

Federal Trade Commission (FTC) Standards for Safeguarding Customer Information: Resource and Tandem Mapping

Introduction

On December 9, 2021, the Federal Trade Commission (FTC) published their revised [Standards for Safeguarding Customer Information](#) (16 CFR Part 314) in accordance with the Gramm-Leach-Bliley Act (GLBA). The rule exists to improve how financial institutions regulated by the FTC develop and implement their information security programs.

This resource is for information purposes only. It serves to provide Tandem's opinion of the regulatory language included in the revised rule. You may use this resource to assist in your understanding of the regulation, but you should interpret the regulation, as appropriate, for your organization.

This resource also serves to identify areas in Tandem where topics from the new rule are addressed and does not guarantee that an organization using Tandem achieves the expectations.

About Tandem: Tandem is a tool designed to assist with compliance goals and improve cybersecurity through the development of an information security program. There are multiple Tandem products referenced in this mapping which can help address the requirements of the updated standards. These products include [Risk Assessment](#), [Policies](#), [Vendor Management](#), [Audit Management](#), [Phishing](#), and [Incident Management](#).

If you do not have access to the Tandem products referenced by this mapping, but would like to learn more, contact us at info@tandem.app or on our website, [Tandem.App/Contact](#).

Mapping

Sections marked with a red asterisk (*) are not effective until 12/09/2022; all other sections are effective 01/10/2022.

Sections marked with a blue square (■) do not apply to financial institutions which maintain customer information for fewer than 5,000 consumers.

Section	Section Text	Tandem Opinion	Tandem Mapping
314.1	<p>Purpose and Scope</p> <p>(b) <i>Scope</i>. 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” over which the Commission has rulemaking authority pursuant to section 501(b) 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 by reference activities enumerated by the Federal Reserve Board in 12 CFR 225.28 and 12 CFR 225.86. The “financial institutions” subject to the Commission’s enforcement authority are those that are not otherwise subject to the enforcement authority of another regulator under section 505 of the Gramm-Leach-Bliley Act, 15 U.S.C. 6805. 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.</p>	<p>This section introduces the types of financial institutions covered by the rule (see highlighted text). Additional types of financial institutions addressed in section 314.2(h)(2) include certain retailers, automobile dealerships, appraisers, career counselors, and check printers. Essentially, the rule applies to any business who offers financial services and is not regulated by another agency. There are some exclusions in section 314.2(h)(4).</p> <p>This section also clarifies that when the rule says “customer information,” it means customer information provided to you by anyone (i.e., customers, other institutions, etc.).</p>	N/A


Section	Section Text	Tandem Opinion	Tandem Mapping
314.2	Definitions <i>(Refer to the final rule for the full text. See pages 124 – 137 of the PDF.)</i>	This section is important to understanding the application of the final rule and includes clarifying examples, but does not contain any regulatory expectations itself.	N/A
314.3	Standards for Safeguarding Customer Information (a) <i>Information security program.</i> 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. The information security program shall include the elements set forth in section 314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.	This section is nearly identical to the previous version of the rule. The only change was an update from “such safeguards” to “the information security program” (see highlighted text).	Tandem is a web-based application designed to help financial institutions develop, implement, and maintain their information security programs in accordance with GLBA. Tandem is currently used by 1,500+ financial institutions.
314.4	Elements In order to develop, implement, and maintain your information security program, you shall:		
314.4(a) *	Designate a qualified individual responsible for overseeing and implementing your information security program and enforcing your information security program (for purposes of this part, “Qualified Individual”). The Qualified Individual may be employed by you, an affiliate, or a service provider. To the extent this requirement is met using a service provider or an affiliate, you shall: (1) Retain responsibility for compliance with this part; (2) Designate a senior member of your personnel responsible for direction and oversight of the Qualified Individual; and (3) Require the service provider or affiliate to maintain an information security program that protects you in accordance with the requirements of this Part.	This section requires a single person to oversee, implement, and enforce your program. The rule refers to this person as a “qualified individual.” FTC commentary on the rule states you “may designate any qualified individual who is appropriate for [your] business.” If you choose to outsource this function, your financial institution is still responsible for 1) complying with the rule, 2) managing the qualified individual, and 3) requiring the service provider to implement the rule on your behalf.	Admin <ul style="list-style-type: none"> Positions Create a position for your “qualified individual” or assign the employee/third-party contact to an existing position (e.g., Information Security Officer, Network Administrator, IT Staff, etc.).

Section	Section Text	Tandem Opinion	Tandem Mapping
314.4(b)	Base your information security program on a risk assessment that identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assesses the sufficiency of any safeguards in place to control these risks.	This section requires the creation of a risk assessment to identify threats and assess the sufficiency of controls.	Risk Assessment <ul style="list-style-type: none"> Threats Controls Risk Management Plans Audit Management <ul style="list-style-type: none"> Control / Audit Association
314.4(b)(1) * 	<p>The risk assessment shall be written and shall include:</p> <p>(i) Criteria for the evaluation and categorization of identified security risks or threats you face;</p> <p>(ii) Criteria for the assessment of the confidentiality, integrity, and availability of your information systems and customer information, including the adequacy of the existing controls in the context of the identified risks or threats you face; and</p> <p>(iii) Requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the risks.</p>	<p>This section requires the risk assessment to be written (documented, not just conceptual) and it must include:</p> <ol style="list-style-type: none"> How you evaluated the risks. How you determined the CIA requirements of your assets and how you determined control adequacy. How you created your risk management plans. 	Risk Assessment <ul style="list-style-type: none"> Download Documents "Introduction" and "Definitions" Sections
314.4(b)(2)	You shall periodically perform additional risk assessments that reexamine the reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and reassess the sufficiency of any safeguards in place to control these risks.	This section clarifies that a risk assessment is not a one-time process and should be performed "periodically."	Risk Assessment <ul style="list-style-type: none"> Version Tracking Revision/Approval Log
314.4(c)	Design and implement safeguards to control the risks you identify through risk assessment, including by:		

Section	Section Text	Tandem Opinion	Tandem Mapping
314.4(c)(1) *	Implementing and periodically reviewing access controls, including technical and, as appropriate, physical controls to (1) authenticate and permit access only to authorized users to protect against the unauthorized acquisition of customer information and (2) limit authorized users' access only to customer information that they need to perform their duties and functions, or, in the case of customers, to access their own information;	This section requires the implementation of technical and physical access controls, including least privilege, to ensure no unauthorized access occurs.	Risk Assessment Controls <ul style="list-style-type: none"> • Limit Local Administrator Access • Logical Access Controls • Physical Access Controls • Separation of Duties Policies <ul style="list-style-type: none"> • Access Control • Administrators • Personnel Security
314.4(c)(2) *	Identify and manage the data, personnel, devices, systems, and facilities that enable you to achieve business purposes in accordance with their relative importance to business objectives and your risk strategy;	This section requires the performance of effective data identification, classification, and asset management.	Risk Assessment <ul style="list-style-type: none"> • Data Types • Data Classifications • Information Assets Policies <ul style="list-style-type: none"> • IT Asset Management
314.4(c)(3) *	Protect by encryption all customer information held or transmitted by you both in transit over external networks and at rest. To the extent you determine that encryption of customer information, either in transit over external networks or at rest, is infeasible, you may instead secure such customer information using effective alternative compensating controls reviewed and approved by your Qualified Individual;	This section requires the encryption of customer data at rest and in transit. If encryption is infeasible, compensating controls are expected.	Risk Assessment Controls <ul style="list-style-type: none"> • Data Encryption Policies <ul style="list-style-type: none"> • Encryption




Section	Section Text	Tandem Opinion	Tandem Mapping
314.4(c)(4) *	Adopt secure development practices for in-house developed applications utilized by you for transmitting, accessing, or storing customer information and procedures for evaluating, assessing, or testing the security of externally developed applications you utilize to transmit, access, or store customer information;	This section requires the use of secure development practices internally, as well as an evaluation of the security of third-party developed applications.	Risk Assessment Controls <ul style="list-style-type: none"> Secure Coding Techniques Policies <ul style="list-style-type: none"> Third-Party Secure Application Development
314.4(c)(5) *	Implement multi-factor authentication for any individual accessing any information system, unless your Qualified Individual has approved in writing the use of reasonably equivalent or more secure access controls;	This section requires multi-factor authentication to be implemented everywhere possible. If approved in writing by the qualified individual, compensating controls may be used.	Risk Assessment Controls <ul style="list-style-type: none"> Multifactor Authentication Policies <ul style="list-style-type: none"> Administrators Authentication Cloud Computing Remote Access
314.4(c)(6) *	<p>(i) Develop, implement, and maintain procedures for the secure disposal of customer information in any format no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates, unless such information is necessary for business operations or for other legitimate business purposes, is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained; and</p> <p>(ii) Periodically review your data retention policy to minimize the unnecessary retention of data;</p>	This section requires the implementation and review of secure data disposal practices for customer information. The data must be disposed "no later than two years" after the last date the information is used for business, except in certain circumstances (e.g., legal requirements, infeasibility, etc.).	Risk Assessment Controls <ul style="list-style-type: none"> Data Retention and Destruction Procedures Policies <ul style="list-style-type: none"> Data Retention and Destruction

Section	Section Text	Tandem Opinion	Tandem Mapping
314.4(c)(7) *	Adopt procedures for change management; and	This section requires change management procedures.	Risk Assessment Controls <ul style="list-style-type: none"> Change Management Policies <ul style="list-style-type: none"> Change Management
314.4(c)(8) *	Implement policies, procedures and controls designed to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users.	This section requires the logging and monitoring of user activity.	Risk Assessment Controls <ul style="list-style-type: none"> Internal Network Monitoring Logical Access Controls User Activity Log Policies <ul style="list-style-type: none"> Access Control Network Monitoring and Log Management
314.4(d)(1)	Regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems.	This section requires validation of controls to ensure they function, as expected.	Audit Management Policies <ul style="list-style-type: none"> Security Testing

Section	Section Text	Tandem Opinion	Tandem Mapping
314.4(d)(2) * 	<p>For information systems, the monitoring and testing shall include continuous monitoring or periodic penetration testing and vulnerability assessments. Absent effective continuous monitoring or other systems to detect, on an ongoing basis, changes in information systems that may create vulnerabilities, you shall conduct:</p> <p>i. Annual penetration testing of your information systems determined each given year based on relevant identified risks in accordance with the risk assessment; and</p> <p>ii. Vulnerability assessments, including any systemic scans or reviews of information systems reasonably designed to identify publicly known security vulnerabilities in your information systems based on the risk assessment, at least every six months; and whenever there are material changes to your operations or business arrangements; and whenever there are circumstances you know or have reason to know may have a material impact on your information security program.</p>	<p>This section requires the continuous monitoring of controls - or - the performance of:</p> <ol style="list-style-type: none"> 1. Annual penetration testing; and 2. Vulnerability assessments 1) semiannually, 2) following significant changes, and 3) when something might impact the information security program. 	<p>Audit Management</p> <p>Policies</p> <ul style="list-style-type: none"> • Security Testing
314.4(e) *	Implement policies and procedures to ensure that personnel are able to enact your information security program by:		
314.4(e)(1) *	Providing your personnel with security awareness training that is updated as necessary to reflect risks identified by the risk assessment;	This section requires up-to-date security awareness training.	<p>Phishing</p> <p>Policies</p> <ul style="list-style-type: none"> • Security Awareness Training <p>Training</p> <ul style="list-style-type: none"> • Security Awareness Training • Phishing Training
314.4(e)(2) *	Utilizing qualified information security personnel employed by you or an affiliate or service provider sufficient to manage your information security risks and to perform or oversee the information security program;	This section requires the people who manage your information security risks and program to be qualified.	<p>Policies</p> <ul style="list-style-type: none"> • Security Awareness Training <p>Vendor Management</p>

Section	Section Text	Tandem Opinion	Tandem Mapping
314.4(e)(3) *	Providing information security personnel with security updates and training sufficient to address relevant security risks; and	This section requires relevant security risks to be addressed in training.	Phishing Policies <ul style="list-style-type: none"> Personnel Security Security Awareness Training Training <ul style="list-style-type: none"> Security Awareness Training Phishing Training
314.4(e)(4) *	Verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.	This section requires information security personnel to maintain current knowledge of information security concepts.	Policies <ul style="list-style-type: none"> Security Awareness Training Personnel Security Training <ul style="list-style-type: none"> Security Awareness Training Phishing Training
314.4(f)	Oversee service providers, by:		
314.4(f)(1)	Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue;	This section requires the selection of capable service providers.	Vendor Management
314.4(f)(2)	Requiring your service providers by contract to implement and maintain such safeguards; and	This section expects service providers be required by contract to maintain the same security controls required of you, per this rule.	Vendor Management <ul style="list-style-type: none"> Contracts Contract Reviews

Section	Section Text	Tandem Opinion	Tandem Mapping
314.4(f)(3) *	Periodically assessing your service providers based on the risk they present and the continued adequacy of their safeguards.	This section requires the performance of regular reviews to make sure service providers are keeping their end of the bargain.	Vendor Management <ul style="list-style-type: none"> Risk Assessment Reviews
314.4(g)	Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (d) of this section; any material changes to your operations or business arrangements; the results of risk assessments performed under paragraph (b)(2) of this section; or any other circumstances that you know or have reason to know may have a material impact on your information security program.	This section requires regularly updating the information security program based on 1) results of testing, 2) changes in the business, 3) results of risk assessments, or 4) any other circumstances which might impact the program.	Tandem products include revision/approval logs to track updates.
314.4(h) * □	Establish a written incident response plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information in your control. Such incident response plan shall address the following areas:	This section requires the creation of a written incident response plan.	Incident Management
314.4(h)(1) * □	The goals of the incident response plan;	This section requires a determination of the plan's goals.	Incident Management <ul style="list-style-type: none"> Introduction
314.4(h)(2) * □	The internal processes for responding to a security event;	This section requires incident response processes.	Incident Management <ul style="list-style-type: none"> Action Plans / Action Steps
314.4(h)(3) * □	The definition of clear roles, responsibilities and levels of decision-making authority;	This section requires defining roles and responsibilities.	Incident Management <ul style="list-style-type: none"> Roles & Responsibilities Incident Handlers

Section	Section Text	Tandem Opinion	Tandem Mapping
314.4(h)(4) * 	External and internal communications and information sharing;	This section requires defining communication guidelines.	Incident Management <ul style="list-style-type: none"> Additional Documentation (i.e., Customer Communication, Internal Communication, Third-Party Communication, Appendix: Communication Templates, etc.)
314.4(h)(5) * 	Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;	This section requires fixing the problem(s) which resulted in the incident.	Incident Management <ul style="list-style-type: none"> Incident Handling Process "Postmortem"
314.4(h)(6) * 	Documentation and reporting regarding security events and related incident response activities; and	This section requires documenting and reporting security incident response details.	Incident Management <ul style="list-style-type: none"> Incident Tracking
314.4(h)(7) * 	The evaluation and revision as necessary of the incident response plan following a security event.	This section requires reviewing and updating the plan following an incident.	Incident Management <ul style="list-style-type: none"> Incident Handling Process "Postmortem"
314.4(i) * 	<p>Require your Qualified Individual to report in writing, regularly and at least annually, to your board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report shall be timely presented to a senior officer responsible for your information security program. The report shall include the following information:</p> <p>(1) The overall status of the information security program and your compliance with this Rule; and</p> <p>(2) Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto, and recommendations for changes in the information security program.</p>	This section requires the qualified individual to report to the Board at least annually on 1) the overall status of the program and 2) significant happenings related to the individual program components, including any proposed changes.	Each product includes a set of reports and download documents designed to facilitate reporting to the Board.

Section	Section Text	Tandem Opinion	Tandem Mapping
314.5	Effective Date Section 314.4(a), (b)(1), (c)(1) through (8), (d)(2), (e), (f)(3), (h), and (i) are effective as of December 9, 2022.	Certain sections are not effective until 12/09/2022. These sections were identified with a red asterisk (*). The rest of the rule is effective 01/10/2022.	N/A
314.6	Exceptions Sections 314.4(b)(1), 314.4(d)(2), 314.4(h), and 314.4(i) do not apply to financial institutions that maintain customer information concerning fewer than five thousand consumers.	Certain sections do not apply to financial institutions which maintain customer information for fewer than 5,000 consumers. These sections were identified with a blue square (□).	N/A