made, if and when changing circumstances warrant.

The scope of personal information that H.R. 10 protects against disclosure will address a major exception in current law -- transaction and experience information. Under FCRA, companies can freely share the confidential information that they derive from their relationship with their customers, including account type and balances, payment history, credit limits, and amount and date of last payment. In the recent matter involving a bank=s transfer to telemarketers of confidential customer information, including credit card and checking account numbers, much of the personal information shared was transaction and experience information. H.R. 10 would expressly prohibit the sharing of account numbers and would require notice and consumer choice with respect to the sharing of the personal information implicated in this case.

In my view, however, a serious question can be raised whether H.R. 10 goes far enough in protecting customer confidence in the confidentiality of their relationships with their bank, and it draws a distinction between information sharing with affiliates and nonaffiliates that may not be relevant for customers. In his May 4th proposal regarding privacy, the President indicated his support for legislation that would give consumers control over the use and sharing of <u>all</u> their financial information, both among affiliates and nonaffiliated third parties. H.R. 10 is a good first step in meeting that goal, but I believe that customers will reasonably expect more. Is it realistic to think that customers will distinguish between situations when their confidential information is transferred to affiliates vs. nonaffiliates of their bank? Would customers believe that the legislation adequately covers their reasonable expectations regarding the use and transfer of their confidential information? If the answers to these questions are in the negative, the failure to provide protection for the sharing of information with affiliates could have a profound effect -- particularly in a world of expanded financial conglomeration -- on the willingness of customers to maintain the kinds of relationships with the banking system they have in the past. While the desire of bankers to take advantage of new cross-marketing opportunities is entirely understandable, I believe that a primary objective of policy makers should be to assure that doing so does not cause fundamental damage the banking system.

Conclusion

I again thank the Chairwoman and other members of the subcommittee for this

opportunity to testify on this important issue. I cannot overstate the importance of addressing consumer expectations about the confidential treatment of financial information to maintaining the public=s confidence in the banking system. And I urge that, in crafting an appropriate response to consumer privacy concerns, banks and Congress put themselves in the shoes of a customer and ask, AWill my financial institution use my personal information in a manner consistent with my expectations?≅ and AWill I have any control over the use of my information?≅ Whatever legislative formulation ultimately results, American consumers deserve to be able to answer AYes≅ to those questions.