For Release Upon Delivery
10:00 a.m., July 28, 1998

TESTIMONY OF

JULIE L. WILLIAMS

ACTING COMPTROLLER OF THE CURRENCY

Before the

COMMITTEE ON BANKING AND FINANCIAL SERVICES

of the

U.S. HOUSE OF REPRESENTATIVES

July 28, 1998

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.

Mr. Chairman, Ranking Member LaFalce and members of the Committee, I appreciate this opportunity to appear before you today to testify on issues regarding the proper handling and safeguarding of customer financial information and the protection of consumer privacy. The Office of the Comptroller of the Currency (OCC) applauds the Chairman's leadership working to curb information broker abuses that victimize both banks and their customers. And, we also commend Congressman LaFalce for identifying and bringing to the Committee's attention other timely privacy concerns that have been heightened by recent changes in the marketplace, particularly mega-mergers and the growing customer databases of the companies that result from those transactions.

The financial services industry has had longstanding experience in handling and safeguarding sensitive customer information and protecting consumer privacy. Access to and use of financial information is the lifeblood of the financial services industry -- ensuring that institutions make appropriate credit determinations, provide proper investment guidance, extend insurance wisely, as well as identify new market opportunities. Information also assists financial institutions in properly identifying their customers in order to prevent fraud and in knowing their customers to guard against money laundering.

It is thus essential that financial institutions maintain customers' trust and confidence in their handling of personal information to ensure the continued flow of this information. Failure to properly safeguard information, or the handling of information contrary to customers' reasonable privacy expectations, can result in loss of business opportunities and could also present safety and soundness risks in the form of potential liability and damage to banks' reputations.

Recent developments, primarily technological advances and the rapidly changing structure of the financial services industry, have presented new opportunities for the financial services industry while, at the same time, heightening the public's concern about financial privacy. Advances in electronic banking and communications technology have enabled banks and other businesses to gather, analyze, and disseminate customer information in a more expedient and efficient manner. Use of on-line computer software facilitates the transfer of information almost instantly.

Proposed bank mega-mergers and the emergence of financial services conglomerates will result in immense databases of customer information. Pending financial modernization legislation would further facilitate the creation of diversified, potentially very large, financial entities that will be able to amass vast amounts of information about customers' credit and investment habits, deposit accounts and insurance transactions. Companies will likely use and manipulate this data to target customers for increasing arrays of products and services tailored to meet a customer's particular needs and financial circumstances. Accordingly, this information can result in increased business opportunities for industry and improved products and services for consumers.

However, these advances in corporate structure and technological capabilities raise pressing issues about how banks will safeguard and use the expanding base of consumer data.

Surveys indicate that consumers are becoming increasingly anxious about how their personal information is being handled by the different companies with which they do business and about their lack of control over its dissemination. In some cases, consumers are kept deliberately ill-informed about the information practices of these companies. Without sufficient information, consumers cannot make informed choices about how and to what extent companies should be able to use their data beyond the purposes for which it was provided. Moreover, an increasing number of news stories have reminded the public about the limits of confidentiality, the ease with which determined crooks can evade protections designed to safeguard data, and the nightmarish consequences that befall individuals victimized by so-called identity theft.

Thus, the parameters of the privacy debate can be defined as the tension between the potential economic benefits for businesses and consumers through the development of enhanced information assets on the one hand and the public's increasing concern over privacy on the other hand. The challenge for financial institutions is to use this wealth of customer information responsibly, to safeguard it against improper access, and to build consumer confidence in the knowledge that both are occurring.

Shortly after I became Acting Comptroller, I formed a Privacy Working Group (PWG) within the OCC to focus on the challenges banks face in addressing emerging consumer privacy issues. The PWG has already begun work to look into the areas of safeguarding bank customer information, website disclosures of bank privacy policies, and the adequacy of information sharing notices furnished by banks to their customers under the Fair Credit Reporting Act (FCRA). Our goal in these areas is to articulate guidance on "effective practices" for website and FCRA disclosures, as well as to consider issuing guidance to banks on safeguarding sensitive customer data. I will discuss each of these initiatives in the testimony.

Based on our work to date, key privacy issues today seem generally to fall into three areas: safeguarding/security of customer information; privacy related disclosures; and the role of regulators. The discussion that follows is organized around these three areas. The first issue area--safeguarding customer information--will include a discussion of the OCC's views on the Chairman's bill, the Financial Information Privacy Act of 1998.

I. Safeguarding/Security of Customer Information

Safeguarding sensitive customer information is essential to a bank's maintaining the trust of its customers and, ultimately, to the bank's safe and sound operations. Banks currently take a number of steps to preserve the integrity of customer data. Banks often use personal identification numbers, passwords, or other unique identifiers in conjunction with other identifying information, such as name, address, mother's maiden name, and account number or account activity, to ensure they are appropriately disclosing information only to their customers. Financial institutions also are exploring the use of biometrics and are using encryption to safeguard customer information that is electronically transmitted. In addition, the OCC routinely examines banks for internal controls to ensure that access to customer data is limited to bank

employees who need the data to properly perform their duties. The agency also examines the banks' data processing systems using the Federal Financial Institutions Examination Council's exam procedures to evaluate information systems. Further, the OCC has published additional guidance for examiners and bankers on data security.

Despite these precautions, however, some banks and their customers have been the victims of scams involving the unauthorized procurement of customer data for legal or illegal financial gain. This problem is exacerbated by the fact that consumer information that used to be confidential is increasingly in the public domain, account numbers are sometimes retrievable from trash cans, and passwords and PINs are not always closely guarded by consumers. Two growing and alarming practices that are thriving on this ready access to consumer information have come to be known in the public arena as account information brokering and identity theft. Mr. Chairman, your bill focuses on a significant abuse in this area, and the OCC strongly supports your efforts.

Account Information Brokering

As I have explained, there is a tremendous demand for information about individuals' and businesses' financial information. For example, attorneys, debt collectors and private investigators use bank account information in lawsuits and other proceedings. This demand for account information, combined with the availability of free advertising on the Internet, has led to a dramatic increase in the number of account information brokers.

These brokers gather confidential financial information, including specific account numbers and balances, from various public sources and from nonpublic sources, such as banks, using a technique known as "pretext telephone calling." Brokers who engage in this practice call banks and use surreptitious or fraudulent means to try to coerce bank employees into providing a customer's account information. For example, a broker armed with an individual's social security number may pose as a bank customer who has misplaced an account number, and repeatedly call the bank until the broker finds a bank employee willing to provide the information. The broker then sells this information to anyone who is willing to pay for it, including identity thieves, who may use account information to engage in check and credit card fraud, and other criminal acts.

The use of surreptitious or fraudulent means to obtain a customer's account information may violate state and federal laws prohibiting unfair and/or deceptive practices. It also may violate the federal wire fraud statute, 18 U.S.C. §1343, although the loss to the individual may not be of sufficient magnitude to result in prosecution under the statute. However, the existing statute prohibiting false statements to financial institutions, 18 U.S.C. §1014, does not apply to account information brokering because it is limited to statements made in connection with applications, loans, advances, commitments or similar transactions, and not with procuring information. There is no federal law that directly prohibits the procurement of customer account information from financial institutions under false pretenses.

Financial Information Privacy Act of 1998

The OCC supports Chairman Leach's bill, the Financial Information Privacy Act of 1998 (FIPA), which is aimed at stopping the practice of obtaining customer account information from financial institutions under false pretenses. Its important to note here that in our experience banks take this issue very seriously, and have traditionally done a good job protecting customer information. But now, more is required. The FIPA addresses an area of growing concern and fills in gaps in federal law.

To summarize, FIPA prohibits persons from obtaining, or causing to be disclosed, customer information held by a financial institution by: (1) knowingly making a false statement to a financial institution's officer, employee or agent; (2) knowingly making a false statement to a financial institution's customer; or (3) knowingly providing any document to an officer, employee, or agent of a financial institution that is forged, counterfeit, lost, stolen, or otherwise fraudulently obtained. FIPA also prohibits any person from receiving financial institution customer information that the person knows or has reason to know was obtained in the manner described above. These prohibitions would be enforced by the FTC for information brokers, by the federal financial supervisory agencies for financial institutions, and by the States. The bill also provides for criminal penalties for violations of the prohibitions, with fines pursuant to Title 18 of the U.S.Code and/or imprisonment up to 10 years. The bill preempts state laws only to the extent they are inconsistent with the statute. It requires the Comptroller General to report to Congress within 18 months after enactment on the adequacy of the Act's remedies, and to make recommendations for additional legislative or regulatory action to address threats to the privacy of financial information.

The provisions of this bill appear to us to be a focused and efficient approach to an emerging problem. We support the FIPA and welcome the opportunity to work with the Committee on this initiative.

Agency Advisory

The OCC has been working with the other banking agencies, the FBI, IRS, Secret Service and FTC and other agencies to develop guidance for the financial services industry about information brokering practices employing pretext phone calling. We expect that our guidance in this area will alert financial institutions to this practice; enhance their awareness of issues surrounding the confidentiality and sensitivity of customer information generally; and suggest appropriate measures for the protection of customer data from unwitting disclosures. We plan to provide specific guidance to banks about the need to ensure proper employee training regarding appropriate security measures, as well as the adoption of policies addressing financial privacy, and the desirability of strong controls to decrease the likelihood of improper or illegal disclosure. Because of the importance of this area, we expect to issue this guidance in the near future, and we are hopeful this can be done by the other agencies as well.

Identity Theft

Identity theft is the practice whereby a person obtains personal information on an individual such as a social security number, and fraudulently uses that information to impersonate the individual in cashing checks, obtaining and using credit cards, or obtaining loans, all with the intention of stealing the funds obtained. It may take a week, a month, or longer to detect the initial fraud, particularly if the crook has the credit card or other bills sent to an address that is not the victim's. These thieves also often strike repeatedly. In the end, the victim is left having to repudiate the debts incurred by the thief. It can take years for the victim to repair a tarnished credit record.

A report released by the General Accounting Office in May found that cases of identity theft are increasing. The American Bankers Association has informed consumers that identity theft is one of the fastest growing types of financial fraud.

For these reasons, the OCC supports S. 512, the "Identity Theft and Assumption Deterrence Act of 1998," and its House counterpart, H.R. 4151. These bills make it a crime to knowingly and unlawfully possess, transfer or use a means of identification of another person with the intent to commit or facilitate any unlawful activity. They provide for restitution to victims of the offense. And they require the FTC to establish a centralized complaint and consumer education service for victims of identity theft, and to refer victims to appropriate entities, including consumer reporting and law enforcement agencies.

The OCC's Privacy Working Group is currently looking into the practices and procedures that banks employ to guard against identity theft. It is clear that banks must have sufficient measures in place to properly identify their customers, but these measures cannot be so intrusive or burdensome that they alienate bank customers attempting to conduct routine business. Depending on our findings, we will consider issuing guidance later this year to assist banks in avoiding situations that put their customers' identity and finances in jeopardy.

II. Adequacy of Privacy-Related Disclosures

The financial services industry, among others, routinely collects sensitive data from individuals in the course of performing routine business. Yet relatively few industries inform their customers about what they do with this information and whether they furnish it to others for purposes unrelated to its initial use. We learned in our work on the Consumer Electronic Payments Task Force (Task Force)[1] that consumers want to be better informed about the use of

[1]To ensure that consumer concerns arising from new electronic payment technologies receive appropriate consideration, the Secretary of the Treasury, Robert E. Rubin, established the Consumer Electronic Payments Task Force ("Task Force") in the fall of 1996. Eugene A. Ludwig, Comptroller of the Currency, chaired the Task Force which included Richard L. Gregg, Commissioner of the Financial Management Service; Jack Guynn, President of the Federal Reserve Bank of Atlanta; Andrew C. Hove, Jr., Chairman of the Federal Deposit Insurance Corporation; Edward W. Kelley, Jr., Member of the Board of Governors of the Federal Reserve System; Robert Pitofsky, Chairman of the

their personal data and they want more control over its ultimate disposition. We found, generally, that consumers want adequate disclosures about a company's information collection and use policies. They do not want to reveal more information than is needed for a transaction. And, consumers are concerned about possible secondary uses of their information beyond that needed for the original transaction. These and other concerns about data security are heightened when consumers are asked to furnish personal information in an on-line environment.

Yet there are no privacy laws that afford consumers comprehensive protection in the private sector uses of their personal information, or even in the disclosure of the uses of that information.[2] Instead, the Task Force, government agencies, and the White House have urged industries to adopt meaningful self-regulatory measures in the privacy area, particularly with respect to Internet data collection. Where privacy protections have been enacted, they have been on a sectoral basis, such as recent amendments to the Fair Credit Reporting Act that provide consumers with disclosures about certain types of information sharing and an opportunity to "opt out" of such sharing.

Self-Regulatory Measures for On-Line Data Collection

In June 1998, the FTC released a report to Congress containing the results of a survey of 1,400 websites, including financial service providers, to determine whether and to what extent these sites posted privacy policies. The FTC also examined the content of these privacy policies to discern whether they addressed four fair information practices: (1) notice of information practices; (2) consumer choice as to how that information is to be used beyond the purpose for which the information was provided; (3) consumers' access to their information and an opportunity to correct it for inaccuracies; and (4) reasonable steps to keep the information secure. The Commission found that over 85 percent of these websites collected personal information, but that only 14 percent provided any notice about information practices, and that only 2 percent provided notice by means of a comprehensive privacy policy. The survey shows that financial service providers fared no better or worse than any other industry in posting privacy policies.

Federal Trade Commission; and Ellen Seidman, Director of the Office of Thrift Supervision.

The Task Force established as its mission to identify, in partnership with the industry and the public, consumer issues raised by emerging electronic money technologies and to explore the extent to which innovative responses are being developed that are consistent with the needs of this developing market.

[2]Privacy protections are essentially evolutionary in the United States, and there is little precedent for comprehensive government established privacy protections. Unlike the nations of Western Europe, the United States does not have universal or omnibus privacy laws. Privacy protections in the United States have evolved on a sectoral basis reflecting in part how federal and state legislatures address competing policy objectives, including the prevention and prosecution of criminal acts.

Attached to the testimony is an excerpt from the Consumer Electronic Payments Task Force Report which contains a discussion of federal and state privacy laws.

The OCC takes the results of this survey seriously and believes that financial institutions that have websites should be posting meaningful privacy policies on their websites. The OCC's Privacy Working Group is currently meeting with interested industry representatives and privacy advocates about effective website privacy disclosures. We are researching what banks now are doing in this area and expect to issue guidance about what constitutes "effective practices" in webpage privacy policies disclosure. I should also note that we have an excellent working relationship with the Federal Trade Commission on these and other related projects.

Fair Credit Reporting Act

Recent amendments to the FCRA permit affiliated companies to share customer information, free of the restrictions placed on credit bureaus, provided that these companies clearly and conspicuously disclose this fact to consumers and provide consumers with an opportunity to direct that the information not be shared.[3] This affiliate-sharing provision provides new opportunities for both industry and consumers. It allows industry to expand its customer databases and it also affords consumers the opportunity to make informed privacy choices. The ability of consumers to make such informed decisions, however, turns on just how meaningful, clear, and conspicuous these notices are.

What we have found, however, are inconsistencies in how the opt out notice process is being implemented. Unfortunately, some affiliate information-sharing opt out disclosures are buried in the middle or near the end of a multi-page account agreement. For existing accounts, some institutions have been known to reduce the opt out disclosures to the fine print along with a long list of other required disclosures. Under these circumstances, few consumers will even notice the opt-out disclosures, let alone take the time to write the required opt-out letter.

On the other hand, I have seen evidence of responsible consumer notification and opportunity to opt out. In one case, the bank sent its customers a separate letter informing them of the benefits by way of greater product and service availability that resulted from the sharing of customer information among affiliates; but also providing a detachable form for its customers to use if they want to opt out. This type of simple, straightforward disclosure, and convenient approach for consumer opt out should be embraced by the banking industry.

The OCC is now working on developing guidance on effective practices for opt-out notices. As in the area of website disclosures, the PWG is meeting with and seeking input from the industry, privacy group representatives, and the FTC in identifying these effective practices. We are also discussing these issues with the other bank regulators. We expect to put out

[3]Specifically, the FCRA allows any company to share within its corporate family or to sell to third parties the company's "transaction and experience" information that it possesses on its own customers. 15 U.S.C. §1681a(d)(2)(a)(I) and (ii). Such sharing or selling does not trigger any notice or opt out requirements. If affiliated companies share any other type of information that would constitute a consumer report if sold outside the corporate family, the affiliate must give a consumer notice of the intent to share the information and an opportunity to opt out. Id. at §1681a(d)(2)(a)(iii).

guidance on opt-out notices sometime this Fall.

III. The Role of Regulators

In this emerging privacy area, the extent of actions taken by the OCC and other regulators will be significantly influenced by the success of the banking industry in adopting meaningful self-regulatory policies and in adhering to the limited laws that are now in place. Self-regulation clearly offers banks the ability to shape their own policies, rather than having a one-size-fits-all approach that could be mandated by law. To be meaningful, the OCC believes that self-regulation must respond to consumers' privacy concerns, provide adequate disclosures about privacy policies, accord consumers meaningful control over the use of the information they furnish, include reasonable steps to protect the security and integrity of that information, and offer some compliance assurance mechanisms.

Laudably, the major banking and thrift trade groups, ABA, ACB, TBR, CBA, and IBAA have endorsed a set of privacy principles adopted by the Banking Industry Technology Secretariat -- BITS -- of The Bankers Roundtable.[4] It is unclear, however, how many individual banks are

---

[4]In September 1997, the American Bankers Association (ABA), The Bankers Roundtable and its division, the Banking Industry Technology Secretariat ("BITS"), the Consumer Bankers Association (CBA), and the Independent Bankers Association of America (IBAA), endorsed a common set of privacy principles ("Banking Industry Principles"). America's Community Bankers (ACB) subsequently also endorsed the principles. These principles provide that subscribing financial institutions should:

(1) recognize a consumer's expectation of privacy by making available privacy guidelines and/or providing a series of questions and answers about financial privacy to their customers;

(2) only collect, retain and use individual customer information where it would be useful (and allowed by law) to administer that organization's business and to provide products, services and other opportunities to its customers;

(3) establish procedures to ensure customer information is accurate, current and complete in accordance with reasonable commercial standards, including responding to requests to correct inaccuracies in a timely manner;

(4) limit employee access to personally identifiable information to those with a business reason for knowing such information, educate employees so that they will understand the importance of confidentiality and customer privacy, and take appropriate disciplinary measures to enforce employee privacy responsibilities;

(5) maintain appropriate security standards and procedures regarding unauthorized access to customer information;

(6) not reveal specific information about customer accounts or other personally identifiable information to unaffiliated third parties for their independent use, except for the exchange of information with reputable information reporting agencies to maximize the accuracy and security of such information or in the performance of bona fide corporate due diligence, unless 1) the information is provided to help complete a customer-initiated transaction, 2) the customer requests it, 3) the disclosure is required by/or allowed by law (e.g., subpoena, investigation of fraudulent activity) or 4) the customer has been informed about the possibility of such disclosure for marketing or similar purposes through a prior communication and is given the opportunity to decline (i.e., "opt-out");

(7) if personally identifiable information is given to a third party, the financial institution should insist that the third party adhere to similar privacy principles that provide for keeping such information confidential;

(8) devise methods of providing a customer with an understanding of their privacy principles.

adopting and adhering to these principles. Failure to adopt more widespread self- regulatory measures may well result in the OCC's stepping up activities in this area.

With respect to the Fair Credit Reporting Act, as I have said, the OCC already has some initiatives underway. In addition to the guidance on effective opt-out notices, the OCC very shortly will be issuing an advisory to banks and bank examiners about the agency's ability to examine banks for compliance with FCRA. The 1996 amendments to the FCRA greatly expanded the duties of banks in the areas of data accuracy and privacy, as well as provided banks new opportunities for gathering and using information on their customers. At the same time, these amendments cut back on the ability of the bank regulators to examine institutions for compliance with the statute. The revised FCRA permits the bank regulators to examine institutions for FCRA compliance only in response to a complaint or if the agency "otherwise has knowledge" of a violation of the statute. 15 U.S.C §1681s (d). There is no other consumer protection statute that we enforce that similarly limits our ability to examine banks for compliance.

On this score, I should also note, however, that the OCC has recently reprogrammed its new customer assistance complaint database to specifically capture privacy-focused consumer complaints. This will provide us with a more meaningful way to assess and investigate consumers' concerns, and also should help us identify consumer complaints that may involve a violation of FCRA -- a trigger for our examination authority.

Conclusion

I will close by again commending the Chairman, Ranking Member LaFalce and this Committee for considering and addressing the issue of consumer privacy. We look forward to working with the Committee so that banks and other financial services providers meet the many challenges emerging in the consumer privacy arena.