(ii) If it shares with nonaffiliated third parties, state, as applicable: "Nonaffiliates we share with can include [list categories of companies such as mortgage companies, insurance companies, direct marketing companies, and nonprofit organizations]."

(3) Joint Marketing. As required by §313.13 of this part, where [joint marketing] appears, the financial institution must:
   (i) If it does not engage in joint marketing, state: "[name of financial institution] doesn’t jointly market"; or
   (ii) If it shares personal information for joint marketing, state, as applicable: "Our joint marketing partners include [list categories of companies such as credit card companies]."

(c) General instructions for the “Other important information” box. This box is optional. The space provided for information in this box is not limited. Only the following types of information can appear in this box:
   (1) State and/or international privacy law information; and/or
   (2) Acknowledgment of receipt form.

[74 FR 62966, Dec. 1, 2009]

PART 314—STANDARDS FOR SAFE-GUARDING 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.
314.6 Exceptions.

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. Namely, this part applies to those “financial institutions” subject to the Commission’s enforcement authority under section 501 of the Gramm-Leach-Bliley Act. An entity is a “financial institution” if its business is engaging in an activity that is financial in nature or incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C. 1843(k), which incorporates activities enumerated by the Federal Reserve Board in 12 CFR 225.28 and 225.86. More specifically, those entities include, but are not limited to, mortgage lenders, "pay day" lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, travel agencies operated in connection with financial services, collection agencies, credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, investment advisors that are not required to register with the Securities and Exchange Commission, and entities acting as finders. They are referred to in this part 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.

EFFECTIVE DATE NOTE: At 86 FR 70304, Dec. 9, 2021, §314.1 was amended by revising paragraph (b), effective Jan. 10, 2022. For the convenience of the user, the revised text is set forth as follows:

§ 314.1 Purpose and scope.

* * * * *

(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. Namely, this part applies to those “financial institutions” subject to the Commission’s enforcement authority under section 501 of the Gramm-Leach-Bliley Act. An entity is a “financial institution” if its business is engaging in an activity that is financial in nature or incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C. 1843(k), which incorporates activities enumerated by the Federal Reserve Board in 12 CFR 225.28 and 225.86. More specifically, those entities include, but are not limited to, mortgage lenders, “pay day” lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, travel agencies operated in connection with financial services, collection agencies, credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, investment advisors that are not required to register with the Securities and Exchange Commission, and entities acting as finders. They are referred to in this part 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
§314.2 Definitions.

(a) Authorized user means any employee, contractor, agent, customer, or other person that is authorized to access any of your information systems or data.

(b)(1) Consumer means an individual who obtains or has obtained a financial product or service from you that is to be used primarily for personal, family, or household purposes, or that individual’s legal representative.

(ii) For example:

(i) An individual who applies to you for credit for personal, family, or household purposes is a consumer of a financial service, regardless of whether the credit is extended.

(ii) An individual who provides nonpublic personal information to you in order to obtain a determination about whether he or she may qualify for a loan to be used primarily for personal, family, or household purposes is a consumer of a financial service, regardless of whether the loan is extended.

(iii) An individual who provides nonpublic personal information to you in connection with obtaining or seeking to obtain financial, investment, or economic advisory services is a consumer, regardless of whether you establish a continuing advisory relationship.

(iv) If you hold ownership or servicing rights to an individual’s loan that is used primarily for personal, family, or household purposes, the individual is your consumer, even if you hold those rights in conjunction with one or more other institutions. (The individual is also a consumer with respect to the other financial institutions involved.) An individual who has a loan in which you have ownership or servicing rights is your consumer, even if you, or another institution with those rights, hire an agent to collect on the loan.

(v) An individual who is a consumer of another financial institution is not your consumer solely because you act as agent for, or provide processing or other services to, that financial institution.

(vi) An individual is not your consumer solely because he or she has designated you as trustee for a trust.

(vii) An individual is not your consumer solely because he or she is a beneficiary of a trust for which you are a trustee.

(viii) An individual is not your consumer solely because he or she is a participant or a beneficiary of an employee benefit plan that you sponsor or for which you act as a trustee or fiduciary.

(c) Customer means a consumer who has a customer relationship with you.

(d) Customer information means any record containing nonpublic personal information 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.

(e)(1) Continuing relationship means a continuing relationship between a consumer and you under which you provide one or more financial products or services to the consumer that are to be used primarily for personal, family, or household purposes.

(e)(2) For example:

(i) Continuing relationship. A consumer has a continuing relationship with you if the consumer:

(A) Has a credit or investment account with you;

(B) Obtains a loan from you;

(C) Purchases an insurance product from you;

(D) Holds an investment product through you, such as when you act as a custodian for securities or for assets in an Individual Retirement Arrangement;

(E) Enters into an agreement or understanding with you whereby you undertake to arrange or broker a home mortgage loan, or credit to purchase a vehicle, for the consumer;

(F) Enters into a lease of personal property on a non-operating basis with you;

(G) Obtains financial, investment, or economic advisory services from you for a fee;

(H) Becomes your client for the purpose of obtaining tax preparation or credit counseling services from you;

(I) Obtains career counseling while seeking employment with a financial institution or the finance, accounting, or audit department of any company (or while employed by such
§ 314.2 16 CFR Ch. I (1–1–22 Edition)

(a) A financial institution or department of any company;

(J) Is obligated on an account that you purchase from another financial institution, regardless of whether the account is in default when purchased, unless you do not locate the consumer or attempt to collect any amount from the consumer on the account;

(h) Obtains real estate settlement services from you; or

(L) Has a loan for which you own the servicing rights.

(ii) No continuing relationship. A consumer does not, however, have a continuing relationship with you if:

(A) The consumer obtains a financial product or service from you only in isolated transactions, such as using your ATM to withdraw cash from an account at another financial institution; purchasing a money order from you; cashing a check with you; or making a wire transfer through you;

(B) You sell the consumer’s loan and do not retain the rights to service that loan;

(C) You sell the consumer airline tickets, travel insurance, or traveler’s checks in isolated transactions;

(D) The consumer obtains one-time personal or real property appraisal services from you; or

(E) The consumer purchases checks for a personal checking account from you.

(f) Encryption means the transformation of data into a form that results in a low probability of assigning meaning without the use of a protective process or key, consistent with current cryptographic standards and accompanied by appropriate safeguards for cryptographic key material.

(g)(1) Financial product or service means any product or service that a financial holding company could offer by engaging in a financial activity under section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)), and issuing that extension of credit through a proprietary credit card demonstrates that a retailer is significantly engaged in extending credit.

(ii) An automobile dealership that, as a usual part of its business, leases automobiles on a nonoperating basis for longer than 90 days is a financial institution with respect to its leasing business because leasing personal property on a nonoperating basis where the initial term of the lease is at least 90 days is a financial activity listed in 12 CFR 225.28(b)(3) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).

(iii) A personal property or real estate appraiser is a financial institution because real and personal property appraisal is a financial activity listed in 12 CFR 225.28(b)(9)(ii) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).

(iv) A career counselor that specializes in providing career counseling services to individuals currently employed by or recently displaced from a financial organization, individuals who are seeking employment with a financial organization, or individuals who are currently employed by or seeking placement with the finance, accounting or audit departments of any company is a financial institution because such career counseling activities are financial activities listed in 12 CFR 225.28(b)(9)(i) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).

(v) A business that prints and sells checks for consumers, either as its sole business or as one of its product lines, is a financial institution because printing and selling checks is a financial activity that is listed in 12 CFR 225.28(b)(10)(ii) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).

(vi) A business that regularly wires money to and from consumers is a financial institution because transferring money is a financial activity referenced in section 4(k)(4)(A) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(A), and regularly providing that service demonstrates that the business is significantly engaged in that activity.

(vii) A check cashing business is a financial institution because cashing a check is exchanging money, which is a financial activity listed in section 4(k)(4)(A) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(A).

(viii) An accountant or other tax preparation service that is in the business of completing income tax returns is a financial institution because tax preparation services is a financial activity listed in 12 CFR 225.28(b)(6)(vi) and referenced in section 4(k)(4)(G) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(G).

456
(ix) A business that operates a travel agency in connection with financial services is a financial institution because operating a travel agency in connection with financial services is a financial activity listed in 12 CFR 225.86(b)(2) and referenced in section 4(k)(4)(G) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(G).

(xi) A mortgage broker is a financial institution because brokering loans is a financial activity listed in 12 CFR 225.28(b)(1) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).

(x) An entity that provides real estate settlement services is a financial institution because providing real estate settlement services is a financial activity listed in 12 CFR 225.28(b)(2)(viii) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).

(ii) A retailer is not a financial institution merely because it accepts payment in the form of cash, checks, or credit cards that it did not issue.

(iii) A merchant is not a financial institution merely because it allows an individual to “run a tab.”

(iv) A grocery store is not a financial institution merely because it allows individuals to whom it sells groceries to cash a check, or write a check for a higher amount than the grocery purchase and obtain cash in return.

(i) 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.

(ii) Information system means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information containing customer information or connected to a system containing customer information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental controls systems that contains customer information or that is connected to a system that contains customer information.

(k) Multi-factor authentication means authentication through verification of at least two of the following types of authentication factors:

(1) Knowledge factors, such as a password;

(2) Possession factors, such as a token; or

(3) Inherence factors, such as biometric characteristics.

(i) Nonpublic personal information means:

(1) Personally identifiable financial information; and

(ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.

(2) Nonpublic personal information does not include:

(i) Publicly available information, except as included on a list described in paragraph (1)(i)(ii) of this section; or

(ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any personally identifiable financial information that is not publicly available.

(3) For example:

(1) Nonpublic personal information includes any list of individuals’ names and street addresses that is derived in whole or
in part using personally identifiable financial information (that is not publicly available), such as account numbers.

(ii) Nonpublic personal information does not include any list of individuals’ names and addresses that contains only publicly available information, is not derived, in whole or in part, using personally identifiable financial information that is not publicly available, and is not disclosed in a manner that indicates that any of the individuals on the list is a consumer of a financial institution.

(m) Penetration testing means a test methodology in which assessors attempt to circumvent or defeat the security features of an information system by attempting penetration of databases or controls from outside or inside your information systems.

(n)(1) Personally identifiable financial information means any information:

(i) A consumer provides to you to obtain a financial product or service from you;

(ii) About a consumer resulting from any transaction involving a financial product or service between you and a consumer; or

(iii) You otherwise obtain about a consumer in connection with providing a financial product or service to that consumer.

(2) For example:

(i) Information included. Personally identifiable financial information includes:

(A) Information a consumer provides to you on an application to obtain a loan, credit card, or other financial product or service;

(B) Account balance information, payment history, overdraft history, and credit or debit card purchase information;

(C) The fact that an individual is or has been one of your customers or has obtained a financial product or service from you;

(D) Any information about your consumer if it is disclosed in a manner that indicates that the individual is or has been your consumer;

(E) Any information that a consumer provides to you or that you or your agent otherwise obtain in connection with collecting on, or servicing, a credit account;

(F) Any information you collect through an internet “cookie” (an information collecting device from a web server); and

(G) Information from a consumer report.

(ii) Information not included. Personally identifiable financial information does not include:

(A) A list of names and addresses of customers of an entity that is not a financial institution; and

(B) Information that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names, or addresses.

(o)(1) Publicly available information means any information that you have a reasonable basis to believe is lawfully made available to the general public from:

(i) Federal, State, or local government records;

(ii) Widely distributed media; or

(iii) Disclosures to the general public that are required to be made by Federal, State, or local law.

(2) You have a reasonable basis to believe that information is lawfully made available to the general public if you have taken steps to determine:

(i) That the information is of the type that is available to the general public; and

(ii) Whether an individual can direct that the information not be made available to the general public and, if so, that your consumer has not done so.

(3) For example:

(i) Government records. Publicly available information in government records includes information in government real estate records and security interest filings.

(ii) Widely distributed media. Publicly available information from widely distributed media includes information from a telephone book, a television or radio program, a newspaper, or a website that is available to the general public on an unrestricted basis. A website is not restricted merely because an internet service provider or a site operator requires a fee or a password, so long as access is available to the general public.

(iii) Reasonable basis. (A) You have a reasonable basis to believe that information is lawfully made available to the general public if you have determined that the information is of the type included on the public record in the jurisdiction where the mortgage would be recorded.

(B) You have a reasonable basis to believe that an individual’s telephone number is lawfully made available to the general public if you have located the telephone number in the telephone book or the consumer has informed you that the telephone number is not unlisted.

(g) Security event means an event resulting in unauthorized access to, or disruption or misuse of, an information system, information stored on such information system, or customer information held in physical form.

(r) 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.

(t) You includes each “financial institution” (but excludes any “other person”) over which the Commission has enforcement jurisdiction pursuant to section 505(a)(7) of the Gramm-Leach-Bliley Act.