Privacy of Consumer Financial Information

Background and Overview

Title V, Subtitle A of the Gramm-Leach-Bliley Act (“GLBA”) governs the treatment of nonpublic personal information about consumers by financial institutions. Section 502 of the Subtitle, subject to certain exceptions, prohibits a financial institution from disclosing nonpublic personal information about a consumer to nonaffiliated third parties, unless the institution satisfies various notice and opt-out requirements, and provided that the consumer has not elected to opt out of the disclosure. Section 503 requires the institution to provide notice of its privacy policies and practices to its customers. Section 504 authorizes the issuance of regulations to implement these provisions.

In 2000, the four federal banking agencies and the National Credit Union Administration (“NCUA”) published regulations implementing provisions of the GLBA governing the treatment of nonpublic personal information about consumers by financial institutions. The regulations establish rules governing duties of a financial institution to provide particular notices and limitations on its disclosure of nonpublic personal information, as summarized below.

The Dodd-Frank Act granted rule-making authority under Sections 502 through 509 of the Gramm-Leach-Bliley Act (15 USC 6802-6809) to the Consumer Financial Protection Bureau (CFPB) and, with respect to entities under its jurisdiction, granted authority to the CFPB to supervise for and enforce compliance with these statutory provisions and their implementing regulations.

The regulations establish rules governing duties of a financial institution to provide particular notices and limitations on its disclosure of nonpublic personal information as summarized below.

- A financial institution must provide a notice of its privacy policies and allow the consumer to opt out of the disclosure of the consumer’s nonpublic personal information to a nonaffiliated third party if the disclosure is outside of the exceptions in Sections 13, 14 or 15 of the regulations.
- Regardless of whether a financial institution shares nonpublic personal information, the institution must provide notices of its privacy policies to its customers.
- A financial institution generally may not disclose customer account numbers to any nonaffiliated third party for marketing purposes.
- A financial institution must follow reuse and redisclosure limitations on any nonpublic personal information it receives from a nonaffiliated financial institution.

---

1 The NCUA published its final rule in the Federal Register on May 18, 2000 (65 FR 31722). The Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision jointly published their final rules on June 1, 2000 (65 FR 35162). For ease of reference, only the Federal Reserve’s implementing regulation is cited in this narrative. However, examiners should review an entity’s compliance with the applicable regulations in effect with respect to that entity.

2 Dodd-Frank Act §§ 1002(12)(J), 1024(b)-(c), and 1025(b)-(c); 12 USC §§ 5481(12)(J), 5514(b)-(c), and 5515(b)-(c). Under Sec. 1002(12)(J), the Dodd-Frank Act excepted from CFPB authority Sec. 505 as it applies to Sec. 501(b) – related to financial institution security safeguards.
Examination Objectives

- To assess the quality of a financial institution’s compliance management policies and procedures for implementing the privacy regulation, specifically ensuring consistency between what the financial institution tells consumers in its notices about its policies and practices and what it actually does.

- To determine the reliance that can be placed on a financial institution’s internal controls and procedures for monitoring the institution’s compliance with the privacy regulation.

- To determine a financial institution’s compliance with the privacy regulation, specifically in meeting the following requirements:
  - Providing to customers notices of its privacy policies and practices that are timely, accurate, clear and conspicuous, and delivered so that each customer can reasonably be expected to receive actual notice;
  - Disclosing nonpublic personal information to nonaffiliated third parties, other than under an exception, after first meeting the applicable requirements for giving consumers notice and the right to opt out;
  - Appropriately honoring consumer opt-out directions;
  - Lawfully using or disclosing nonpublic personal information received from a nonaffiliated financial institution; and
  - Disclosing account numbers only according to the limits in the regulations.

- To initiate effective corrective actions when violations of law are identified, or when policies or internal controls are deficient.

Initial Procedures

1. Through discussions with management and review of available information, identify the institution’s information sharing practices (and changes to those practices) with affiliates and nonaffiliated third parties; how it treats nonpublic personal information; and how it administers opt outs. Consider the following as appropriate:
   - Notices (initial, annual, revised, opt-out, short-form, and simplified);
   - Institutional privacy policies and procedures, including those to:
     — process requests for nonpublic personal information, including requests for aggregated data;
     — deliver notices to consumers;
DECISION TREE: PRIVACY NOTICE AND OPT-OUT

Does the financial institution share nonpublic personal information with nonaffiliated third parties under Sections 14 and/or 15 and outside of the exceptions (with or without also sharing under 13)?

Yes

Module 1
Privacy notice (presentation, content, and delivery) (with or without Section 13 notice & contracting)
Short-form notice (optional for consumers)
Customer notice delivery rules
Opt-out rules

No

Does the financial institution share nonpublic personal information with nonaffiliated third parties under Sections 13, 14 and/or 15 but not outside the exceptions?

Yes

Module 2
Privacy notice
Customer notice delivery rules
Section 13 notice & contracting

No

Does the financial institution share nonpublic personal information with nonaffiliated third parties only under Sections 14 and/or 15?

Yes

Module 3
Privacy notice
Simplified notice (if applicable)
Customer notice delivery rules

No

Exam Date:  
Prepared By:  
Reviewed By:  
Docket #:  
Privacy of Consumer Financial Information

SUBPART A

Initial Privacy Notice

NOTE: No notice is required if nonpublic personal information is disclosed to nonaffiliated third parties only under an exception in Sections 14 and 15, and there is no customer relationship. [§4(b)] With respect to credit relationships, an institution establishes a customer relationship when it originates a consumer loan. If the institution subsequently sells the servicing rights to the loan to another financial institution, the customer relationship transfers with the servicing rights. [§4(c)]

1. Does the institution provide a clear and conspicuous notice that accurately reflects its privacy policies and practices to all customers not later than when the customer relationship is established, other than as allowed in paragraph (e) of Section four (4) of the regulation [§4(a)(1)]?

2. Does the institution provide a clear and conspicuous notice that accurately reflects its privacy policies and practices to all consumers, who are not customers, before any nonpublic personal information about the consumer is disclosed to a nonaffiliated third party, other than under an exception in Sections 14 or 15 [§4(a)(2)]?

3. Does the institution provide to existing customers, who obtain a new financial product or service, an initial privacy notice that covers the customer's new financial product or service, if the most recent notice provided to the customer was not accurate with respect to the new financial product or service [§4(d)(1)]?

4. Does the institution provide initial notice after establishing a customer relationship only if:
   • The customer relationship is not established at the customer's election [§4(e)(1)(i)] or
   • To do otherwise would substantially delay the customer's transaction (e.g. in the case of a telephone application), and the customer agrees to the subsequent delivery [§4(e)(1)(ii)]?

5. When the subsequent delivery of a privacy notice is permitted, does the institution provide notice after establishing a customer relationship within a reasonable time [§4(e)]?

Annual Privacy Notice

6. Does the institution provide a clear and conspicuous notice that accurately reflects its privacy policies and practices at least annually (that is, at least once in any period of 12 consecutive months) to all customers, throughout the customer relationship?