U.S. COMMODITY FUTURES TRADING COMMISSION
Division of Swap Dealer and Intermediary Oversight
1155 21st Street N.W., Washington, DC 20581
Telephone: (202) 418-5977
E-Mail: gbarnett@cftc.gov

Gary Barnett
Director

CFTC Staff Advisory No. 14-21
Division of Swap Dealer and Intermediary Oversight
February 26, 2014

To: **All CFTC Regulated Intermediaries**
Attention: **Chief Financial Officer**
Subject: **Gramm-Leach-Bliley Act Security Safeguards**

Congress enacted Title V of the Gramm-Leach-Bliley Act (GLBA) in 1999 to ensure that financial institutions respect the privacy of their customers and protect the security and confidentiality of nonpublic personal information.[1] In enacting the GLBA, Congress directed certain Federal financial regulators to adopt and implement rules to achieve Title V's goals. Through the Commodity Futures Modernization Act of 2000, Congress added the Commodity Futures Trading Commission (Commission) as a Federal financial regulator with responsibility for implementing Title V.[2] The Commission promulgated Title V privacy rules in 2001, and has updated those regulations over time to include additional types of covered financial institutions to ensure that the goals of Title V continue to be met.[3]

At this time, the Division of Swap Dealer and Intermediary Oversight (Division) believes it important to outline recommended best practices for covered financial institutions to comply with Title V and Part 160 of the Commission's regulations concerning security safeguards. These recommendations are consistent with guidelines and regulations issued by other Federal financial regulators.[4]

---

[1] Financial Services Modernization Act of 1999, commonly known as the Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (codified in scattered sections of 12 U.S.C. and 15 U.S.C.). Title V is codified in scattered sections of 15 U.S.C.

[2] Section 5g of the Commodity Exchange Act, 7 U.S.C. § 7b-2.

[3] 17 C.F.R. Part 160 (2013). The Part 160 regulations initially applied to futures commission merchants, commodity trading advisors, commodity pool operators, and introducing brokers. Privacy of Consumer Financial Information, 66 FR 21236 (Apr. 27, 2001). Retail foreign exchange dealers became subject to the regulations in 2010. Regulation of Off-Exchange Retail Foreign Exchange Transactions and Intermediaries, 75 FR 55410 (Sept. 10, 2010). Swap dealers and major swap participants were added to Part 160 in 2011. Privacy of Consumer Financial Information; Conforming Amendments Under Dodd-Frank Act, 76 FR 43874 (July 22, 2011).

[4] With some variation, these best practices are designed to be generally consistent with regulations promulgated by the Federal Trade Commission, Standards for Safeguarding Customer Information, 16 C.F.R. Part 314 (2013) (FTC Safeguards Rule); rules proposed by the Securities and Exchange Commission, Part 248—Regulation S—P: Privacy of Consumer Financial Information and Safeguarding Personal Information, 73 FR 13692 (Mar. 13, 2008) (SEC Proposed Rule); and guidance issued jointly by the Office of the Comptroller of the Currency, the Department of the Treasury, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision. See Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness, 66 FR 8616 (Feb. 1, 2001) (Interagency Guidelines); and Interagency Guidance on Response Programs for Unauthorized Access to Customer

Background

Under Part 160 of the Commission's regulations, futures commission merchants, commodity trading advisors, commodity pool operators, introducing brokers, retail foreign exchange dealers, swap dealers and major swap participants (covered entities) "must adopt policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information."[5] As outlined in Part 160.30, those policies and procedures must:

(1) insure the security and confidentiality of customer records and information;

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

(3) protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.[6]

Below are recommended best practices for the required "administrative, technical and physical safeguards."

Recommended Best Practices

Each covered entity should develop, implement and maintain a written information security and privacy program that is appropriate to its size and complexity, the nature and scope of its activities, and which requires it to, at a minimum:

1. Designate a specific employee with privacy and security management oversight responsibilities, who develops strategic organizational plans for implementing the required controls, is part of or reports directly to senior management or the Board of Directors, and designates employee(s) to coordinate, implement and regularly assess the effectiveness of the program.[7]
2. Identify, in writing, all reasonably foreseeable internal and external risks to security, confidentiality, and integrity of personal information and systems processing personal information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information or systems, and establish processes and controls to assess and mitigate such risks;[8] also, identify such risks, and establish processes and controls to assess and mitigate risks, before implementing new or material changes to internal systems.

Information and Customer Notice, 70 FR 15736 (Mar. 29, 2005) (Interagency Guidance on Response Programs).

[5] 17 C.F.R. § 160.30 (2013).

[6] Section 501(b) of the GLBA, 15 U.S.C. § 6801(b).

[7] See FTC Safeguards Rule, 16 C.F.R. § 314.4(a); SEC Proposed Rule 248.30(a)(3)(i); Interagency Guidelines, Appendix B, Section III.A.

[8] See FTC Safeguards Rule, 16 C.F.R. § 314.4(b); SEC Proposed Rule 248.30(a)(3)(ii); Interagency Guidelines, Appendix B, Section III.B.

3. Design and implement safeguards to control the identified risks, and maintain a written record of such designs.[9]
4. Train staff to implement the program,[10] and provide regular refresher training.
5. Regularly test or otherwise monitor the safeguards' controls, systems, policies and procedures, and maintain written records of the effectiveness of the controls, including the effectiveness of:
    a. Access controls on personal information;
    b. Appropriate encryption of electronic information in storage and transit;
    c. Controls to detect, prevent and respond to incidents of unauthorized access to or use of personal information; and
    d. Employee training and supervision relating to the program.[11]
6. At least once every two years, arrange for an independent party to test and monitor the safeguards' controls, systems, policies and procedures, maintaining written records of the effectiveness of the controls, as explained above.
7. To the extent that third party service providers have access to customer records and information, oversee service providers and document in writing that in such oversight the entity is:
    a. Taking reasonable steps to select and retain service providers capable of maintaining appropriate safeguards; and
    b. Contractually requiring service providers to implement and maintain appropriate safeguards.[12]
8. Regularly evaluate and adjust the program in light of:
    a. The results of the risk assessment process;
    b. Relevant changes in technology and business processes;
    c. Any material changes to operations or business arrangements; and
    d. Any other circumstances that the entity knows or reasonably believes may have a material impact on the program.[13]

---

[9] See FTC Safeguards Rule, 16 C.F.R. § 314.4(c); SEC Proposed Rule 248.30(a)(3)(iii); Interagency Guidelines, Appendix B, Section III.C.

[10] See also FTC Safeguards Rule, 16 C.F.R. § 314.4(b)(1); SEC Proposed Rule 248.30(a)(3)(v); Interagency Guidelines, Appendix B, Section III.C.2.

[11] See FTC Safeguards Rule, 16 C.F.R. § 314.4 (b) and (c); SEC Proposed Rule 248.30(a)(3)(iv); Interagency Guidelines, Appendix B, Section III.C.3.

[12] See FTC Safeguards Rule, 16 C.F.R. § 314.4(d); SEC Proposed Rule 248.30(a)(3)(vi); Interagency Guidelines, Appendix B, Section III.D.

[13] See FTC Safeguards Rule, 16 C.F.R. § 314.4(e); SEC Proposed Rule 248.30(a)(3)(vii); Interagency Guidelines, Appendix B, Section III.E.

9. Design and implement policies and procedures for responding to an incident involving unauthorized access, disclosure or use of personal information, including policies and procedures to:
    a. Assess the nature and scope of any such incident, and maintain a written record of the systems and information involved;
    b. Take appropriate steps to contain and control the incident to prevent further unauthorized access, disclosure or use, and maintain a written record of steps taken;
    c. Promptly conduct a reasonable investigation, determine the likelihood that personal information has or will be misused, and maintain a written record of such determination; and
    d. If the covered entity determines that misuse of information has occurred or is reasonably possible, then as soon as possible notify individuals whose information was or may be misused and notify the Commission in writing explaining the situation and possible risks (unless law enforcement requests in writing that notification be delayed).[14]
10. Provide the Board of Directors an annual assessment of the program, including updates to the program, the effectiveness of the program, and instances during the year of unauthorized access or disclosure of personal information.[15]

The Division issues these recommended best practices with the expectation that the Division will enhance its audit and review standards as it continues to focus more resources on GLBA Title V compliance.[16]

Sincerely,

Gary Barnett
Director
Division of Swap Dealer and Intermediary Oversight

[14] See SEC Proposed Rule 248.30(a)(4); Interagency Guidance on Response Programs, Supplement A to Appendix B, Section II.

[15] See Interagency Guidelines, Appendix B, Section III.F.

[16] See, e.g., Press Release 5670-09, 6/29/2009, CFTC Sanctions Foreign Currency Broker Who Allowed Confidential Personal Information of its Customers to Appear on the Internet.