



Comptroller of the Currency
Administrator of National Banks

Privacy Laws and Regulations

September 8, 2000

CONTENTS

PURPOSE AND SUMMARY	3
BACKGROUND	3
SUMMARY OF GLBA PRIVACY PROVISIONS AND OTHER LAWS	5
GLBA Privacy Provisions	5
Fair Credit Reporting Act	7
Electronic Fund Transfer Act	8
Right to Financial Privacy Act	8
Children's Online Privacy Protection Act	8
General Laws	9
COMPARISON OF GLBA AND FCRA PROVISIONS	10
SAFETY AND SOUNDNESS CONSIDERATIONS	12
CONTACT INFORMATION	13
NOTES	13

PURPOSE AND SUMMARY

This document is designed to assist national banks and their subsidiaries in complying with federal laws and regulations relating to the disclosure of consumer financial information. Accordingly, it summarizes the requirements of the relevant federal laws, particularly: Title V of the Gramm-Leach-Bliley Act (GLBA) (Pub. L. 106-102; 15 U.S.C. 6801 et seq.); the Fair Credit Reporting Act (FCRA) (15 U.S.C. 1681 et seq.); the Electronic Fund Transfer Act (EFTA) (15 U.S.C. 1693 et seq.); the Right to Financial Privacy Act (RFPA) (12 U.S.C. 3401 et seq.); and the Children's Online Privacy Protection Act (COPPA) (15 U.S.C. 6501 et seq.). Because the GLBA and the FCRA contain the most extensive requirements governing the disclosure of consumer information by banks and other private entities, this document discusses the relationship between these laws to help banks better understand the scope of their obligations under each statute.

BACKGROUND

The GLBA, signed into law on November 12, 1999, enacted new privacy-related provisions applicable to financial institutions and authorized the federal financial institution regulatory agencies (Agencies) to adopt regulations to implement those new provisions and the pre-existing provisions of the FCRA.¹ The financial institutions covered by the GLBA include national banks and their financial and operating subsidiaries, as well as a wide range of other businesses engaged in financial and financially-related activities. For ease of reference, this document frequently refers to relevant legal requirements (under the GLBA, the FCRA, or other laws) as being applicable to "banks;" as a general matter, these requirements also will be applicable to national banks' financial and operating subsidiaries.

The Agencies recently promulgated final rules to implement the GLBA provisions. The GLBA requirements will become effective on November 13, 2000, and compliance with these requirements is mandatory as of July 1, 2001. To be in compliance with the regulations, prior to July 1, 2001, banks must have delivered copies of their privacy policies to their customers, and, as appropriate, provided them with a reasonable opportunity to opt out of certain information sharing arrangements between the bank and nonaffiliated third parties before such information sharing occurs. Senior management and the boards of directors of national banks and their subsidiaries are strongly encouraged to ensure that their institutions take all appropriate steps before this mandatory compliance date so that they are prepared to

comply fully with the GLBA regulations at that time. These steps should include, as appropriate for the institution:

- conducting an inventory of information collection and disclosure practices;
- evaluating agreements with third parties that involve the disclosure of consumer information;
- establishing mechanisms to handle opt-out elections by consumers;
- developing or revising existing privacy policies to reflect the new regulatory requirements;
- determining how to deliver privacy notices to consumers;
- establishing employee training and compliance programs; and
- setting target dates for all features of the implementation program.

While the GLBA is the most extensive of the federal financial privacy laws, there are a number of other statutes that bear upon the information sharing practices of national banks and their subsidiaries, most notably the FCRA. These other laws are currently in full effect, and national banks and their subsidiaries are expected to be in compliance with them and any applicable state privacy laws.

SUMMARY OF GLBA PRIVACY PROVISIONS AND OTHER LAWS

GLBA Privacy Provisions

Principal Privacy Requirements in the GLBA

The three principal requirements relating to the privacy of consumer financial information in the GLBA are:

- Financial institutions must provide their customers with notices describing their privacy policies and practices, including their policies with respect to the disclosure of nonpublic personal information² to their affiliates and to nonaffiliated third parties. The notices must be provided at the time the customer relationship is established and annually thereafter.
- Subject to specified exceptions, financial institutions may not disclose nonpublic personal information about consumers to any nonaffiliated third party unless consumers are given a reasonable opportunity to direct that such information not be shared (to "opt out").
- Financial institutions generally may not disclose customer account numbers to any nonaffiliated third party for marketing purposes.

Privacy Notices. Under the GLBA, a bank must provide a notice that accurately describes its privacy policies and practices to individual consumers who establish a customer relationship with the bank, not later than the time the customer relationship is established. Unless an exception applies, this initial privacy notice also must be provided to any other consumer, even if not a "customer" of the bank, before the bank discloses that consumer's nonpublic personal information to a nonaffiliated third party. Banks also must provide their customers an annual privacy notice. All privacy notices must be clear and conspicuous, and must be provided so that each intended recipient can reasonably be expected to receive actual notice. Notices must be in writing (unless the consumer agrees to electronic delivery). The notices must describe, among other things, the types of nonpublic personal information collected and disclosed, the types of affiliated and nonaffiliated third parties with whom the information may be shared, and the consumer's right to opt out and thereby limit certain information sharing by the bank.

Opt-Out Requirements. Banks generally may not, directly or through an affiliate, disclose a consumer's nonpublic personal information to any nonaffiliated third party unless the consumer is given a reasonable opportunity to direct that such information not be disclosed, i.e., to opt out. Thus, before a bank may disclose nonpublic personal information about a consumer to a nonaffiliated third party, the bank must provide the consumer with an initial privacy notice and an opt-out notice (which may be included in the privacy notice). The GLBA contains a number of specific exceptions to these opt-out requirements, however, to ensure that banks can continue to disclose information to nonaffiliated third parties to conduct routine business. These exceptions include, for instance, the disclosure of information by banks to third parties who are providing services to the bank or to their customers as the bank's agent.

Other Restrictions. The GLBA also provides that a bank generally may not disclose an account number or similar form of access number or access code for a credit card account, deposit account, or transaction account of a consumer to any nonaffiliated third party for use in telemarketing, direct mail, or other marketing through electronic mail to the consumer. The statute also limits the redisclosure or reuse of information obtained from other nonaffiliated financial institutions.

Fair Credit Reporting Act

Principal FCRA Information Sharing Provisions

The FCRA sets standards for the collection, communication, and use of information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living. The communication of this type of information may be a "consumer report" subject to the FCRA's requirements. The definition of consumer report contains a number of exceptions, however, including exceptions that permit a bank:

- To share with any other party information solely as to the bank's transactions or experiences with a consumer; and
- To share with bank affiliates other types of information, such as information from a credit report or from a consumer's loan application, if it is clearly and conspicuously disclosed to the consumer that such information sharing may occur, and the consumer is given an opportunity to direct that the information not be shared, i.e., to "opt out."

Banks that share consumer report information among affiliates or with third parties under other circumstances may become consumer reporting agencies subject to the FCRA's requirements applicable to those entities. These requirements relate to furnishing consumer reports only for permissible purposes, maintaining high standards for ensuring the accuracy of information in consumer reports, resolving customer disputes, and other matters.

As a general matter, a bank will not be subject to the FCRA's substantial requirements that apply to consumer reporting agencies if the bank communicates only transaction or experience information to third parties or among its affiliates. Additionally, a bank will not become a consumer reporting agency if it shares with its affiliates other information that would ordinarily be considered consumer report information if it does so in accordance with the consumer opt-out process noted above.

The FCRA does, however, impose a number of requirements on persons that use consumer reports or furnish information to consumer reporting agencies, and these provisions can apply to national banks and their subsidiaries.³ Several of these provisions protect the privacy of consumer information, including one that requires a bank to use or obtain consumer reports only for specific permissible purposes under

the statute. Another provision requires a bank that solicits consumers for offers of credit based on information in consumer reports ("prescreened offers") to provide a clear and conspicuous notice with each offer informing consumers, among other things, how they can opt out of further solicitations.

Electronic Fund Transfer Act

The EFTA and the Federal Reserve Board's Regulation E (12 C.F.R. Part 205) require that banks make certain disclosures at the time a consumer contracts for an electronic fund transfer service or before the first electronic fund transfer is made involving the consumer's account. For example, the financial institution must disclose the circumstances under which, in the ordinary course of business, the financial institution may provide information concerning the consumer's account to third parties, whether or not the third party is affiliated with the bank. This disclosure must encompass any information that may be provided concerning the account (not just information relating to the electronic fund transfers themselves). The EFTA and Regulation E requirements apply with respect to demand deposit, savings deposit, and other consumer asset accounts.

The OCC will treat an initial privacy notice that satisfies the GLBA regulations as sufficient for compliance with the EFTA and Regulation E.

Right to Financial Privacy Act

The RFPA prohibits financial institutions from disclosing a customer's financial records to the federal government except in limited circumstances such as pursuant to the customer's authorization, an administrative subpoena or summons, a search warrant, a judicial subpoena, or a formal written request in connection with a legitimate law enforcement inquiry, or to a supervisory agency in connection with its supervisory, regulatory, or monetary functions.

Children's Online Privacy Protection Act

The COPPA and the Federal Trade Commission's implementing regulations (16 C.F.R. Part 312) generally apply to financial institutions that operate commercial web sites or online services (or portions thereof) that are directed to children, or that

operate web sites or online services and knowingly collect personal information from children under the age of 13.⁴

COPPA and the FTC's regulations establish a number of requirements applicable to operators of covered web sites and online services, including requirements that the operator must provide online notice about its information practices with respect to children. With limited exceptions, the operator also must obtain verifiable parental consent prior to any collection, use, or disclosure of personal information from children. The operator also must provide a reasonable means for a parent to review the personal information collected from a child and to refuse to permit its further use or maintenance. Operators also are prohibited from conditioning a child's participation in a game, the offering of a prize, or any other activity upon the child's disclosing more personal information than is reasonably necessary to participate in such activity. Finally, operators must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

General Laws

National banks and their subsidiaries also should be aware of other federal and state laws that may affect their practices relating to consumer financial information. For example, on the federal level, the Federal Trade Commission Act (15 U.S.C. 41 et seq.) prohibits unfair or deceptive acts or practices in or affecting commerce, and provides a basis for government enforcement actions against deception resulting from misleading statements concerning a company's privacy practices or policies, or failures to abide by a stated policy. A number of states have enacted privacy laws that specifically relate to the disclosure of consumer financial information, as well as laws that more generally target unfair and deceptive acts and practices. The GLBA maintains that state laws that afford greater protection for consumer privacy than that provided by the GLBA are not preempted by Title V of the GLBA. The FCRA, however, provides that state laws that prohibit or impose requirements on the exchange of information among affiliates are preempted unless enacted after January 1, 2004.

COMPARISON OF GLBA AND FCRA DISCLOSURE PROVISIONS

Types of Information Covered

GLBA applies to "nonpublic personal information" which is broadly defined by regulation to cover any information that is provided to a bank by a consumer to obtain a financial product or service, that results from a transaction with a bank involving a financial product or service, or that is otherwise obtained by a bank in connection with providing a financial product or service to a consumer. In some circumstances, "publicly available" information is also considered "nonpublic personal information."

FCRA more narrowly applies to the disclosure of "consumer reports," which contain information on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living.

Types of Disclosures Covered

GLBA restricts disclosures to nonaffiliated third parties.

FCRA, more broadly, restricts disclosures to both affiliates and nonaffiliated third parties.

Types of Restrictions on Information Disclosures

GLBA prohibits a bank from disclosing nonpublic personal information to nonaffiliated third parties unless the bank has provided consumers with a privacy notice and an opportunity to opt out of such information sharing.

FCRA provides that a bank may become a consumer reporting agency if it discloses consumer report information to its affiliates without providing consumers notice of the disclosure and an opportunity to opt out. Additionally, a bank may become a consumer reporting agency if it discloses consumer reports to nonaffiliated third parties. There is no notice and opt-out provision that would permit a bank to share consumer reports with nonaffiliated third parties without becoming a consumer reporting agency.

Scope of Consumer's Opt-Out Right

GLBA opt-out permits consumers to limit a bank's sharing nonpublic personal information with nonaffiliated third parties.

FCRA opt-out permits consumers to limit a bank's sharing information that would otherwise be a "consumer report" with affiliates.

Scope of Exceptions

GLBA contains a number of specific exceptions to the consumer's opt-out right.

FCRA explicitly permits banks to share freely only information relating solely to transactions or experiences between the bank and the consumer.

It is critical that national banks remain cognizant of the differences between the GLBA and the FCRA provisions to reduce compliance risks in this area. The GLBA and the FCRA both govern the disclosure of consumer information by banks and other entities. The statutes, however, differ in the scope of their coverage, as well as in their requirements with respect to a bank's treatment of consumer information. As a result, what may be a permissible disclosure under one statute may be prohibited or subject to different conditions under the other statute. Because compliance with one statute will not entail compliance with the other, banks are therefore strongly advised to evaluate the requirements of both laws in connection with their disclosures of consumer information.

In certain respects, each statute is broader in scope than the other. For example, while the FCRA restricts only the disclosure of "consumer report" information (information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living that is used or expected to be used or collected for certain specified purposes), the GLBA applies to all personally identifiable financial information of a consumer that is not publicly available, including information about the bank's transactions and experiences with the consumer, and even the fact that the bank has a relationship with the consumer. As a result, although a bank could disclose information about its transactions and experiences with its consumers to nonaffiliated third parties under the FCRA without condition, such a disclosure would trigger notice and opt-out requirements under the GLBA (subject to specific exceptions, such as reporting to credit bureaus in accordance with the FCRA).

On the other hand, the GLBA is narrower than the FCRA to the extent that it restricts the disclosure of information only to nonaffiliated third parties. By contrast, if information is consumer report information, the FCRA restricts its disclosure both to nonaffiliated third parties and to affiliates. Thus, while the GLBA may permit a bank to disclose consumer report information to nonaffiliated third parties in accordance with the notice and opt-out requirements, such a disclosure could turn a bank into a consumer reporting agency under the FCRA, triggering numerous statutory obligations.

The consumer's opt-out right also functions differently under the two statutes. Under the GLBA, a bank is prohibited, subject to specific exceptions, from sharing information with nonaffiliated third parties unless the bank has provided consumers with a privacy notice and an opportunity to opt out of the information sharing. If the consumer does not opt out, a bank may share information with nonaffiliated third parties. Additionally, if a consumer opts out of third-party sharing, a bank may

nonetheless share such information with affiliates because the GLBA does not provide consumers with an option to limit a bank's sharing of information with the bank's affiliates.

Under the FCRA, a bank may share consumer report information with its affiliates if it provides consumers with a notice about the intended disclosure and an opportunity for consumers to opt out of the information sharing. Unlike the GLBA, a bank is not prohibited from making such disclosures without providing notice and opt-out. Rather, failure to provide a notice and opt-out may turn a bank into a consumer reporting agency. With respect to nonaffiliated third parties, the FCRA provides no similar opportunity for banks to disclose consumer report information without becoming a consumer reporting agency. There is no option to provide consumers with a notice and opt-out. Accordingly, if a bank shares consumer reports with nonaffiliated third parties the bank may become a consumer reporting agency.

Finally, while the FCRA contains no significant explicit exceptions to the notice and opt-out rights other than that for transaction or experience information, the GLBA sets forth a number of specific exceptions to its general restrictions on information disclosure, including exceptions for sharing information with service providers and joint marketers, for disclosures necessary to process or service transactions, and for a variety of other circumstances. It should be noted, however, that although the GLBA has many more exceptions, the transaction or experience information that is not covered by the FCRA is subject to the GLBA restrictions.

SAFETY AND SOUNDNESS CONSIDERATIONS

In addition to legal and compliance risks associated with the handling of consumer information, a failure to respect customers' expectations of privacy could severely damage a bank's customer relationships and its overall reputation. Thus, it is critical for the boards of directors and senior management of national banks and their subsidiaries -- in consultation with legal counsel, where appropriate -- to establish policies and procedures to meet legal requirements and otherwise control these risks.

CONTACT INFORMATION

For further information about the matters discussed in this document, contact Amy Friend, Assistant Chief Counsel (202-874-5200), Michael S. Bylsma, Director, Community and Consumer Law Division (202-874-5750), or Stephen Van Meter, Senior Attorney, Community and Consumer Law Division (202-874-5750).

NOTES

¹Before passage of the GLBA, no agency had rulemaking authority with respect to the FCRA. The OCC is currently working with the other Agencies in drafting proposed FCRA regulations.

²Generally, this means any information that is provided by a consumer to a bank in order to obtain a financial product or service, that results from a transaction between a bank and a consumer involving a financial product or service, or that is otherwise obtained by a bank in connection with providing a financial product or service to the consumer. If a bank obtains information about its consumers from a publicly available source, that information will not be protected (i.e., subject to notice and opt-out) unless the information is disclosed as part of a list, description, or other grouping of a bank's consumers.

³Among the more important requirements that banks should be mindful of are the following:

Consumer Reports only for Permissible Purposes. A bank may not use or obtain a consumer report for any purpose unless the report is obtained for a permissible purpose under the FCRA and the purpose is certified by the user to the consumer reporting agency through a general or specific certification.

Special Requirements for Employment Purposes. A bank must follow special procedures when obtaining a consumer report for employment purposes and when taking adverse action, in whole or in part on the basis of a consumer report, in connection with a consumer's employment.

Special Requirements for Investigative Reports. A bank must meet particular requirements to obtain an "investigative consumer report."

Requirements When Adverse Action is Taken. A bank that takes adverse action based on information in a consumer report (or, in certain circumstances, based on information obtained from affiliates or from third parties) must provide certain notices to the consumer relating to the nature of the adverse action and the basis of the decision.

Prescreened Transactions. A bank that uses consumer reports in connection with credit or insurance transactions not initiated by the consumer must provide certain clear and conspicuous notices relating to the consumer's right to opt out of such solicitations.

Duties of Furnishers of Information. A bank that furnishes information to consumer reporting agencies has particular duties relating to the completeness and accuracy of the information provided, including duties to investigate consumer disputes.

⁴National banks are expected to comply with the regulations that the FTC issues under COPPA in accordance with 15 U.S.C. 6502(b). The OCC is authorized to enforce these regulations with respect to national banks under section 8 of the Federal Deposit Insurance Act as set forth in 15 U.S.C. 6505(b)(1)(A).