CLIENT UPDATE

CFTC ADVISORY ON GRAMM-LEACH-BLILEY ACT SECURITY SAFEGUARDS

NEW YORK
Byungkwon Lim
blim@debevoise.com

Gary E. Murphy
gemurphy@debevoise.com

Aaron J. Levy
ajlevy@debevoise.com

On February 26, 2014, the Division of Swap Dealer and Intermediary Oversight ("DSIO") of the Commodity Futures Trading Commission (the "CFTC") issued an advisory[1] (the "Advisory") recommending certain "best practices" for covered financial institutions to comply with Title V of the Gramm-Leach-Bliley Act (the "GLB Act") and Part 160 of the CFTC's regulations concerning security safeguards. The recommendations are consistent with guidelines and regulations issued by other federal financial regulators.[2]

BACKGROUND

Congress enacted Title V of the GLB Act in 1999 to ensure that financial institutions respect their customers' privacy and protect the security and confidentiality of nonpublic personal information. In enacting the GLB Act, Congress directed certain federal financial

---

1 CFTC Staff Advisory 14-21, Division of Swap Dealer and Intermediary Oversight (Feb. 26, 2014), available at: http://www.cftc.gov/ucm/groups/public/@lrlettergeneral/documents/letter/14-21.pdf

2 With some variation, the best practices recommended by DSIO are designed to be generally consistent with the Federal Trade Commission's regulations (16 C.F.R. Part 314 (2013)); the Securities and Exchange Commission's proposed rules (73 Fed. Reg. 13692 (Mar. 13, 2008)); 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 (66 Fed. Reg. 8616 (Feb. 1, 2001) and 70 Fed. Reg. 15736 (Mar. 29, 2005)).

regulators to adopt and implement rules to achieve the goals of Title V. Through the Commodity Futures Modernization Act of 2000, Congress added the CFTC as a federal financial regulator with responsibility for implementing Title V. In 2001, the CFTC promulgated Title V privacy rules in Part 160 of its regulations.[3]

Part 160 provides that futures commission merchants, commodity trading advisors, commodity pool operators, introducing brokers, retail foreign exchange dealers, swap dealers and major swap participants ("covered entities")[4] "must adopt policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information."[5] These policies and procedures must:

- insure the security and confidentiality of customer records and information;
- protect against any anticipated threats or hazards to the security or integrity of such records; and
- protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

RECOMMENDED BEST PRACTICES

The Advisory recommends, as best practices for the required "administrative, technical and physical safeguards," that each covered company should develop, implement and maintain a written information security and privacy program appropriate to its size and complexity, the nature and scope of its activities, and which requires it to, at a minimum:

- Designate a specific employee with privacy and security management oversight responsibilities, who develops 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 program's effectiveness;
- 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,

---

3 Part 160 is available at: http://www.ecfr.gov/cgi-bin/text-idx?SID=9b77ad5234e03c9e726d8c6be4f67d2b&node=17:1.0.1.1.59&rgn=div5.

4 The CFTC has updated Part 160 over time to include additional types of covered financial institutions. The Part 160 regulations initially applied to futures commission merchants, commodity trading advisors, commodity pool operators and introducing brokers. Retail foreign exchange dealers became subject to the regulations in 2010. Finally, swap dealers and major swap participants were added to Part 160 in 2011.

5 See section 160.30 of the CFTC regulations.

destruction or other compromise of such information or systems, and establish processes and controls to assess and mitigate such risks (both as a general matter and before implementing new or material changes to internal systems);

- Design and implement safeguards to control the identified risks and maintain a written record of such designs;
- Train staff to implement the program and provide regular refresher training;
- 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 unauthorized access to or use of personal information and (d) employee training and supervision relating to the program;
- Importantly, 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;
- To the extent third party service providers have access to customer records, 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;
- 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;
- Design and implement policies and procedures for responding to unauthorized 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 CFTC in writing explaining the situation and possible risks (unless law enforcement requests in writing that notification be delayed); and

- (10) Provide the Board of Directors an annual assessment of the program, including any updates to the program, the effectiveness of the program and instances during the year of unauthorized access or disclosure of personal information.

DSIO notes in the Advisory that it expects to enhance its audit and review standards as it continues to focus more resources on compliance with Title V of the GLB Act.

* * *

Please do not hesitate to contact us with any questions.

February 28, 2014