such statute, regulation, order, or interpretation affords any consumer is greater than the protection provided under this part, as determined by the Commission on its own motion or upon the petition of any interested party, after consultation with the applicable federal functional regulator or other authority.

§ 313.18 Effective date; transition rule.

(a) *Effective date*—(1) *General rule.* This part is effective November 13, 2000. In order to provide sufficient time for you to establish policies and systems to comply with the requirements of this part, the Commission has extended the time for compliance with this part until July 1, 2001.

(2) *Exception.* This part is not effective as to any institution that is significantly engaged in activities that the Federal Reserve Board determines, after November 12, 1999, (pursuant to its authority in Section 4(k)(1–3) of the Bank Holding Company Act), are activities that a financial holding company may engage in, until the Commission so determines.

(b)(1) *Notice requirement for consumers who are your customers on the compliance date.* By July 1, 2001, you must have provided an initial notice, as required by § 313.4, to consumers who are your customers on July 1, 2001.

(2) *Example.* You provide an initial notice to consumers who are your customers on July 1, 2001, if, by that date, you have established a system for providing an initial notice to all new customers and have mailed the initial notice to all your existing customers.

(c) *Two-year grandfathering of service agreements.* Until July 1, 2002, a contract that you have entered into with a nonaffiliated third party to perform services for you or functions on your behalf satisfies the provisions of § 313.13(a)(1) of this part, even if the contract does not include a requirement that the third party maintain the confidentiality of nonpublic personal information, as long as you entered into the contract on or before July 1, 2000.

APPENDIX A TO PART 313—SAMPLE CLAUSES

Financial institutions, including a group of financial holding company affiliates that use a common privacy notice, may use the following sample clauses, if the clause is accurate for each institution that uses the notice. (Note that disclosure of certain information, such as assets and income, and information from a consumer reporting agency, may give rise to obligations under the Fair Credit Reporting Act, such as a requirement to permit a consumer to opt out of disclosures to affiliates or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.)

A–1—Categories of Information You Collect (All Institutions)

You may use this clause, as applicable, to meet the requirement of § 313.6(a)(1) to describe the categories of nonpublic personal information you collect.

Sample Clause A–1

We collect nonpublic personal information about you from the following sources:

- Information we receive from you on applications or other forms;
- Information about your transactions with us, our affiliates, or others; and
- Information we receive from a consumer reporting agency.

A–2—Categories of Information You Disclose (Institutions That Disclose Outside of the Exceptions)

You may use one of these clauses, as applicable, to meet the requirement of § 313.6(a)(2) to describe the categories of nonpublic personal information you disclose. You may use these clauses if you disclose nonpublic personal information other than as permitted by the exceptions in §§ 313.13, 313.14, and 313.15.

Sample Clause A–2, Alternative 1

We may disclose the following kinds of nonpublic personal information about you:

- Information we receive from you on applications or other forms, such as [*provide illustrative examples, such as ''your name, address, social security number, assets, and income''*];
- Information about your transactions with us, our affiliates, or others, such as [*provide illustrative examples, such as ''your account balance, payment history, parties to transactions, and credit card usage''*]; and
- Information we receive from a consumer reporting agency, such as [*provide illustrative examples, such as ''your creditworthiness and credit history''*].

Sample Clause A–2, Alternative 2

We may disclose all of the information that we collect, as described [*describe location in the notice, such as ''above'' or ''below''*].

A–3—Categories of Information You Disclose and Parties to Whom You Disclose (Institutions That Do Not Disclose Outside of the Exceptions)

You may use this clause, as applicable, to meet the requirements of §§313.6(a)(2), (3), and (4) to describe the categories of nonpublic personal information about customers and former customers that you disclose and the categories of affiliates and nonaffiliated third parties to whom you disclose. You may use this clause if you do not disclose nonpublic personal information to any party, other than as permitted by the exceptions in §§313.14, and 313.15.

Sample Clause A–3

We do not disclose any nonpublic personal information about our customers or former customers to anyone, except as permitted by law.

A–4—Categories of Parties to Whom You Disclose (Institutions That Disclose Outside of the Exceptions)

You may use this clause, as applicable, to meet the requirement of §313.6(a)(3) to describe the categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information. You may use this clause if you disclose nonpublic personal information other than as permitted by the exceptions in §§313.13, 313.14, and 313.15, as well as when permitted by the exceptions in §§313.14, and 313.15.

Sample Clause A–4

We may disclose nonpublic personal information about you to the following types of third parties:

• Financial service providers, such as [*provide illustrative examples, such as ''mortgage bankers, securities broker-dealers, and insurance agents''*];

• Non-financial companies, such as [*provide illustrative examples, such as ''retailers, direct marketers, airlines, and publishers''*]; and

• Others, such as [*provide illustrative examples, such as ''non-profit organizations''*].

We may also disclose nonpublic personal information about you to nonaffiliated third parties as permitted by law.

A–5—Service Provider/Joint Marketing Exception

You may use one of these clauses, as applicable, to meet the requirements of §313.6(a)(5) related to the exception for service providers and joint marketers in §313.13. If you disclose nonpublic personal information under this exception, you must describe the categories of nonpublic personal information you disclose and the categories of third parties with whom you have contracted.

Sample Clause A–5, Alternative 1

We may disclose the following information to companies that perform marketing services on our behalf or to other financial institutions with whom we have joint marketing agreements:

• Information we receive from you on applications or other forms, such as [*provide illustrative examples, such as ''your name, address, social security number, assets, and income''*];

• Information about your transactions with us, our affiliates, or others, such as [*provide illustrative examples, such as ''your account balance, payment history, parties to transactions, and credit card usage''*]; and

• Information we receive from a consumer reporting agency, such as [*provide illustrative examples, such as ''your creditworthiness and credit history''*].

Sample Clause A–5, Alternative 2

We may disclose all of the information we collect, as described [*describe location in the notice, such as ''above'' or ''below''*] to companies that perform marketing services on our behalf or to other financial institutions with whom we have joint marketing agreements.

A–6—Explanation of Opt Out Right (Institutions that Disclose Outside of the Exceptions)

You may use this clause, as applicable, to meet the requirement of §313.6(a)(6) to provide an explanation of the consumer's right to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the method(s) by which the consumer may exercise that right. You may use this clause if you disclose nonpublic personal information other than as permitted by the exceptions in §§313.13, 313.14, and 313.15.

Sample Clause A–6

If you prefer that we not disclose nonpublic personal information about you to nonaffiliated third parties, you may opt out of those disclosures, that is, you may direct us not to make those disclosures (other than disclosures permitted by law). If you wish to opt out of disclosures to nonaffiliated third parties, you may [*describe a reasonable means of opting out, such as ''call the following toll-free number: (insert number)''*].

A–7—Confidentiality and Security (All Institutions)

You may use this clause, as applicable, to meet the requirement of §313.6(a)(8) to describe your policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.

Sample Clause A–7

We restrict access to nonpublic personal information about you to [*provide an appropriate description, such as ''those employees who need to know that information to provide products or services to you''*]. We maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic personal information.

PART 314—STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

Sec.
314.1 Purpose and scope.
314.2 Definitions.
314.3 Standards for safeguarding customer information.
314.4 Elements.
314.5 Effective date.

AUTHORITY: 15 U.S.C. 6801(b), 6805(b)(2).

SOURCE: 67 FR 36493, May 23, 2002, unless otherwise noted.

§314.1 Purpose and scope.

(a) *Purpose.* This part, which implements sections 501 and 505(b)(2) of the Gramm-Leach-Bliley Act, sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

(b) *Scope.* This part applies to the handling of customer information by all financial institutions over which the Federal Trade Commission (''FTC'' or ''Commission'') has jurisdiction. This part refers to such entities as ''you.'' This part applies to all customer information in your possession, regardless of whether such information pertains to individuals with whom you have a customer relationship, or pertains to the customers of other financial institutions that have provided such information to you.

§314.2 Definitions.

(a) *In general.* Except as modified by this part or unless the context otherwise requires, the terms used in this part have the same meaning as set forth in the Commission's rule governing the Privacy of Consumer Financial Information, 16 CFR part 313.

(b) *Customer information* means any record containing nonpublic personal information as defined in 16 CFR 313.3(n), about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates.

(c) *Information security program* means the administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

(d) *Service provider* means any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution that is subject to this part.

§314.3 Standards for safeguarding customer information.

(a) *Information security program.* You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. Such safeguards shall include the elements set forth in §314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.

(b) *Objectives.* The objectives of section 501(b) of the Act, and of this part, are to:

(1) Insure the security and confidentiality of customer information;

(2) Protect against any anticipated threats or hazards to the security or integrity of such information; and

(3) Protect against unauthorized access to or use of such information that