NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document : Secure Controls Framework (SCF) version 2026.1
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Financial Industry Regulatory Authority (FINRA)**
Focal Document URL: https://www.finra.org/rules-guidance/key-topics/cybersecurity#rules
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-sro-finra.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
1220(b)(3)	Operations Professional	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1220(b)(3)(A)	Requirement	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1220(b)(3)(A)(i)	Covered Persons	Each of the following persons shall be required to register with FINRA as an Operations Professional:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1220(b)(3)(A)(i)(a)	Covered Persons	senior management with direct responsibility over the covered functions specified in paragraph (b)(3)(A)(ii) of this Rule;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1220(b)(3)(A)(i)(b)	Covered Persons	any person designated by senior management specified in paragraph (b)(3)(A)(i)a. of this Rule as a supervisor, manager or other person responsible for approving or authorizing work, including work of other persons, in direct furtherance of each of the covered functions specified in paragraph (b)(3)(A)(ii) of this Rule, as applicable, provided that there is sufficient designation of such persons by senior management to address each of the applicable covered functions; and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1220(b)(3)(A)(i)(c)	Covered Persons	persons with the authority or discretion materially to commit a member's capital in direct furtherance of the covered functions specified in paragraph (b)(3)(A)(ii) of this Rule or to commit a member to any material contract or agreement (written or oral) in direct furtherance of the covered functions specified in paragraph (b)(3)(A)(ii) of this Rule.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1220(b)(3)(A)(ii)	Covered Functions	For purposes of paragraph (b)(3) of this Rule, the following are the covered functions:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1220(b)(3)(A)(ii)(a)	Covered Functions	client on-boarding (customer account data and document maintenance);	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1220(b)(3)(A)(ii)(b)	Covered Functions	collection, maintenance, re-investment (i.e., sweeps) and disbursement of funds;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1220(b)(3)(A)(ii)(c)	Covered Functions	receipt and delivery of securities and funds, account transfers;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1220(b)(3)(A)(ii)(d)	Covered Functions	bank, custody, depository and firm account management and reconciliation;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1220(b)(3)(A)(ii)(e)	Covered Functions	settlement, fail control, buy ins, segregation, possession and control;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1220(b)(3)(A)(ii)(f)	Covered Functions	trade confirmation and account statements;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1220(b)(3)(A)(ii)(g)	Covered Functions	margin;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1220(b)(3)(A)(ii)(h)	Covered Functions	stock loan or securities lending;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1220(b)(3)(A)(ii)(i)	Covered Functions	prime brokerage (services to other broker-dealers and financial institutions);	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1220(b)(3)(A)(ii)(j)	Covered Functions	approval of pricing models used for valuations;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1220(b)(3)(A)(ii)(k)	Covered Functions	financial control, including general ledger and treasury;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1220(b)(3)(A)(ii)(l)	Covered Functions	contributing to the process of preparing and filing financial regulatory reports;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1220(b)(3)(A)(ii)(m)	Covered Functions	defining and approving business requirements for sales and trading systems and any other systems related to the covered functions, and validation that these systems meet such business requirements;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1220(b)(3)(A)(ii)(n)	Covered Functions	defining and approving business security requirements and policies for information technology, including, but not limited to, systems and data, in connection with the covered functions;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1220(b)(3)(A)(ii)(o)	Covered Functions	defining and approving information entitlement policies in connection with the covered functions; and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1220(b)(3)(A)(ii)(p)	Covered Functions	posting entries to a member's books and records in connection with the covered functions to ensure integrity and compliance with the federal securities laws and regulations and FINRA rules.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1220(b)(3)(B)	Qualifications	See fDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2010	STANDARDS OF COMMERCIAL HONOR AND PRINCIPLES OF TRADE	A member, in the conduct of its business, shall observe high standards of commercial honor and just and equitable principles of trade.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110	Supervision	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(a)	Supervisory System	Each member shall establish and maintain a system to supervise the activities of each associated person that is reasonably designed to achieve compliance with applicable securities laws and regulations, and with applicable FINRA rules. Final responsibility for proper supervision shall rest with the member. A member's supervisory system shall provide, at a minimum, for the following:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(a)(1)	Supervisory System	The establishment and maintenance of written procedures as required by this Rule.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(a)(2)	Supervisory System	The designation, where applicable, of an appropriately registered principal(s) with authority to carry out the supervisory responsibilities of the member for each type of business in which it engages for which registration as a broker-dealer is required.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(a)(3)	Supervisory System	The registration and designation as a branch office or an office of supervisory jurisdiction (OSJ) of each location, including the main office, that meets the definitions contained in paragraph (f) of this Rule.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(a)(4)	Supervisory System	The designation of one or more appropriately registered principals in each OSJ and one or more appropriately registered representatives or principals in each non-OSJ branch office with authority to carry out the supervisory responsibilities assigned to that office by the member.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(a)(5)	Supervisory System	The assignment of each registered person to an appropriately registered representative(s) or principal(s) who shall be responsible for supervising that person's activities.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(a)(6)	Supervisory System	The use of reasonable efforts to determine that all supervisory personnel are qualified, either by virtue of experience or training, to carry out their assigned responsibilities.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(a)(7)	Supervisory System	The participation of each registered representative and registered principal, either individually or collectively, no less than annually, in an interview or meeting conducted by persons designated by the member at which compliance matters relevant to the activities of the representative(s) and principal(s) are discussed. Such interview or meeting may occur in conjunction with the discussion of other matters and may be conducted at a central or regional location or at the representative's(') or principal's(') place of business.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(b)	Written Procedures	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(b)(1)	General Requirements	Each member shall establish, maintain, and enforce written procedures to supervise the types of business in which it engages and the activities of its associated persons that are reasonably designed to achieve compliance with applicable securities laws and regulations, and with applicable FINRA rules.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(b)(2)	Review of Member's Investment Banking and Securities Business	The supervisory procedures required by this paragraph (b) shall include procedures for the review by a registered principal, evidenced in writing, of all transactions relating to the investment banking or securities business of the member.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(b)(3)	Reserved	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(b)(4)	Review of Correspondence and Internal Communications	The supervisory procedures required by this paragraph (b) shall include procedures for the review of incoming and outgoing written (including electronic) correspondence and internal communications relating to the member's investment banking or securities business. The supervisory procedures must be appropriate for the member's business, size, structure, and customers. The supervisory procedures must require the member's review of:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(b)(4)(A)	Review of Correspondence and Internal Communications	incoming and outgoing written (including electronic) correspondence to properly identify and handle in accordance with firm procedures, customer complaints, instructions, funds and securities, and communications that are of a subject matter that require review under FINRA rules and federal securities laws.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(b)(4)(B)	Review of Correspondence and Internal Communications	internal communications to properly identify those communications that are of a subject matter that require review under FINRA rules and federal securities laws. Reviews of correspondence and internal communications must be conducted by a registered principal and must be evidenced in writing, either electronically or on paper.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(b)(5)	Review of Customer Complaints	The supervisory procedures required by this paragraph (b) shall include procedures to capture, acknowledge, and respond to all written (including electronic) customer complaints.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(b)(6)	Documentation and Supervision of Supervisory Personnel	The supervisory procedures required by this paragraph (b) shall set forth the supervisory system established by the member pursuant to paragraph (a) above, and shall include:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(b)(6)(A)	Documentation and Supervision of Supervisory Personnel	the titles, registration status, and locations of the required supervisory personnel and the responsibilities of each supervisory person as these relate to the types of business engaged in, applicable securities laws and regulations, and FINRA rules.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(b)(6)(B)	Documentation and Supervision of Supervisory Personnel	a record, preserved by the member for a period of not less than three years, the first two years in an easily accessible place, of the names of all persons who are designated as supervisory personnel and the dates for which such designation is or was effective.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(b)(6)(C)	Documentation and Supervision of Supervisory Personnel	procedures prohibiting associated persons who perform a supervisory function from:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(b)(6)(C)(i)	Documentation and Supervision of Supervisory Personnel	supervising their own activities; and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(b)(6)(C)(ii)	Documentation and Supervision of Supervisory Personnel	reporting to, or having their compensation or continued employment determined by, a person or persons they are supervising.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(b)(6)(C)(ii)(a)	Documentation and Supervision of Supervisory Personnel	if a member determines, with respect to any of its supervisory personnel, that compliance with subparagraph (i) or (ii) above is not possible because of the member's size or a supervisory personnel's position within the firm, the member must document:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(b)(6)(C)(ii)(a)(1)	Documentation and Supervision of Supervisory Personnel	the factors the member used to reach such determination; and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(b)(6)(C)(ii)(a)(2)	Documentation and Supervision of Supervisory Personnel	how the supervisory arrangement with respect to such supervisory personnel otherwise complies with paragraph (a) of this Rule.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
3110(b)(6)(D)	Documentation and Supervision of Supervisory Personnel	procedures reasonably designed to prevent the supervisory system required pursuant to paragraph (a) of this Rule from being compromised due to the conflicts of interest that may be present with respect to the associated person being supervised, including the position of such person, the revenue such person generates for the firm, or any compensation that the associated person conducting the supervision may derive from the associated person being supervised.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(b)(7)	Maintenance of Written Supervisory Procedures	A copy of a member's written supervisory procedures, or the relevant portions thereof, shall be kept and maintained in each OSJ and at each location where supervisory activities are conducted on behalf of the member. Each member shall promptly amend its written supervisory procedures to reflect changes in applicable securities laws or regulations, including FINRA rules, and as changes occur in its supervisory system. Each member is responsible for promptly communicating its written supervisory procedures and amendments to all associated persons to whom such written supervisory procedures and amendments are relevant based on their activities and responsibilities.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(c)	Internal Inspections	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(c)(1)	Internal Inspections	Each member shall conduct a review, at least annually (on a calendar-year basis), of the businesses in which it engages. The review shall be reasonably designed to assist the member in detecting and preventing violations of, and achieving compliance with, applicable securities laws and regulations, and with applicable FINRA rules. Each member shall review the activities of each office, which shall include the periodic examination of customer accounts to detect and prevent irregularities or abuses. Each member shall also retain a written record of the date upon which each review and inspection is conducted.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(c)(1)(A)	Internal Inspections	Each member shall inspect at least annually (on a calendar-year basis) every OSJ and any branch office that supervises one or more non-branch locations.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(c)(1)(B)	Internal Inspections	Each member shall inspect at least every three years every branch office that does not supervise one or more non-branch locations. In establishing how often to inspect each non-supervisory branch office, the member shall consider whether the nature and complexity of the securities activities for which the location is responsible, the volume of business done at the location, and the number of associated persons assigned to the location require the non-supervisory branch office to be inspected more frequently than every three years. If a member establishes a more frequent inspection cycle, the member must ensure that at least every three years, the inspection requirements enumerated in paragraph (c)(2) have been met. The member's written supervisory and inspection procedures shall set forth the non-supervisory branch office examination cycle, an explanation of the factors the member used in determining the frequency of the examinations in the cycle, and the manner in which a member will comply with paragraph (c)(2) if using more frequent inspections than every three years.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(c)(1)(C)	Internal Inspections	Each member shall inspect on a regular periodic schedule every non-branch location. In establishing such schedule, the member shall consider the nature and complexity of the securities activities for which the location is responsible and the nature and extent of contact with customers. The member's written supervisory and inspection procedures shall set forth the schedule and an explanation regarding how the member determined the frequency of the examination.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(c)(2)	Internal Inspections	An inspection and review by a member pursuant to paragraph (c)(1) must be reduced to a written report and kept on file by the member for a minimum of three years, unless the inspection is being conducted pursuant to paragraph (c)(1)(C) and the regular periodic schedule is longer than a three-year cycle, in which case the report must be kept on file at least until the next inspection report has been written.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(c)(2)(A)	Internal Inspections	If applicable to the location being inspected, that location's written inspection report must include, without limitation, the testing and verification of the member's policies and procedures, including supervisory policies and procedures in the following areas:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(c)(2)(A)(i)	Internal Inspections	safeguarding of customer funds and securities;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(c)(2)(A)(ii)	Internal Inspections	maintaining books and records;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(c)(2)(A)(iii)	Internal Inspections	supervision of supervisory personnel;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(c)(2)(A)(iv)	Internal Inspections	transmittals of funds (e.g., wires or checks, etc.) or securities from customers to third party accounts; from customer accounts to outside entities (e.g., banks, investment companies, etc.); from customer accounts to locations other than a customer's primary residence (e.g., post office box, "in care of" accounts, alternate address, etc.); and between customers and registered representatives, including the hand-delivery of checks; and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(c)(2)(A)(v)	Internal Inspections	changes of customer account information, including address and investment objectives changes and validation of such changes.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(c)(2)(B)	Internal Inspections	The policies and procedures required by paragraph (c)(2)(A)(iv) must include a means or method of customer confirmation, notification, or follow-up that can be documented. Members may use reasonable risk-based criteria to determine the authenticity of the transmittal instructions.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(c)(2)(C)	Internal Inspections	The policies and procedures required by paragraph (c)(2)(A)(v) must include, for each change processed, a means or method of customer confirmation, notification, or follow-up that can be documented and that complies with SEA Rules 17a-3(a)(17)(i)(B)(2) and 17a-3(a)(17)(i)(B)(3).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(c)(2)(D)	Internal Inspections	If a member does not engage in all of the activities enumerated in paragraphs (c)(2)(A)(i) through (c)(2)(A)(v) at the location being inspected, the member must identify those activities in the member's written supervisory procedures or the location's written inspection report and document in the member's written supervisory procedures or the location's written inspection report that supervisory policies and procedures for such activities must be in place at that location before the member can engage in them.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(c)(3)	Internal Inspections	For each inspection conducted pursuant to paragraph (c), a member must:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(c)(3)(A)	Internal Inspections	have procedures reasonably designed to prevent the effectiveness of the inspections required pursuant to paragraph (c)(1) of this Rule from being compromised due to the conflicts of interest that may be present with respect to the location being inspected, including but not limited to, economic, commercial, or financial interests in the associated persons and businesses being inspected; and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(c)(3)(B)	Internal Inspections	ensure that the person conducting an inspection pursuant to paragraph (c)(1) is not an associated person assigned to the location or is not directly or indirectly supervised by, or otherwise reporting to, an associated person assigned to the location.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(c)(3)(C)	Internal Inspections	If a member determines that compliance with paragraph (c)(3)(B) is not possible either because of a member's size or its business model, the member must document in the inspection report both the factors the member used to make its determination and how the inspection otherwise complies with paragraph (c)(1).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(d)	Transaction Review and Investigation	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(d)(1)	Transaction Review and Investigation	Each member shall include in its supervisory procedures a process for the review of securities transactions that are reasonably designed to identify trades that may violate the provisions of the Exchange Act, the rules thereunder, or FINRA rules prohibiting insider trading and manipulative and deceptive device that are effected for the:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(d)(1)(A)	Transaction Review and Investigation	accounts of the member;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(d)(1)(B)	Transaction Review and Investigation	accounts introduced or carried by the member in which a person associated with the member has a beneficial interest or the authority to make investment decisions;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(d)(1)(C)	Transaction Review and Investigation	accounts of a person associated with the member that are disclosed to the member pursuant to Rule 3210; and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(d)(1)(D)	Transaction Review and Investigation	covered accounts.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(d)(2)	Transaction Review and Investigation	Each member must conduct promptly an internal investigation into any such trade to determine whether a violation of those laws or rules has occurred.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(d)(3)	Transaction Review and Investigation	A member engaging in investment banking services must file with FINRA, written reports, signed by a senior officer of the member, at such times and, without limitation, including such content, as follows:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(d)(3)(A)	Transaction Review and Investigation	within ten business days of the end of each calendar quarter, a written report describing each internal investigation initiated in the previous calendar quarter pursuant to paragraph (d)(2), including the identity of the member, the date each internal investigation commenced, the status of each open internal investigation, the resolution of any internal investigation reached during the previous calendar quarter, and, with respect to each internal investigation, the identity of the security, trades, accounts, associated persons of the member, or associated person of the member's family members holding a covered account, under review, and that includes a copy of the member's policies and procedures required by paragraph (d)(1).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(d)(3)(B)	Transaction Review and Investigation	within five business days of completion of an internal investigation pursuant to paragraph (d)(2) in which it was determined that a violation of the provisions of the Exchange Act, the rules thereunder, or FINRA rules prohibiting insider trading and manipulative and deceptive devices had occurred, a written report detailing the completion of the investigation, including the results of the investigation,any internal disciplinary action taken, and any referral of the matter to FINRA, another self-regulatory organization, the SEC, or any other federal, state, or international regulatory authority.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(d)(4)	Definitions	See fDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(e)	Responsibility of Member to Investigate Applicants for Registration	See fDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3110(f)	Definitions	See fDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
3310	Anti-Money Laundering Compliance Program	Each member shall develop and implement a written anti-money laundering program reasonably designed to achieve and monitor the member's compliance with the requirements of the Bank Secrecy Act (31 U.S.C. 5311, et seq.), and the implementing regulations promulgated thereunder by the Department of the Treasury. Each member's anti-money laundering program must be approved, in writing, by a member of senior management. The anti-money laundering programs required by this Rule shall, at a minimum,	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3310(a)	Anti-Money Laundering Compliance Program	Establish and implement policies and procedures that can be reasonably expected to detect and cause the reporting of transactions required under 31 U.S.C. 5318(g) and the implementing regulations thereunder;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3310(b)	Anti-Money Laundering Compliance Program	Establish and implement policies, procedures, and internal controls reasonably designed to achieve compliance with the Bank Secrecy Act and the implementing regulations thereunder;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3310(c)	Anti-Money Laundering Compliance Program	Provide for annual (on a calendar-year basis) independent testing for compliance to be conducted by member personnel or by a qualified outside party, unless the member does not execute transactions for customers or otherwise hold customer accounts or act as an introducing broker with respect to customer accounts (e.g., engages solely in proprietary trading or conducts business only with other broker-dealers), in which case such "independent testing" is required every two years (on a calendar-year basis);	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3310(d)	Anti-Money Laundering Compliance Program	Designate and identify to FINRA (by name, title, mailing address, e-mail address, telephone number, and facsimile number) an individual or individuals responsible for implementing and monitoring the day-to-day operations and internal controls of the program (such individual or individuals must be an associated person of the member) and provide prompt notification to FINRA regarding any change in such designation(s);	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3310(e)	Anti-Money Laundering Compliance Program	Provide ongoing training for appropriate personnel; and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3310(f)	Anti-Money Laundering Compliance Program	Include appropriate risk-based procedures for conducting ongoing customer due diligence, to include, but not be limited to:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3310(f)(i)	Anti-Money Laundering Compliance Program	Understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3310(f)(ii)	Anti-Money Laundering Compliance Program	Conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information. For purposes of paragraph (f)(ii), customer information shall include information regarding the beneficial owners of legal entity customers (as defined in 31 CFR 1010.230(e)).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3120	Supervisory Control System	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3120(a)	Supervisory Control System	Each member shall designate and specifically identify to FINRA one or more principals who shall establish, maintain, and enforce a system of supervisory control policies and procedures that:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3120(a)(1)	Supervisory Control System	test and verify that the member's supervisory procedures are reasonably designed with respect to the activities of the member and its associated persons, to achieve compliance with applicable securities laws and regulations, and with applicable FINRA rules; and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3120(a)(2)	Supervisory Control System	create additional or amend supervisory procedures where the need is identified by such testing and verification. The designated principal or principals must submit to the member's senior management no less than annually, a report detailing each member's system of supervisory controls, the summary of the test results and significant identified exceptions, and any additional or amended supervisory procedures created in response to the test results.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3120(b)	Supervisory Control System	Each report provided to senior management pursuant to paragraph (a) in the calendar year following a calendar year in which a member reported $200 million or more in gross revenue must include, to the extent applicable to the member's business:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3120(b)(1)	Supervisory Control System	a tabulation of the reports pertaining to customer complaints and internal investigations made to FINRA during the preceding year; and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3120(b)(2)	Supervisory Control System	discussion of the preceding year's compliance efforts, including procedures and educational programs, in each of the following areas:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3120(b)(2)(A)	Supervisory Control System	trading and market activities;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3120(b)(2)(B)	Supervisory Control System	investment banking activities;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3120(b)(2)(C)	Supervisory Control System	antifraud and sales practices;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3120(b)(2)(D)	Supervisory Control System	finance and operations;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3120(b)(2)(E)	Supervisory Control System	supervision; and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3120(b)(2)(F)	Supervisory Control System	anti-money laundering.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3120(c)	Supervisory Control System	For purposes of paragraph (b), "gross revenue" is defined as:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3120(c)(1)	Supervisory Control System	total revenue as reported on FOCUS Form Part II or IIA (line item 4030) less commodities revenue (line item 3990), if applicable; or	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3120(c)(2)	Supervisory Control System	total revenue as reported on FOCUS Form Part II CSE (line item 4030) less, if applicable, (A) commissions on commodity transactions (line item 3991); and (B) commodities gains or losses (line items 3924 and 3904).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4370	Business Continuity Plans and Emergency Contact Information	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4370(a)	Business Continuity Plans and Emergency Contact Information	Each member must create and maintain a written business continuity plan identifying procedures relating to an emergency or significant business disruption. Such procedures must be reasonably designed to enable the member to meet its existing obligations to customers. In addition, such procedures must address the member's existing relationships with other broker-dealers and counter-parties. The business continuity plan must be made available promptly upon request to FINRA staff.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4370(b)	Business Continuity Plans and Emergency Contact Information	Each member must update its plan in the event of any material change to the member's operations, structure, business or location. Each member must also conduct an annual review of its business continuity plan to determine whether any modifications are necessary in light of changes to the member's operations, structure, business, or location.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4370(c)	Business Continuity Plans and Emergency Contact Information	The elements that comprise a business continuity plan are flexible and may be tailored to the size and needs of a member. Each plan, however, must at a minimum, address: Each member must address the above-listed categories to the extent applicable and necessary. If any of the above-listed categories is not applicable, the member's business continuity plan need not address the category. The member's business continuity plan, however, must document the rationale for not including such category in its plan. If a member relies on another entity for any one of the above-listed categories or any mission critical system, the member's business continuity plan must address this relationship.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4370(c)(1)	Business Continuity Plans and Emergency Contact Information	Data back-up and recovery (hard copy and electronic);	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4370(c)(2)	Business Continuity Plans and Emergency Contact Information	All mission critical systems;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4370(c)(3)	Business Continuity Plans and Emergency Contact Information	Financial and operational assessments;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4370(c)(4)	Business Continuity Plans and Emergency Contact Information	Alternate communications between customers and the member;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4370(c)(5)	Business Continuity Plans and Emergency Contact Information	Alternate communications between the member and its employees;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4370(c)(6)	Business Continuity Plans and Emergency Contact Information	Alternate physical location of employees;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4370(c)(7)	Business Continuity Plans and Emergency Contact Information	Critical business constituent, bank, and counter-party impact;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4370(c)(8)	Business Continuity Plans and Emergency Contact Information	Regulatory reporting;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4370(c)(9)	Business Continuity Plans and Emergency Contact Information	Communications with regulators; and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4370(c)(10)	Business Continuity Plans and Emergency Contact Information	How the member will assure customers' prompt access to their funds and securities in the event that the member determines that it is unable to continue its business.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4370(d)	Business Continuity Plans and Emergency Contact Information	Members must designate a member of senior management to approve the plan and he or she shall be responsible for conducting the required annual review. The member of senior management must also be a registered principal.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4370(e)	Business Continuity Plans and Emergency Contact Information	Each member must disclose to its customers how its business continuity plan addresses the possibility of a future significant business disruption and how the member plans to respond to events of varying scope. At a minimum, such disclosure must be made in writing to customers at account opening, posted on the member's Web site (if the member maintains a Web site), and mailed to customers upon request.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4370(f)(1)	Business Continuity Plans and Emergency Contact Information	Each member shall report to FINRA, via such electronic or other means as FINRA may specify, prescribed emergency contact information for the member. The emergency contact information for the member includes designation of two associated persons as emergency contact persons. At least one emergency contact person shall be a member of senior management and a registered principal of the member. If a member designates a second emergency contact person who is not a registered principal, such person shall be a member of senior management who has knowledge of the member's business operations. A member with only one associated person shall designate as a second emergency contact person an individual, either registered with another firm or nonregistered, who has knowledge of the member's business operations (e.g., the member's attorney, accountant, or clearing firm contact).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
4370(f)(2)	Business Continuity Plans and Emergency Contact Information	Each member must promptly update its emergency contact information, via such electronic or other means as FINRA may specify, in the event of any material change. With respect to the designated emergency contact persons, each member must identify, review, and, if necessary, update such designations in the manner prescribed by Rule 4517.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4370(g)	Business Continuity Plans and Emergency Contact Information	For purposes of this Rule, the following terms shall have the meanings specified below:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4370(g)(1)	Business Continuity Plans and Emergency Contact Information	"Mission critical system" means any system that is necessary, depending on the nature of a member's business, to ensure prompt and accurate processing of securities transactions, including, but not limited to, order taking, order entry, execution, comparison, allocation, clearance and settlement of securities transactions, the maintenance of customer accounts, access to customer accounts and the delivery of funds and securities.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4370(g)(2)	Business Continuity Plans and Emergency Contact Information	"Financial and operational assessment" means a set of written procedures that allow a member to identify changes in its operational, financial, and credit risk exposures.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4530	Reporting Requirements	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4530(a)	Reporting Requirements	Each member shall promptly report to FINRA, but in any event not later than 30 calendar days, after the member knows or should have known of the existence of any of the following:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4530(a)(1)	Reporting Requirements	the member or an associated person of the member:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4530(a)(1)(A)	Reporting Requirements	has been found to have violated any securities-, insurance-, commodities-, financial- or investment-related laws, rules, regulations or standards of conduct of any domestic or foreign regulatory body, self-regulatory organization or business or professional organization;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4530(a)(1)(B)	Reporting Requirements	is the subject of any written customer complaint involving allegations of theft or misappropriation of funds or securities or of forgery;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4530(a)(1)(C)	Reporting Requirements	is named as a defendant or respondent in any proceeding brought by a domestic or foreign regulatory body or self-regulatory organization alleging the violation of any provision of the Exchange Act, or of any other federal, state or foreign securities, insurance or commodities statute, or of any rule or regulation thereunder, or of any provision of the by-laws, rules or similar governing instruments of any securities, insurance or commodities domestic or foreign regulatory body or self-regulatory organization;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4530(a)(1)(D)	Reporting Requirements	is denied registration or is expelled, enjoined, directed to cease and desist, suspended or otherwise disciplined by any securities, insurance or commodities industry domestic or foreign regulatory body or self-regulatory organization or is denied membership or continued membership in any such self-regulatory organization; or is barred from becoming associated with any member of any such self-regulatory organization;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4530(a)(1)(E)	Reporting Requirements	is indicted, or convicted of, or pleads guilty to, or pleads no contest to, any felony; or any misdemeanor that involves the purchase or sale of any security, the taking of a false oath, the making of a false report, bribery, perjury, burglary, larceny, theft, robbery, extortion, forgery, counterfeiting, fraudulent concealment, embezzlement, fraudulent conversion, or misappropriation of funds, or securities, or a conspiracy to commit any of these offenses, or substantially equivalent activity in a domestic, military or foreign court;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4530(a)(1)(F)	Reporting Requirements	is a director, controlling stockholder, partner, officer or sole proprietor of, or an associated person with, a broker, dealer, investment company, investment advisor, underwriter or insurance company that was suspended, expelled or had its registration denied or revoked by any domestic or foreign regulatory body, jurisdiction or organization or is associated in such a capacity with a bank, trust company or other financial institution that was convicted of or pleaded no contest to, any felony or misdemeanor in a domestic or foreign court;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4530(a)(1)(G)	Reporting Requirements	is a defendant or respondent in any securities- or commodities-related civil litigation or arbitration, is a defendant or respondent in any financial-related insurance civil litigation or arbitration, or is the subject of any claim for damages by a customer, broker or dealer that relates to the provision of financial services or relates to a financial transaction, and such civil litigation, arbitration or claim for damages has been disposed of by judgment, award or settlement for an amount exceeding $15,000. However, when the member is the defendant or respondent or is the subject of any claim for damages by a customer, broker or dealer, then the reporting to FINRA shall be required only when such judgment, award or settlement is for an amount exceeding $25,000; or	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4530(a)(1)(H)	Reporting Requirements	(i) is subject to a "statutory disqualification" as that term is defined in the Exchange Act; or (ii) is involved in the sale of any financial instrument, the provision of any investment advice or the financing of any such activities with any person that is subject to a "statutory disqualification" as that term is defined in the Exchange Act, provided, however, that this requirement shall not apply to activities with a member or an associated person that has been approved (or is otherwise permitted pursuant to FINRA rules and the federal securities laws) to be a member or to be associated with a member. The report shall include the name of the person subject to the statutory disqualification and details concerning the disqualification; or	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4530(a)(2)	Reporting Requirements	(2) an associated person of the member is the subject of any disciplinary action taken by the member involving suspension, termination, the withholding of compensation or of any other remuneration in excess of $2,500, the imposition of fines in excess of $2,500 or is otherwise disciplined in any manner that would have a significant limitation on the individual's activities on a temporary or permanent basis.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4530(b)	Reporting Requirements	Each member shall promptly report to FINRA, but in any event not later than 30 calendar days, after the member has concluded or reasonably should have concluded that an associated person of the member or the member itself has violated any securities-, insurance-, commodities-, financial- or investment-related laws, rules, regulations or standards of conduct of any domestic or foreign regulatory body or self-regulatory organization.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4530(c)	Reporting Requirements	Each person associated with a member shall promptly report to the member the existence of any of the events set forth in paragraph (a)(1) of this Rule.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4530(d)	Reporting Requirements	Each member shall report to FINRA statistical and summary information regarding written customer complaints in such detail as FINRA shall specify by the 15th day of the month following the calendar quarter in which customer complaints are received by the member.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4530(e)	Reporting Requirements	Nothing contained in this Rule shall eliminate, reduce or otherwise abrogate the responsibilities of a member or person associated with a member to promptly disclose required information on the Forms BD, U4 or U5, as applicable, to make any other required filings or to respond to FINRA with respect to any customer complaint, examination or inquiry. In addition, members are required to comply with the reporting obligations under paragraphs (a), (b) and (d) of this Rule, regardless of whether the information is reported or disclosed pursuant to any other rule or requirement, including the requirements of the Form BD. However, a member need not report: (1) an event otherwise required to be reported under paragraph (a)(1) of this Rule if the member discloses the event on the Form U4, consistent with the requirements of that form, and indicates, in such manner and format that FINRA may require, that such disclosure satisfies the requirements of paragraph (a)(1) of this Rule, as applicable; or (2) an event otherwise required to be reported under paragraphs (a) or (b) of this Rule if the member discloses the event on the Form U5, consistent with the requirements of that form.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4530(f)	Reporting Requirements	Each member shall promptly file with FINRA copies of:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4530(f)(1)	Reporting Requirements	any indictment, information or other criminal complaint or plea agreement for conduct reportable under paragraph (a)(1)(E) of this Rule;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4530(f)(2)	Reporting Requirements	any complaint in which a member is named as a defendant or respondent in any securities- or commodities-related private civil litigation, or is named as a defendant or respondent in any financial-related insurance private civil litigation;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4530(f)(3)	Reporting Requirements	any securities- or commodities-related arbitration claim, or financial-related insurance arbitration claim, filed against a member in any forum other than the FINRA Dispute Resolution forum;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4530(f)(4)	Reporting Requirements	any indictment, information or other criminal complaint, any plea agreement, or any private civil complaint or arbitration claim against a person associated with a member that is reportable under question 14 on Form U4, irrespective of any dollar thresholds Form U4 imposes for notification, unless, in the case of an arbitration claim, the claim has been filed in the FINRA Dispute Resolution forum.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4530(g)	Reporting Requirements	Members may file electronically, in such manner and format as specified by FINRA, the documents required by paragraph (f); provided, however, that the filings shall be accompanied by summary information regarding the documents in such detail as specified by FINRA.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4530(h)	Reporting Requirements	Members shall not be required to comply separately with paragraph (f) in the event that any of the documents required by paragraph (f) have been the subject of a request by FINRA's Credentialing, Registration, Education and Disclosure staff, provided that the member produces those requested documents to the Credentialing, Registration, Education and Disclosure staff not later than 30 days after receipt of such request. This paragraph does not supersede any FINRA rule or policy that requires production of documents specified in paragraph (f) sooner than 30 days after receipt of a request by the Credentialing, Registration, Education and Disclosure staff.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.1	Purpose and scope	See fDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.2	Model privacy form: rule of construction	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.2(a)	Model privacy form	Use of the model privacy form in appendix A to subpart A of this part, consistent with the instructions in appendix A to subpart A, constitutes compliance with the notice content requirements of §§ 248.6 and 248.7 of this part, although use of the model privacy form is not required.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
248.2(b)	Examples	The examples in this part provide guidance concerning the rule's application in ordinary circumstances. The facts and circumstances of each individual situation, however, will determine whether compliance with an example, to the extent practicable, constitutes compliance with this part.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.2(c)	Substituted compliance with CFTC financial privacy rules by futures commission merchants and introducing brokers	Except with respect to § 248.30(b), any futures commission merchant or introducing broker (as those terms are defined in the Commodity Exchange Act (7 U.S.C. 1, et seq.)) registered by notice with the Commission for the purpose of conducting business in security futures products pursuant to section 15(b)(11)(A) of the Securities Exchange Act of 1934 (15 U.S.C. 78o(b)(11)(A)) that is subject to and in compliance with the financial privacy rules of the Commodity Futures Trading Commission (17 CFR part 160) will be deemed to be in compliance with this part.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.3	Definitions	See fDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.4	Initial privacy notice to consumers required	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.4(a)	Initial notice requirement	You must provide a clear and conspicuous notice that accurately reflects your privacy policies and practices to:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.4(a)(1)	Customer	An individual who becomes your customer, not later than when you establish a customer relationship, except as provided in paragraph (e) of this section; and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.4(a)(2)	Consumer	A consumer, before you disclose any nonpublic personal information about the consumer to any nonaffiliated third party, if you make such a disclosure other than as authorized by §§ 248.14 and 248.15.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.4(b)	When initial notice to a consumer is not required	You are not required to provide an initial notice to a consumer under paragraph (a) of this section if:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.4(b)(1)	When initial notice to a consumer is not required	You do not disclose any nonpublic personal information about the consumer to any nonaffiliated third party, other than as authorized by §§ 248.14 and 248.15; and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.4(b)(2)	When initial notice to a consumer is not required	You do not have a customer relationship with the consumer.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.4(c)	When you establish a customer relationship —	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.4(c)(1)	General rule	You establish a customer relationship when you and the consumer enter into a continuing relationship.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.4(c)(2)	Special rule for loans	You do not have a customer relationship with a consumer if you buy a loan made to the consumer but do not have the servicing rights for that loan.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.4(c)(3)	Examples of establishing customer relationship	You establish a customer relationship when the consumer:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.4(c)(3)(i)	Examples of establishing customer relationship	Effects a securities transaction with you or opens a brokerage account with you under your procedures;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.4(c)(3)(ii)	Examples of establishing customer relationship	Opens a brokerage account with an introducing broker or dealer that clears transactions with and for its customers through you on a fully disclosed basis;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.4(c)(3)(iii)	Examples of establishing customer relationship	Enters into an advisory contract with you (whether in writing or orally); or	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.4(c)(3)(iv)	Examples of establishing customer relationship	Purchases shares you have issued (and the consumer is the record owner of the shares), if you are an investment company.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.4(d)	Existing customers	When an existing customer obtains a new financial product or service from you that is to be used primarily for personal, family, or household purposes, you satisfy the initial notice requirements of paragraph (a) of this section as follows:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.4(d)(1)	Existing customers	You may provide a revised privacy notice, under § 248.8, that covers the customer's new financial product or service; or	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.4(d)(2)	Existing customers	If the initial, revised, or annual notice that you most recently provided to that customer was accurate with respect to the new financial product or service, you do not need to provide a new privacy notice under paragraph (a) of this section.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.4(e)	Exceptions to allow subsequent delivery of notice	See fDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.5	Annual privacy notice to customers required	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.5(a)	Annual privacy notice to customers required	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.5(a)(1)	General rule	Except as provided by paragraph (e) of this section, you must provide a clear and conspicuous notice to customers that accurately reflects your privacy policies and practices not less than annually during the continuation of the customer relationship. Annually means at least once in any period of 12 consecutive months during which that relationship exists. You may define the 12-consecutive-month period, but you must apply it to the customer on a consistent basis.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.5(a)(2)	Example	See fDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.5(b)	Annual privacy notice to customers required	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.5(b)(1)	Termination of customer relationship	You are not required to provide an annual notice to a former customer.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.5(b)(2)	Examples	See fDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.5(c)	Special rule for loans	If you do not have a customer relationship with a consumer under the special provision for loans in § 248.4(c)(2), then you need not provide an annual notice to that consumer under this section.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.5(d)	Delivery	When you are required to deliver an annual privacy notice by this section, you must deliver it according to § 248.9.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.5(e)	Exception to annual privacy notice requirement —	See fDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.6	Information to be included in privacy notices	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.6(a)	General rule	The initial, annual, and revised privacy notices that you provide under §§ 248.4, 248.5, and 248.8 must include each of the following items of information that applies to you or to the consumers to whom you send your privacy notice, in addition to any other information you wish to provide:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.6(a)(1)	General rule	The categories of nonpublic personal information that you collect;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.6(a)(2)	General rule	The categories of nonpublic personal information that you disclose;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.6(a)(3)	General rule	The categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information, other than those parties to whom you disclose information under §§ 248.14 and 248.15;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.6(a)(4)	General rule	The categories of nonpublic personal information about your former customers that you disclose and the categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information about your former customers, other than those parties to whom you disclose information under §§ 248.14 and 248.15;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.6(a)(5)	General rule	If you disclose nonpublic personal information to a nonaffiliated third party under § 248.13 (and no other exception applies to that disclosure), a separate statement of the categories of information you disclose and the categories of third parties with whom you have contracted;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.6(a)(6)	General rule	An explanation of the consumer's right under § 248.10(a) 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 at that time;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.6(a)(7)	General rule	Any disclosures that you make under section 603(d)(2)(A)(iii) of the Fair Credit Reporting Act (15 U.S.C. 1681a(d)(2)(A)(iii)) (that is, notices regarding the ability to opt out of disclosures of information among affiliates);	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.6(a)(8)	General rule	Your policies and practices with respect to protecting the confidentiality and security of nonpublic personal information; and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.6(a)(9)	General rule	Any disclosure that you make under paragraph (b) of this section.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.6(b)	Description of nonaffiliated third parties subject to exceptions	If you disclose nonpublic personal information to third parties as authorized under §§ 248.14 and 248.15, you are not required to list those exceptions in the initial or annual privacy notices required by §§ 248.4 and 248.5. When describing the categories with respect to those parties, it is sufficient to state that you make disclosures to other nonaffiliated companies:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.6(b)(1)	Description of nonaffiliated third parties subject to exceptions	For your everyday business purposes such as [include all that apply] to process transactions, maintain account(s), respond to court orders and legal investigations, or report to credit bureaus; or	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.6(b)(2)	Description of nonaffiliated third parties subject to exceptions	As permitted by law.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.6(c)	Examples	See fDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.6(d)	Short-form initial notice with opt out notice for non-customers	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.6(d)(1)	Short-form initial notice with opt out notice for non-customers	You may satisfy the initial notice requirements in §§ 248.4(a)(2), 248.7(b), and 248.7(c) for a consumer who is not a customer by providing a short-form initial notice at the same time as you deliver an opt out notice as required in § 248.7.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.6(d)(2)	Short-form initial notice with opt out notice for non-customers	A short-form initial notice must:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.6(d)(2)(i)	Short-form initial notice with opt out notice for non-customers	Be clear and conspicuous;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.6(d)(2)(ii)	Short-form initial notice with opt out notice for non-customers	State that your privacy notice is available upon request; and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
248.6(d)(2)(iii)	Short-form initial notice with opt out notice for non-customers	Explain a reasonable means by which the consumer may obtain the privacy notice.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.6(d)(3)	Short-form initial notice with opt out notice for non-customers	You must deliver your short-form initial notice according to § 248.9. You are not required to deliver your privacy notice with your short-form initial notice. You instead may simply provide the consumer a reasonable means to obtain your privacy notice. If a consumer who receives your short-form notice requests your privacy notice, you must deliver your privacy notice according to § 248.9.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.6(d)(4)	Examples of obtaining privacy notice	See fDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.6(e)	Future disclosures	Your notice may include:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.6(d)(1)	Future disclosures	Categories of nonpublic personal information that you reserve the right to disclose in the future, but do not currently disclose; and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.6(d)(2)	Future disclosures	Categories of affiliates or nonaffiliated third parties to whom you reserve the right in the future to disclose, but to whom you do not currently disclose, nonpublic personal information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.6(f)	Model privacy form	Pursuant to § 248.2(a) and appendix A to subpart A of this part, Form S-P meets the notice content requirements of this section.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.7	Form of opt out notice to consumers; opt out methods	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.7(a)	Form of opt out notice to consumers; opt out methods	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.7(a)(1)	Form of opt out notice	If you are required to provide an opt out notice under § 248.10(a), you must provide a clear and conspicuous notice to each of your consumers that accurately explains the right to opt out under that section. The notice must state:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.7(a)(1)(i)	Form of opt out notice	That you disclose or reserve the right to disclose nonpublic personal information about your consumer to a nonaffiliated third party;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.7(a)(1)(ii)	Form of opt out notice	That the consumer has the right to opt out of that disclosure; and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.7(a)(1)(iii)	Form of opt out notice	A reasonable means by which the consumer may exercise the opt out right.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.7(a)(2)	Examples	See fDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.7(b)	Same form as initial notice permitted	You may provide the opt out notice together with or on the same written or electronic form as the initial notice you provide in accordance with § 248.4.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.7(c)	Initial notice required when opt out notice delivered subsequent to initial notice	If you provide the opt out notice after the initial notice in accordance with § 248.4, you must also include a copy of the initial notice with the opt out notice in writing or, if the consumer agrees, electronically.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.7(d)	Joint relationships	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.7(d)(1)	Joint relationships	If two or more consumers jointly obtain a financial product or service from you, you may provide a single opt out notice. Your opt out notice must explain how you will treat an opt out direction by a joint consumer.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.7(d)(2)	Joint relationships	Any of the joint consumers may exercise the right to opt out. You may either:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.7(d)(2)(i)	Joint relationships	Treat an opt out direction by a joint consumer as applying to all of the associated joint consumers; or	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.7(d)(2)(ii)	Joint relationships	Permit each joint consumer to opt out separately.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.7(d)(3)	Joint relationships	If you permit each joint consumer to opt out separately, you must permit one of the joint consumers to opt out on behalf of all of the joint consumers.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.7(d)(4)	Joint relationships	You may not require all joint consumers to opt out before you implement any opt out direction.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.7(d)(5)	Example	See fDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.7(e)	Time to comply with opt out	You must comply with a consumer's opt out direction as soon as reasonably practicable after you receive it.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.7(f)	Continuing right to opt out	A consumer may exercise the right to opt out at any time.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.7(g)	Duration of consumer's opt out direction	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.7(g)(1)	Duration of consumer's opt out direction	A consumer's direction to opt out under this section is effective until the consumer revokes it in writing or, if the consumer agrees, electronically.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.7(g)(2)	Duration of consumer's opt out direction	When a customer relationship terminates, the customer's opt out direction continues to apply to the nonpublic personal information that you collected during or related to that relationship. If the individual subsequently establishes a new customer relationship with you, the opt out direction that applied to the former relationship does not apply to the new relationship.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.7(h)	Delivery	When you are required to deliver an opt out notice by this section, you must deliver it according to § 248.9.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.7(i)	Model privacy form	Pursuant to § 248.2(a) and appendix A to subpart A of this part, Form S-P meets the notice content requirements of this section.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.8	Revised privacy notices	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.8(a)	General rule	Except as otherwise authorized in this subpart, you must not, directly or through any affiliate, disclose any nonpublic personal information about a consumer to a nonaffiliated third party other than as described in the initial notice that you provided to that consumer under § 248.4, unless:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.8(a)(1)	General rule	You have provided to the consumer a clear and conspicuous revised notice that accurately describes your policies and practices;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.8(a)(2)	General rule	You have provided to the consumer a new opt out notice;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.8(a)(3)	General rule	You have given the consumer a reasonable opportunity, before you disclose the information to the nonaffiliated third party, to opt out of the disclosure; and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.8(a)(4)	General rule	The consumer does not opt out.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.8(b)	Examples	See fDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.8(c)	Delivery	When you are required to deliver a revised privacy notice by this section, you must deliver it according to § 248.9.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.9	Delivering privacy and opt out notices	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.9(a)	How to provide notices	You must provide any privacy notices and opt out notices, including short-form initial notices that this subpart requires so that each consumer can reasonably be expected to receive actual notice in writing or, if the consumer agrees, electronically.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.9(b)	Delivering privacy and opt out notices	See fDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.9(c)	Annual notices only	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.9(c)(1)	Annual notices only	You may reasonably expect that a customer will receive actual notice of your annual privacy notice if:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.9(c)(1)(i)	Annual notices only	The customer uses your web site to access financial products and services electronically and agrees to receive notices at the web site and you post your current privacy notice continuously in a clear and conspicuous manner on the web site; or	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.9(c)(1)(ii)	Annual notices only	The customer has requested that you refrain from sending any information regarding the customer relationship, and your current privacy notice remains available to the customer upon request.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.9(c)(2)	Example of reasonable expectation of receipt of annual privacy notice	See fDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.9(d)	Oral description of notice insufficient	You may not provide any notice required by this subpart solely by orally explaining the notice, either in person or over the telephone.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.9(e)	Retention or accessibility of notices for customers	For customers only, you must provide the initial notice required by § 248.4(a)(1), the annual notice required by § 248.5(a), and the revised notice required by § 248.8, so that the customer can retain them or obtain them later in writing or, if the customer agrees, electronically.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.9(e)(1)	Retention or accessibility of notices for customers	For customers only, you must provide the initial notice required by § 248.4(a)(1), the annual notice required by § 248.5(a), and the revised notice required by § 248.8, so that the customer can retain them or obtain them later in writing or, if the customer agrees, electronically.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.9(e)(2)	Examples of retention or accessibility	See fDE for details	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.9(f)	Joint notice with other financial institutions	You may provide a joint notice from you and one or more of your affiliates or other financial institutions, as identified in the notice, as long as the notice is accurate with respect to you and the other institutions.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.9(g)	Joint relationships	If two or more consumers jointly obtain a financial product or service from you, you may satisfy the initial, annual, and revised notice requirements of paragraph (a) of this section by providing one notice to those consumers jointly.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.10	Limits on disclosure of nonpublic personal information to nonaffiliated third parties	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.10(a)	Limits on disclosure of nonpublic personal information to nonaffiliated third parties	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.10(a)(1)	Conditions for disclosure	Except as otherwise authorized in this subpart, you may not, directly or through any affiliate, disclose any nonpublic personal information about a consumer to a nonaffiliated third party unless:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.10(a)(1)(i)	Conditions for disclosure	You have provided to the consumer an initial notice as required under § 248.4;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.10(a)(1)(ii)	Conditions for disclosure	You have provided to the consumer an opt out notice as required in § 248.7;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.10(a)(1)(iii)	Conditions for disclosure	You have given the consumer a reasonable opportunity, before you disclose the information to the nonaffiliated third party, to opt out of the disclosure; and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.10(a)(1)(iv)	Conditions for disclosure	The consumer does not opt out.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.10(a)(2)	Opt out definition	See fDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.10(a)(3)	Examples of reasonable opportunity to opt out	See fDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
248.10(b)	Application of opt out to all consumers and all nonpublic personal information	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.10(b)(1)	Application of opt out to all consumers and all nonpublic personal information	You must comply with this section, regardless of whether you and the consumer have established a customer relationship.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.10(b)(2)	Application of opt out to all consumers and all nonpublic personal information	Unless you comply with this section, you may not, directly or through any affiliate, disclose any nonpublic personal information about a consumer that you have collected, regardless of whether you collected it before or after receiving the direction to opt out from the consumer.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.10(c)	Partial opt out	You may allow a consumer to select certain nonpublic personal information or certain nonaffiliated third parties with respect to which the consumer wishes to opt out.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.11	Limits on redisclosure and reuse of information	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.11(a)	Limits on redisclosure and reuse of information	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.11(a)(1)	Information you receive under an exception	If you receive nonpublic personal information from a nonaffiliated financial institution under an exception in § 248.14 or § 248.15, your disclosure and use of that information is limited as follows:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.11(a)(1)(i)	Information you receive under an exception	You may disclose the information to the affiliates of the financial institution from which you received the information;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.11(a)(1)(ii)	Information you receive under an exception	You may disclose the information to your affiliates, but your affiliates may, in turn, disclose and use the information only to the extent that you may disclose and use the information; and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.11(a)(1)(iii)	Information you receive under an exception	You may disclose and use the information pursuant to an exception in § 248.14 or § 248.15 in the ordinary course of business to carry out the activity covered by the exception under which you received the information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.11(a)(2)	Example	See fDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.11(b)	Limits on redisclosure and reuse of information	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.11(b)(1)	Information you receive outside of an exception	If you receive nonpublic personal information from a nonaffiliated financial institution other than under an exception in § 248.14 or § 248.15, you may disclose the information only:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.11(b)(1)(i)	Information you receive outside of an exception	To the affiliates of the financial institution from which you received the information;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.11(b)(1)(ii)	Information you receive outside of an exception	To your affiliates, but your affiliates may, in turn, disclose the information only to the extent that you can disclose the information; and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.11(b)(1)(iii)	Information you receive outside of an exception	To any other person, if the disclosure would be lawful if made directly to that person by the financial institution from which you received the information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.11(b)(2)	Example	See fDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.11(c)	Information you disclose under an exception	If you disclose nonpublic personal information to a nonaffiliated third party under an exception in § 248.14 or § 248.15, the third party may disclose and use that information only as follows:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.11(c)(1)	Information you disclose under an exception	The third party may disclose the information to your affiliates;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.11(c)(2)	Information you disclose under an exception	The third party may disclose the information to its affiliates, but its affiliates may, in turn, disclose and use the information only to the extent that the third party may disclose and use the information; and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.11(c)(3)	Information you disclose under an exception	The third party may disclose and use the information pursuant to an exception in § 248.14 or § 248.15 in the ordinary course of business to carry out the activity covered by the exception under which it received the information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.11(d)	Information you disclose outside of an exception	If you disclose nonpublic personal information to a nonaffiliated third party other than under an exception in § 248.14 or § 248.15, the third party may disclose the information only:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.11(d)(1)	Information you disclose outside of an exception	To your affiliates;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.11(d)(2)	Information you disclose outside of an exception	To its affiliates, but its affiliates, in turn, may disclose the information only to the extent the third party can disclose the information; and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.11(d)(3)	Information you disclose outside of an exception	To any other person, if the disclosure would be lawful if you made it directly to that person.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.12	Limits on sharing account number information for marketing purposes	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.12(a)	General prohibition on disclosure of account numbers	You must not, directly or through an affiliate, disclose, other than to a consumer reporting agency, an account number or similar form of access number or access code for a consumer's credit card account, deposit account, or transaction account to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.12(b)	Exceptions	See fDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.12(c)	Example—Account number	See fDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.13	Exception to opt out requirements for service providers and joint marketing	See fDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.14	Exceptions to notice and opt out requirements for processing and servicing transactions	See fDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.15	Other exceptions to notice and opt out requirements	See fDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.16	Protection of Fair Credit Reporting Act	Nothing in this subpart shall be construed to modify, limit, or supersede the operation of the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), and no inference shall be drawn on the basis of the provisions of this subpart regarding whether information is transaction or experience information under section 603 of that Act.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.17	Relation to State laws	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.17(a)	In general	This subpart shall not be construed as superseding, altering, or affecting any statute, regulation, order, or interpretation in effect in any State, except to the extent that such State statute, regulation, order, or interpretation is inconsistent with the provisions of this subpart, and then only to the extent of the inconsistency.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.17(b)	Greater protection under State law	For purposes of this section, a State statute, regulation, order, or interpretation is not inconsistent with the provisions of this subpart if the protection such statute, regulation, order, or interpretation affords any consumer is greater than the protection provided under this subpart, as determined by the Consumer Financial Protection Bureau, after consultation with the Commission, on theConsumer Financial Protection Bureau's own motion, or upon the petition of any interested party.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.18	Effective date; transition rule	See fDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.19-248.29	[Reserved]	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.30	Procedures to safeguard customer information, including response programs for unauthorized access to customer information and customer notice; disposal of customer information and consumer information	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.30(a)	Policies and procedures to safeguard customer information —	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.30(a)(1)	General requirements	Every covered institution must develop, implement, and maintain written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer information.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
248.30(a)(2)	Objectives	These written policies and procedures must be reasonably designed to:	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
248.30(a)(2)(i)	Objectives	Ensure the security and confidentiality of customer information;	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
248.30(a)(2)(ii)	Objectives	Protect against any anticipated threats or hazards to the security or integrity of customer information; and	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
248.30(a)(2)(iii)	Objectives	Protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.	Functional	Intersects With	Sensitive / Regulated Data Access Enforcement	CFG-08	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to restrict access to sensitive/regulated data.	8	
248.30(a)(2)(iii)	Objectives	Protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
248.30(a)(2)(iii)	Objectives	Protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	8	
248.30(a)(3)	Response programs for unauthorized access to or use of customer information	Written policies and procedures in paragraph (a)(1) of this section must include a program reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information, including customer notification procedures. This response program must include procedures for the covered institution to:	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	
248.30(a)(3)	Response programs for unauthorized access to or use of customer information	Written policies and procedures in paragraph (a)(1) of this section must include a program reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information, including customer notification procedures. This response program must include procedures for the covered institution to:	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover:(1) Preparation;(2) Automated event detection or manual incident report intake;(3) Analysis;(4) Containment;(5) Eradication; and(6) Recovery.	8	
248.30(a)(3)	Response programs for unauthorized access to or use of customer information	Written policies and procedures in paragraph (a)(1) of this section must include a program reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information, including customer notification procedures. This response program must include procedures for the covered institution to:	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
248.30(a)(3)(i)	Response programs for unauthorized access to or use of customer information	Assess the nature and scope of any incident involving unauthorized access to or use of customer information and identify the customer information systems and types of customer information that may have been accessed or used without authorization;	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover:(1) Preparation;(2) Automated event detection or manual incident report intake;(3) Analysis;(4) Containment;(5) Eradication; and(6) Recovery.	10	
248.30(a)(3)(i)	Response programs for unauthorized access to or use of customer information	Assess the nature and scope of any incident involving unauthorized access to or use of customer information and identify the customer information systems and types of customer information that may have been accessed or used without authorization;	Functional	Intersects With	Incident Classification & Prioritization	IRO-02.4	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	8	
248.30(a)(3)(ii)	Response programs for unauthorized access to or use of customer information	Take appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information; and	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover:(1) Preparation;(2) Automated event detection or manual incident report intake;(3) Analysis;(4) Containment;(5) Eradication; and(6) Recovery.	10	
248.30(a)(3)(iii)	Response programs for unauthorized access to or use of customer information	Notify each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization in accordance with paragraph (a)(4) of this section unless the covered institution determines, after a reasonable investigation of the facts and circumstances of the incident of unauthorized access to or use of sensitive customer information, that the sensitive customer information has not been, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	5	
248.30(a)(4)	Notifying affected individuals of unauthorized access or use —	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.30(a)(4)(i)	Notification obligation	Unless a covered institution has determined, after a reasonable investigation of the facts and circumstances of the incident of unauthorized access to or use of sensitive customer information that occurred at the covered institution or one of its service providers that is not itself a covered institution, that sensitive customer information has not been, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience, the covered institution must provide a clear and conspicuous notice, or ensure that such notice is provided, to each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization. The notice must be transmitted by a means designed to ensure that each affected individual can reasonably be expected to receive actual notice in writing.	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
248.30(a)(4)(i)	Notification obligation	Unless a covered institution has determined, after a reasonable investigation of the facts and circumstances of the incident of unauthorized access to or use of sensitive customer information that occurred at the covered institution or one of its service providers that is not itself a covered institution, that sensitive customer information has not been, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience, the covered institution must provide a clear and conspicuous notice, or ensure that such notice is provided, to each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization. The notice must be transmitted by a means designed to ensure that each affected individual can reasonably be expected to receive actual notice in writing.	Functional	Intersects With	Public Relations & Reputation Repair	IRO-16	Mechanisms exist to proactively manage public relations associated with incidents and employ appropriate measures to prevent further reputational damage and develop plans to repair any damage to the organization's reputation.	8	
248.30(a)(4)(ii)	Affected individuals	If an incident of unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred, but the covered institution is unable to identify which specific individuals' sensitive customer information has been accessed or used without authorization, the covered institution must provide notice to all individuals whose sensitive customer information resides in the customer information system that was, or was reasonably likely to have been, accessed or used without authorization. Notwithstanding the foregoing, if the covered institution reasonably determines that a specific individual's sensitive customer information that resides in the customer information system was not accessed or used without authorization, the covered institution is not required to provide notice to that individual under this paragraph.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	5	
248.30(a)(4)(iii)	Timing	A covered institution must provide the notice as soon as practicable, but not later than 30 days, after becoming aware that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred unless the United States Attorney General determines that the notice required under this rule poses a substantial risk to national security or public safety, and notifies the Commission of such determination in writing, in which case the covered institution may delay providing such notice for a time period specified by the Attorney General, up to 30 days following the date when such notice was otherwise required to be provided. The notice may be delayed for an additional period of up to 30 days if the Attorney General determines that the notice continues to pose a substantial risk to national security or public safety and notifies the Commission of such determination in writing. In extraordinary circumstances, notice required under this section may be delayed for a final additional period of up to 60 days if the Attorney General determines that such notice continues to pose a substantial risk to national security and notifies the Commission of such determination in writing. Beyond the final 60-day delay under this paragraph (a)(4)(iii), if the Attorney General indicates that further delay is necessary, the Commission will consider additional requests for delay and may grant such delay through Commission exemptive order or other action.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	5	
248.30(a)(4)(iv)	Notice contents	The notice must:	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
248.30(a)(4)(iv)(A)	Notice contents	Describe in general terms the incident and the type of sensitive customer information that was or is reasonably believed to have been accessed or used without authorization;	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
248.30(a)(4)(iv)(B)	Notice contents	Include, if the information is reasonably possible to determine at the time the notice is provided, any of the following: the date of the incident, the estimated date of the incident, or the date range within which the incident occurred;	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
248.30(a)(4)(iv)(C)	Notice contents	Include contact information sufficient to permit an affected individual to contact the covered institution to inquire about the incident, including the following: a telephone number (which should be a toll-free number if available), an email address or equivalent method or means, a postal address, and the name of a specific office to contact for further information and assistance;	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
248.30(a)(4)(iv)(D)	Notice contents	If the individual has an account with the covered institution, recommend that the customer review account statements and immediately report any suspicious activity to the covered institution;	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
248.30(a)(4)(iv)(E)	Notice contents	Explain what a fraud alert is and how an individual may place a fraud alert in the individual's credit reports to put the individual's creditors on notice that the individual may be a victim of fraud, including identity theft;	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
248.30(a)(4)(iv)(F)	Notice contents	Recommend that the individual periodically obtain credit reports from each nationwide credit reporting company and that the individual have information relating to fraudulent transactions deleted;	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
248.30(a)(4)(iv)(G)	Notice contents	Explain how the individual may obtain a credit report free of charge; and	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
248.30(a)(4)(iv)(H)	Notice contents	Include information about the availability of online guidance from the Federal Trade Commission and usa.gov regarding steps an individual can take to protect against identity theft, a statement encouraging the individual to report any incidents of identity theft to the Federal Trade Commission, and include the Federal Trade Commission's website address where individuals may obtain government information about identity theft and report suspected incidents of identity theft.	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
248.30(a)(5)	Service providers	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.30(a)(5)(i)	Service providers	A covered institution's response program prepared in accordance with paragraph (a)(3) of this section must include the establishment, maintenance, and enforcement of written policies and procedures reasonably designed to require oversight, including through due diligence and monitoring, of service providers, including to ensure that the covered institution notifies affected individuals as set forth in paragraph (a)(4) of this section. The policies and procedures must be reasonably designed to ensure service providers take appropriate measures to:	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
248.30(a)(5)(i)(A)	Service providers	Protect against unauthorized access to or use of customer information; and	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
248.30(a)(5)(i)(B)	Service providers	Provide notification to the covered institution as soon as possible, but no later than 72 hours after becoming aware that a breach in security has occurred resulting in unauthorized access to a customer information system maintained by the service provider. Upon receipt of such notification, the covered institution must initiate its incident response program adopted pursuant to paragraph (a)(3) of this section.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	5	
248.30(a)(5)(ii)	Service providers	As part of its incident response program, a covered institution may enter into a written agreement with its service provider to notify affected individuals on the covered institution's behalf in accordance with paragraph (a)(4) of this section.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	5	
248.30(a)(5)(ii)	Service providers	As part of its incident response program, a covered institution may enter into a written agreement with its service provider to notify affected individuals on the covered institution's behalf in accordance with paragraph (a)(4) of this section.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
248.30(a)(5)(iii)	Service providers	Notwithstanding a covered institution's use of a service provider in accordance with paragraphs (a)(5)(i) and (ii) of this section, the obligation to ensure that affected individuals are notified in accordance with paragraph (a)(4) of this section rests with the covered institution.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
248.30(b)	Disposal of consumer information and customer information —	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.30(b)(1)	Standard	Every covered institution, other than notice-registered broker-dealers, must properly dispose of consumer information and customer information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.	Functional	Subset Of	Information Disposal	DCH-21	Mechanisms exist to securely dispose of, destroy or erase information.	10	
248.30(b)(2)	Written policies, procedures, and records	Every covered institution, other than notice-registered broker-dealers, must adopt and implement written policies and procedures that address the proper disposal of consumer information and customer information according to the standard identified in paragraph (b)(1) of this section.	Functional	Subset Of	Information Disposal	DCH-21	Mechanisms exist to securely dispose of, destroy or erase information.	10	
248.30(b)(3)	Relation to other laws	Nothing in this paragraph (b) shall be construed:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.30(b)(3)(i)	Relation to other laws	To require any covered institution to maintain or destroy any record pertaining to an individual that is not imposed under other law; or	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.30(b)(3)(ii)	Relation to other laws	To alter or affect any requirement imposed under any other provision of law to maintain or destroy records.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.30(c)	Recordkeeping	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.30(c)(1)	Recordkeeping	Every covered institution that is an investment company under the Investment Company Act of 1940 (15 U.S.C. 80a), but is not registered under section 8 thereof (15 U.S.C. 80a-8), must make and maintain:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.30(c)(1)(i)	Recordkeeping	The written policies and procedures required to be adopted and implemented pursuant to paragraph (a)(1) of this section;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.30(c)(1)(ii)	Recordkeeping	The written documentation of any detected unauthorized access to or use of customer information, as well as any response to, and recovery from such unauthorized access to or use of customer information required by paragraph (a)(3) of this section;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.30(c)(1)(iii)	Recordkeeping	The written documentation of any investigation and determination made regarding whether notification is required pursuant to paragraph (a)(4) of this section, including the basis for any determination made, any written documentation from the United States Attorney General related to a delay in notice, as well as a copy of any notice transmitted following such determination;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.30(c)(1)(iv)	Recordkeeping	The written policies and procedures required to be adopted and implemented pursuant to paragraph (a)(5)(i) of this section;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.30(c)(1)(v)	Recordkeeping	The written documentation of any contract or agreement entered into pursuant to paragraph (a)(5) of this section; and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.30(c)(1)(vi)	Recordkeeping	The written policies and procedures required to be adopted and implemented pursuant to paragraph (b)(2) of this section.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.30(c)(2)	Recordkeeping	In the case of covered institutions described in paragraph (c)(1) of this section, such records, apart from any policies and procedures, must be preserved for a time period not less than six years, the first two years in an easily accessible place. In the case of policies and procedures required under paragraphs (a) and (b)(2) of this section, covered institutions described in paragraph (c)(1) of this section must maintain a copy of such policies and procedures in effect, or that at any time within the past six years were in effect, in an easily accessible place.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.30(d)	Definitions	See fDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.31-248.100	[Reserved]	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.201	Duties regarding the detection, prevention, and mitigation of identity theft	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.201(a)	Scope	This section applies to a financial institution or creditor, as defined in the Fair Credit Reporting Act (15 U.S.C. 1681), that is:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.201(a)(1)	Scope	A broker, dealer or any other person that is registered or required to be registered under the Securities Exchange Act of 1934;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.201(a)(2)	Scope	An investment company that is registered or required to be registered under the Investment Company Act of 1940, that has elected to be regulated as a business development company under that Act, or that operates as an employees' securities company under that Act; or	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.201(a)(3)	Scope	An investment adviser that is registered or required to be registered under the Investment Advisers Act of 1940.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.201(b)	Definitions	See fDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.201(c)	Periodic identification of covered accounts	Each financial institution or creditor must periodically determine whether it offers or maintains covered accounts. As a part of this determination, a financial institution or creditor must conduct a risk assessment to determine whether it offers or maintains covered accounts described in paragraph (b)(3)(ii) of this section, taking into consideration:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.201(c)(1)	Periodic identification of covered accounts	The methods it provides to open its accounts;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.201(c)(2)	Periodic identification of covered accounts	The methods it provides to access its accounts; and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.201(c)(3)	Periodic identification of covered accounts	Its previous experiences with identity theft.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.201(d)	Establishment of an Identity Theft Prevention Program —	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.201(d)(1)	Program requirement	Each financial institution or creditor that offers or maintains one or more covered accounts must develop and implement a written Identity Theft Prevention Program (Program) that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities.	Functional	Intersects With	Insider Threat Response Capability	IRO-02.2	Mechanisms exist to implement and govern an insider threat program.	5	
248.201(d)(2)	Elements of the Program	The Program must include reasonable policies and procedures to:	Functional	Intersects With	Insider Threat Response Capability	IRO-02.2	Mechanisms exist to implement and govern an insider threat program.	5	
248.201(d)(2)(i)	Elements of the Program	Identify relevant Red Flags for the covered accounts that the financial institution or creditor offers or maintains, and incorporate those Red Flags into its Program;	Functional	Intersects With	Insider Threat Response Capability	IRO-02.2	Mechanisms exist to implement and govern an insider threat program.	5	
248.201(d)(2)(ii)	Elements of the Program	Detect Red Flags that have been incorporated into the Program of the financial institution or creditor;	Functional	Intersects With	Insider Threat Response Capability	IRO-02.2	Mechanisms exist to implement and govern an insider threat program.	5	
248.201(d)(2)(iii)	Elements of the Program	Respond appropriately to any Red Flags that are detected pursuant to paragraph (d)(2)(ii) of this section to prevent and mitigate identity theft; and	Functional	Intersects With	Insider Threat Response Capability	IRO-02.2	Mechanisms exist to implement and govern an insider threat program.	5	
248.201(d)(2)(iv)	Elements of the Program	Ensure the Program (including the Red Flags determined to be relevant) is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.	Functional	Intersects With	Insider Threat Response Capability	IRO-02.2	Mechanisms exist to implement and govern an insider threat program.	5	
248.201(e)	Administration of the Program	Each financial institution or creditor that is required to implement a Program must provide for the continued administration of the Program and must:	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
248.201(e)(1)	Administration of the Program	Obtain approval of the initial written Program from either its board of directors or an appropriate committee of the board of directors;	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
248.201(e)(2)	Administration of the Program	Involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the Program;	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
248.201(e)(3)	Administration of the Program	Train staff, as necessary, to effectively implement the Program; and	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	5	
248.201(e)(4)	Administration of the Program	Exercise appropriate and effective oversight of service provider arrangements.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
248.201(f)	Guidelines	Each financial institution or creditor that is required to implement a Program must consider the guidelines in Appendix A to this subpart and include in its Program those guidelines that are appropriate.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.202	Duties of card issuers regarding changes of address	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.202(a)	Scope	This section applies to a person described in § 248.201(a) that issues a credit or debit card (card issuer).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.202(b)	Definitions	See fDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.202(c)	Address validation requirements	A card issuer must establish and implement reasonable written policies and procedures to assess the validity of a change of address if it receives notification of a change of address for a consumer's debit or credit card account and, within a short period of time afterwards (during at least the first 30 days after it receives such notification), the card issuer receives a request for an additional or replacement card for the same account. Under these circumstances, the card issuer may not issue an additional or replacement card, until, in accordance with its reasonable policies and procedures and for the purpose of assessing the validity of the change of address, the card issuer:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.202(c)(1)	Address validation requirements	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.202(c)(1)(i)	Address validation requirements	Notifies the cardholder of the request:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.202(c)(1)(i)(A)	Address validation requirements	At the cardholder's former address; or	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.202(c)(1)(i)(B)	Address validation requirements	By any other means of communication that the card issuer and the cardholder have previously agreed to use; and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.202(c)(1)(ii)	Address validation requirements	Provides to the cardholder a reasonable means of promptly reporting incorrect address changes; or	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.202(d)	Alternative timing of address validation	Otherwise assesses the validity of the change of address in accordance with the policies and procedures the card issuer has established pursuant to § 248.201.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
248.202(e)	Form of notice	Any written or electronic notice that the card issuer provides under this paragraph must be clear and conspicuous and be provided separately from its regular correspondence with the cardholder.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control