NEW YORK LAW SCHOOL

NYLS Journal of Human Rights

Volume 17 | Issue 1 Article 8

2000

# The New Consumer Financial Privacy Regulations: Balancing the Interests of Consumers and Industry

Dolores S. Smith

James H. Mann

# The New Consumer Financial Privacy Regulations: Balancing the Interests of Consumers and Industry

*Dolores S. Smith & James H. Mann*[1]

President Clinton signed the Gramm-Leach-Bliley Act ("GLBA") into law on November 12, 1999.[2] The GLBA contains many provisions relating to privacy issues. For example, it directs the Federal Reserve Board ("Board") and the other Federal bank and thrift regulators to issue joint regulations implementing the Fair Credit Reporting Act ("FCRA"), as well as standards for the security of customer data held by financial institutions.[3] Other provisions are aimed at combating pretext calling, which involves the fraudulent acquisition of customer information from financial institutions or even from customers themselves.[4]

Subtitle A of Title V of the GLBA governs consumer financial privacy.[5] Section 504 directs eight agencies, including the Board, to issue implementing regulations that are consistent "to the extent possible."[6] The Board issued regulations on June 1, 2000 that are substantively identical to the regulations of the other Federal bank and thrift regulators.[7]

The regulations seek to strike a balance between the interests of consumers and of industry.[8] Consumers' interests, broadly

---

[1] Ms. Smith is Director of the Division of Consumer and Community Affairs of the Board of Governors of the Federal Reserve System ("Board"). Mr. Mann is a Senior Attorney in the Division. The views they express in this article are not necessarily those of the Board.

[2] *See* Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (1999).

[3] *Id.* at §§ 501, 506.

[4] *Id.* at § 521.

[5] *Id.* at §§ 501–510.

[6] *See id.* The agencies include the Board, the Department of the Treasury, the Federal Deposit Insurance Corporation, the Federal Trade Commission ("FTC"), the National Credit Union Administration, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, and the Securities and Exchange Commission.

[7] *See* 65 Fed. Reg. 35,162 (June 1, 2000) (codified at 12 C.F.R. pts. 40, 216, 332, and 573).

[8] *See Privacy Issue Could Further Complicate Banking Reform*, CONG. DAILY, April 30, 1999, available at 1999 WL 5951334 (stating that consumers' goal of financial privacy conflicted with industry's goal of sharing clients' information).

speaking, include controlling data about themselves and being informed about financial institutions' privacy policies and practices. Financial institutions' interests, speaking equally broadly, include minimizing the cost of affording consumers this control and information. The regulations seek to optimize these interests.

Several factors reinforced this effort, including the extremely vigorous and diverse public response to the agencies' request for comment on their proposed regulations.[9] For example, the Board alone received more than 2,000 comments.[10] These included more than 1,400 comments from individuals — an unusual level of participation from an industry sector, reflecting not only widespread public awareness of privacy issues, but also public knowledge about the agency rulemaking process.

This article gives a brief overview of the regulations, and then discusses several provisions that exemplify the balance they strike. The article also identifies a few provisions that elevate consumer interests over industry interests.

## I. OVERVIEW OF THE REGULATIONS

The regulations establish certain duties on the part of financial institutions toward "consumers" and "customers" regarding the disclosure of nonpublic personal information to nonaffiliated third parties.[11] (The Fair Credit Reporting Act governs the sharing of consumer information among affiliates.) For purposes of the regulations, the term "financial institution" generally includes any institution whose business is engaging in activities that the Bank Holding Company Act treats as financial in nature, or as incidental to those activities.[12] Although the GLBA mandates a few limited exceptions, "financial institution" includes not only banks and thrifts, but also a potentially broad range of other entities.

---

[9] *See id.*

[10] *See, e.g., id.*

[11] *Id.*

[12] *See* 12 C.F.R. § 216.3 (b).

A "consumer" is an individual who obtains or has obtained a financial product or service from a financial institution for personal, family, or household purposes.[13] A "customer" is a consumer who has a "customer relationship" with a financial institution, defined as a continuing relationship under which the institution provides financial products or services to the consumer.[14]

"Nonpublic personal information" generally includes personally identifiable financial information, as well as any list of consumers derived using that information. "Personally identifiable financial information" includes any information that a financial institution obtains about a consumer in connection with providing the consumer with a financial product or service.[15]

"Nonpublic personal information" generally does not include information, from specified sources such as government records, that a financial institution has a reasonable basis to believe is lawfully available to the general public.[16]

A "nonaffiliated third party" generally includes any person other than a financial institution's affiliate. An "affiliate" of a financial institution is any company that controls, is controlled by, or is under common control with the financial institution.[17]

Turning to the duties imposed by the regulations: first, a financial institution must not disclose nonpublic personal information about a consumer to a nonaffiliated third party, other than as authorized by the statute, unless (1) the financial institution has provided the consumer with an initial notice about the institution's privacy policies and practices and with an opt out notice; (2) the financial institution has given the consumer a reasonable opportunity, before the financial institution discloses information to a nonaffiliated third party, to opt out; and (3) the consumer has not opted out.

The initial notice must be clear and conspicuous, and must accurately reflect the financial institution's privacy policies and

---

[13] *See* 12 C.F.R. § 216.3 (e).
[14] *Id.* at § 216.3 (h).
[15] *Id.* at § 216.3 (n), (o), (p).
[16] *Id.*
[17] *Id.* at § 216.3 (a).

practices. The opt out notice must also be clear and conspicuous, must accurately explain the consumer's right to opt out, and must provide (or be accompanied by) a reasonable means for doing so. To "opt out" means to foreclose a financial institution's disclosure of nonpublic personal information about a consumer to a nonaffiliated third party.[18] What constitutes a reasonable opportunity to opt out depends on the circumstances of the consumer's transaction; the regulations offer examples.[19]

The act and regulations allow some exceptions. A financial institution may disclose nonpublic personal information, under certain circumstances, to a nonaffiliated third party that is performing services for the financial institution; or as necessary to effect, administer, or enforce a transaction that a consumer requests or authorizes (section 14 exceptions); or, in certain other instances involving, for example, the financial institution's attorneys, accountants, and auditors (section 15 exceptions).[20]

Second, if a financial institution intends to disclose nonpublic personal information about a consumer to a nonaffiliated third party, and the disclosure was not described in the initial notice that the institution provided to the consumer, the financial institution may not make the disclosure unless: (1) it furnishes an accurate revised notice, as well as a new opt out notice; (2) the financial institution again gives the consumer a reasonable opportunity, before the institution discloses information to the nonaffiliated third party, to opt out; and (3) the consumer does not opt out. This duty is subject to the same exceptions as the duty described above.

Third, if a financial institution receives nonpublic personal information from a nonaffiliated financial institution under a section 14 or 15 exception, the recipient's disclosure and use of the information is limited in various ways, as discussed below.[21]

Fourth, if the financial institution receives nonpublic personal information from a nonaffiliated financial institution on another basis,

---

[18] *See* 12 C.F.R. § 216.7.

[19] *Id.* at § 216.1.

[20] *Id.* at §§ 216.14, 216.15.

[21] *Id.* at § 216.1.

the recipient's disclosure of the information is subject to certain limitations — although its use of the information is unlimited.[22]

Fifth, a financial institution generally must not disclose the number of a consumer's credit card account, deposit account, or transaction account to any nonaffiliated third party (other than a consumer reporting agency) for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer. The regulations create some limited exceptions.[23]

Sixth, a financial institution must provide an initial notice about its privacy policies, in most cases not later than the time when the financial institution establishes a customer relationship.[24] The regulations permit subsequent notice in a few cases.

Seventh, a financial institution must provide (not less than annually) a clear and conspicuous notice to customers that accurately reflects its privacy policies and practices during the continuation of the customer relationship.[25]

And eighth, when an existing customer obtains a new financial product or service from a financial institution for personal, family, or household purposes, and the most recent notice provided to the customer does not reflect the institution's practices, the financial institution must provide a revised notice that covers the new product or service.[26]

---

[22] *Id.*

[23] 12 C.F.R. § 216.12.

[24] *See* Privacy of Consumer Financial Information, 12 C.F.R. § 216.4 (2000).

[25] *Id.* at § 216.5.

[26] *Id.* at § 216.4. Several general principles apply to the delivery of notices. For example, a financial institution must deliver notices so that the consumer can reasonably be expected to receive actual notice in writing or, if the consumer agrees, electronically. Also, for customers only, a financial institution must provide the initial notice, the annual notice, and the revised notice so that the customer can retain them or obtain them later in writing, or, if the customer agrees, electronically.

## II. BALANCING THE INTERESTS OF CONSUMERS AND INSTITUTIONS

The overall structure of the regulations warrants a brief comment. The regulations generally present broadly couched rules, and then illustrate with several non-exclusive examples. For instance, the regulations mandate that under certain circumstances a financial institution must provide a consumer with a "reasonable means" by which the consumer can exercise the opt out right. The regulations offer several examples of reasonable means, but do not restrict a financial institution to the examples given. The regulations also describe means not considered reasonable. Thus, the general rule protects the consumer by requiring the provision of a reasonable opt out means, while the non-exclusivity of the examples permits financial institutions to use other ways that may work better for them. This structure, accommodating the interests of both consumers and industry, recurs often in the regulations.[27]

## III. "CONSUMERS" AND "CUSTOMERS"

The regulations generally give rights to two classes of individuals: consumers whose data a financial institution plans to disclose, and consumers with whom the financial institution has a continuing relationship — that is, "customers." Consumers who are not "customers," and whose data the financial institution does not plan to disclose, generally have no rights under the regulations.[28] Financial institutions, correspondingly, bear no duties to those individuals, and thus, generally will experience compliance costs only with respect to consumers from whom they might anticipate a revenue stream — through a customer relationship, through the sale of data, or both. Similarly, consumers not receiving privacy notices from a financial institution are those who could have no practical interest in them. No data of these consumers are being disclosed, nor are these

---

[27] *See* 12 C.F.R. § 216 (2000).

[28] *Id.* at § 216.4 (b).

consumers entering into, or participating in, a continuing relationship with the institution.[29]

## IV. DEFINITION OF "PERSONALLY IDENTIFIABLE FINANCIAL INFORMATION"

The regulations define the statutory term "personally identifiable financial information" broadly — to embrace, substantially all the information that a financial institution obtains about a consumer in connection with providing a financial product or service.[30] The information need not be intrinsically financial. For example, if an institution obtains a consumer's e-mail address in connection with providing the consumer a financial product or service, the address would be "personally identifiable financial information." Similarly, a consumer's date of birth is personally identifiable financial information if an institution learns it from the consumer's application for a financial product or service.[31]

The breadth of this definition benefits consumers by bringing a large volume and variety of information within the protection of the regulations. Returning to the example of the e-mail address, the financial institution generally could not disclose the address to a nonaffiliated third party, outside of the exceptions, unless the institution provided the consumer with notice and an opportunity to opt out. The broad definition correspondingly expands the range of information with respect to which financial institutions have duties toward consumers. At the same time, however, the breadth and simplicity of the definition should reduce the compliance burden. Institutions need not puzzle over whether any individual item of the consumer data they hold is personally identifiable financial information; they can simply assume that it is.

---

[29] *Id.*

[30] *See* 12 C.F.R. § 216.3(o) (2000).

[31] *See id.*

## V. CONTENT OF THE PRIVACY NOTICE

The regulations require that privacy notices address a broad range of topics.[32] These include, among others (as applicable to the particular financial institution), the nonpublic personal information the institution collects; information the institution discloses; which affiliates and nonaffiliated third parties receive the information; the nonpublic personal information the institution discloses about former customers, and to whom; and how the institution safeguards the nonpublic personal information it possesses. At the same time, the regulations promote concise notices, which consumers are more apt to absorb.[33] (Indeed, examples and sample clauses clarify that the privacy notice need not be lengthy.) Institutions are to describe the information they collect and disclose, and the affiliates and third parties who receive it, by category. Appropriate examples are required in some cases, but the regulations clarify that the examples need only be "a few." Institutions that reserve the right to disclose all the nonpublic personal information that they collect about consumers, may simply say so in their notice, without categorizing or providing examples of the information disclosed. Institutions may provide an abbreviated notice if they do not disclose, and do not reserve the right to disclose, nonpublic personal information other than as permitted by the section 14 or 15 exceptions — such as, to carry out a transaction requested by a consumer, or to comply with the anti-money laundering laws. Institutions providing opt out notices to non-customers need not attach the full privacy notices; instead, they may simply inform consumers of how to obtain them.

In addition, the preamble to the regulations presents an informal compliance guide for institutions that do not have affiliates and do not disclose or reserve the right to disclose nonpublic personal information to nonaffiliated third parties other than in accordance with the section 14 and 15 exceptions.[34] The compliance guide

---

[32] 12 C.F.R. § 216.6.

[33] *Id.*

[34] Privacy of Consumer Financial Information, 65 Fed. Reg. 33,646 (2000) (preamble).

briefly explains how these institutions can satisfy the regulations' requirements regarding the content, timing, and delivery of initial and annual notices to customers.[35] The guide also gives an example of a notice that would comply.[36]

## VI. DISCLOSURE OF ACCOUNT NUMBERS

One provision of the statute flatly bars financial institutions from sharing with nonaffiliated third parties (other than consumer reporting agencies) the numbers of certain types of consumer accounts. However, the statute also authorizes the agencies to create exceptions to this provision.

The agencies concluded that certain exceptions would benefit both consumers and financial institutions, by allowing the continuation of existing business practices that do not pose a substantial risk of third parties' making unauthorized charges to consumers' accounts. Thus, for example, the regulations permit institutions, under certain circumstances, to disclose consumer account numbers to "mail houses" that send out billing statements, along with materials that promote the institutions' products — so long as the mail houses are not permitted to directly initiate charges to consumers' accounts. Similarly, the regulations permit institutions to disclose consumer account numbers to their clients in "private label" or "affinity" credit card programs, so long as consumers are aware, when entering into the program, that the program involves, not only the client, but also the institution.[37]

## VII. COMPLIANCE DATE

The statute provides that agency regulations will take effect a year after enactment — November 13, 2000 — unless the agencies specify a later date. Consumers have an interest in receiving the

[35] *Id.* (preamble).
[36] *Id.* (preamble).
[37] 12 C.F.R. § 216.12.

protections afforded by the regulations at an early date. Financial institutions have an interest in establishing the necessary systems and procedures in a methodical fashion, developing and testing them appropriately, and avoiding year-end mailings when they may already be sending other notices to consumers. In their comment letters, many institutions asked that the effective date be extended by one to two years.

The regulations delay the date for full compliance from November 13, 2000, to July 1, 2001.[38] The agencies judged that this would give financial institutions time to put their policies and systems in place, without excessively delaying the applicability of the consumer protections that the law provides.

## VIII. PRO-CONSUMER PROVISIONS

A few provisions of the regulations favor the interests of consumers over those of financial institutions, in keeping with the statute.

### *A. The Consent Exception*

The statute provides that the consumer's right to opt out does not apply to disclosures of nonpublic personal information made "with the consent or at the direction of the consumer."[39] The agencies could have interpreted consent to include a consumer's execution of an account agreement that includes a broad boilerplate consent. Such an interpretation, arguably, would have undermined the opt out right conferred by the statute, and made largely superfluous the other statutory exceptions to that right.

While not expressly precluding this reading of the statute, the regulations expressly endorse an interpretation that is much narrower, giving the following as an example: "A consumer may specifically consent to [the institution's] disclosure to a nonaffiliated insurance

---

[38] *Id.* § 216.18.

[39] Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, § 502 (e) (2), 113 Stat. 1338 (1999).

company of the fact that the consumer has applied to [the institution] for a mortgage so that the insurance company can offer homeowner's insurance to the consumer."[40]

*B. Limitations on Re-use*

The statute does not expressly limit the re-use of nonpublic personal information by institutions that receive it.[41] Omitting such limits from the regulations would, therefore, have been consistent with the statutory language.[42] The agencies recognized, however, that the practical result would have been to permit institutions to circumvent consumers' exercise of their statutory rights.[43] For example, a consumer might opt out from an institution's disclosure of data to a nonaffiliated third party for marketing purposes. But assume that, without giving the consumer the right to opt out, the institution lawfully disclosed the same data to the same party for a non-marketing purpose covered by a statutory exception — such as "to protect against . . . actual or potential fraud."[44] Absent a limitation, the party receiving the data for this purpose could then re-use the data for marketing. The agencies, considering this and similar scenarios, concluded that limitations on re-use were compelled by the statute, even though not expressly required. The regulations, therefore, include such limitations, blocking a route to circumvention of the statute.

---

[40] 12 C.F.R. § 216.15 (b) (1).

[41] Privacy of Consumer Financial Information, 65 Fed. Reg, at 33,667 (to be codified as 16 CFR 313.15 (b) (1)) (stating, ". . . section 502(c) expressly addresses only redisclosures and not re-use").

[42] *Id.* (stating "[a] few [commentators] opined that the Commission would exceed its rulemaking authority if the final rule were to retain limits on re-use of information").

[43] *Id.* (stating "[I]t would be inappropriate to undermine the key privacy requirements of the Act that ensure a consumer can generally control the disclosure of his or her nonpublic personal information by allowing the recipient of nonpublic personal information under the section 502(e) exception to re-use the information for any purpose, including marketing").

[44] 12 C.F.R. § 216.15 (a) (3).

## CONCLUSION

This article describes only one part of a broader, ongoing process. Consumer and industry interests regarding privacy matters must be balanced not only in agency rulemaking, but also by firms, as they develop their privacy policies, and by the Congress and state legislatures, as they consider additional privacy legislation. Indeed, to some extent these balancing efforts are interactive — for example, certain industry efforts might reduce the likelihood of legislation.[45]

Moreover, the regulators will be making many further attempts to balance consumer and industry interests — in connection with examination procedures implementing the consumer financial privacy regulations, with data-security standards, and with regulations under the FCRA. Thus, the process described in this article will be played out over the coming years in many other contexts. The results cannot now be predicted.

---

[45] *See Oversight Hearing on Electronic Communications Privacy Policy Disclosures Before The Subcommittee On Courts And Intellectual Property Committee On The Judiciary, U.S. House Of Representatives*, 106th Cong. (2000) (statement of Marc Rotenberg, Director, Electronic Privacy Information Center).