§ 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.

~~*(a)Scope of information covered by this section.* The provisions of this section apply to all customer information in the possession of a covered institution, and all consumer information that a covered institution maintains or otherwise possesses for a business purpose, as applicable, regardless of whether such information pertains to individuals with whom the covered institution has a customer relationship, or pertains to the customers of other financial institutions and has been provided to the covered institution.~~

~~*(b)Policies and procedures to safeguard customer information.*~~

(a) *Policies and procedures to safeguard customer information.* (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.

(2) *Objectives*. These written policies and procedures must be reasonably designed to:

(i) Ensure the security and confidentiality of customer information;

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

~~(iii)~~( ) Protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.

(3) *Response programs for unauthorized access to or use of customer information.* Written policies and procedures in paragraph (~~b~~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:

(i) 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;

(ii) Take appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information; and

(iii) 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 (~~b~~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.

(4) *Notifying affected individuals of unauthorized access or use.* (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.

(ii) ~~(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.

~~*(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 ~~of the United States informs the covered institution, in writing,~~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 ~~a~~ notice for a time period specified by the Attorney General ~~of the United States, but not for longer than 15~~, 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 ~~15~~30 days if the Attorney General ~~of the United States~~ 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.

~~*(iv)*~~ (iv) *Notice contents*. The notice must:

(A) 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;

~~(B) Describe what has been done to protect the sensitive customer information from further unauthorized access or use;~~

~~(C)~~(B) 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;

~~(D)~~(C) 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;

~~(A)~~(D) 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;

~~(B)~~(E) 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;

~~(C)~~(F) 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;

~~(D)~~(G) Explain how the individual may obtain a credit report free of charge; and

~~(E)~~(H) 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.

(5) *Service providers*. (i) 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:

(A) ~~(i) A covered institution's response program prepared in accordance with paragraph (b)(3) of this section must include written policies and procedures requiring the institution, pursuant to a written contract between the covered institution and its service providers, to require the service providers to take appropriate measures that are designed to protect~~Protect against unauthorized access to or use of customer information~~, including~~; and

(B) Provide notification to the covered institution as soon as possible, but no later than ~~48~~72 hours after becoming aware ~~of~~that a breach~~, in the event of any breach~~ in security has occurred resulting in unauthorized access to a customer information system maintained by the service provider ~~to enable~~. Upon receipt of such notification, the covered institution ~~to implement~~must initiate its incident response program adopted pursuant to paragraph (a)(3) of this section.

(ii) 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 ~~its~~the covered institution's behalf in accordance with paragraph (~~b~~a)(4) of this section.

~~(c~~(iii) 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.

(b) *Disposal of consumer information and customer information.*

(1)Standard. Every covered institution, other than notice-registered broker-dealers, ~~that maintains or otherwise possesses customer information or consumer information for a business purpose~~ must properly dispose of ~~the~~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.

(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 (~~c~~b)(1) of this section.

(3)Relation to other laws. Nothing in this paragraph (~~c~~b) shall be construed:

(i) To require any covered institution to maintain or destroy any record pertaining to an individual that is not imposed under other law; or

(ii) To alter or affect any requirement imposed under any other provision of law to maintain or destroy records.

(~~d~~c) *Recordkeeping*.

~~(1)~~ (1) 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 ~~written records documenting its compliance with the requirements of paragraphs (b) and (c)(2) of this section.~~:

(i) The written policies and procedures required to be adopted and implemented pursuant to paragraph (a)(1) of this section;

(ii) 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;

(iii)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;

(iv)The written policies and procedures required to be adopted and implemented pursuant to paragraph (a)(5)(i) of this section;

(v) The written documentation of any contract or agreement entered into pursuant to paragraph (a)(5) of this section; and

(vi)The written policies and procedures required to be adopted and implemented pursuant to paragraph (b)(2) of this section.

~~(2)~~ (2) In the case of covered institutions described in paragraph (~~d~~c)(1) of this section, ~~the~~such records ~~required under paragraphs (b) and (c)(2) of this section~~, apart from any policies and procedures ~~thereunder~~, 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 (~~b~~a) and (~~c~~b)(2) of this section, covered institutions described in paragraph (~~d~~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.

(~~e~~d) *Definitions*. As used in this section, unless the context otherwise requires:

~~*(1)*~~ (1) *Consumer information* means any record about an individual, whether in paper, electronic or other form, that is a consumer report or is derived from a consumer report~~. Consumer information also means a compilation of such records.~~, or a compilation of such records, that a covered institution maintains or otherwise possesses for a business purpose regardless of whether such information pertains to (i) individuals with whom the covered institution has a customer relationship, or (ii) to the customers of other financial institutions where such information has been provided to the covered institution. Consumer

information does not include information that does not identify individuals, such as aggregate information or blind data.

(2) Consumer report has the same meaning as in section 603(d) of the Fair Credit Reporting Act (15 U.S.C. 1681a(d)).

(3) Covered institution means any broker or dealer, any investment company, and any investment adviser or transfer agent registered with the Commission or another appropriate regulatory agency ("ARA") as defined in section 3(a)(34)(B) of the Securities Exchange Act of 1934.

(4)(i) *Customer* has the same meaning as in § 248.3(j) unless the covered institution is a transfer agent registered with the Commission or another ARA.

(ii) With respect to a transfer agent registered with the Commission or another ARA, for purposes of this section, *customer* means any natural person who is a securityholder of an issuer for which the transfer agent acts or has acted as a transfer agent.

(5)(i) *Customer information* for any covered institution other than a transfer agent registered with the Commission or another ARA means any record containing nonpublic personal information as defined in § 248.3(t) about a customer of a financial institution, whether in paper, electronic or other form, that is in the possession of a covered institution or that is handled or maintained by the covered institution or on its behalf regardless of whether such information pertains to (a) individuals with whom the covered institution has a customer relationship, or (b) to the customers of other financial institutions where such information has been provided to the covered institution.

(ii) With respect to a transfer agent registered with the Commission or another ARA, *customer information* means any record containing nonpublic personal information as defined in § 248.3(t) identified with any natural person, who is a securityholder of an issuer for which the transfer agent acts or has acted as transfer agent, that is in the possession of a transfer agent or that is handled or maintained by the transfer agent or on its behalf, regardless of whether such information pertains to individuals with whom the transfer agent has a customer relationship, or pertains to the customers of other financial institutions and has been provided to the transfer agent.

~~(6)~~ (6) *Customer information systems* means the information resources owned or used by a covered institution, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of customer information to maintain or support the covered institution's operations.

~~(7)~~ (7) *Disposal* means:

(i) ~~(i)~~ The discarding or abandonment of consumer information or customer information; or

(ii) ~~(ii)~~ The sale, donation, or transfer of any medium, including computer equipment, on which consumer information or customer information is stored.

(8) *Notice-registered broker-dealer* means a broker or dealer registered by notice with the Commission under section 15(b)(11) of the Securities Exchange Act of 1934 (15 U.S.C. 78o(b)(11)).

(9)(i) *Sensitive customer information* means any component of customer information alone or in conjunction with any other information, the compromise of which could create a

reasonably likely risk of substantial harm or inconvenience to an individual identified with the information.

(ii) Examples of sensitive customer information include:

(A) Customer information uniquely identified with an individual that has a reasonably likely use as a means of authenticating the individual's identity, including

(1) A Social Security number, official State- or government--issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

(2) A biometric record;

(3) A unique electronic identification number, address, or routing code;

(4) Telecommunication identifying information or access device (as defined in 18 U.S.C. 1029(e)); or

(B) Customer information identifying an individual or the individual's account, including the individual's account number, name or online user name, in combination with authenticating information such as information described in paragraph (ed)(9)(ii)(A) of this section, or in combination with similar information that could be used to gain access to the customer's account such as an access code, a credit card expiration date, a partial Social Security number, a security code, a security question and answer identified with the individual or the individual's account, or the individual's date of birth, place of birth, or mother's maiden name.

(10) Service provider means any person or entity that ~~is a third party and~~ receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a covered institution.

~~*(11) Substantial harm or inconvenience* means personal injury, or financial loss, expenditure of effort or loss of time that is more than trivial, including theft, fraud, harassment, physical harm, impersonation, intimidation, damaged reputation, impaired eligibility for credit, or the misuse of information identified with an individual to obtain a financial product or service, or to access, log into, effect a transaction in, or otherwise misuse the individual's account.~~

(11) *Transfer agent* has the same meaning as in section 3(a)(25) of the Securities ~~*(12)*~~ Exchange Act of 1934 (15 U.S.C. 78c(a)(25)).