CORE COMPLIANCE & LEGAL SERVICES, INC.

Risk Management Update
November 2013

FEDERAL AND STATE REGULATIONS GOVERNING INVESTMENT ADVISER PRIVACY SAFEGUARDS

In response to the Gramm-Leach-Bliley Act[1] ("GLB Act") that was enacted by Congress in 1999, both federal and state regulatory agencies have promulgated extensive rules pertaining to consumer privacy notifications and the safeguarding of nonpublic personal information. Effective November 13, 2000, the Securities and Exchange Commission ("SEC") adopted Regulation S-P – Privacy of Consumer Information[2] ("Regulation S-P"), which requires broker-dealers, investment advisers registered with the SEC and other financial institutions subject to SEC oversight to:

- Adopt written policies and procedures that outline how the institution handles and ensures the privacy of client confidential nonpublic information;
- Deliver a written statement (the "Privacy Notice") to each client:
  - at the inception of the client relationship;
  - annually thereafter; and
  - anytime the information in the Privacy Notice is changed; and
- Provide clients, when applicable, with the ability to opt-out in writing prior to sharing their confidential nonpublic information to non-affiliates.[3]

Under Regulation S-P, the Privacy Notice is required to contain a description of the general types of information collected, along with the firm's sharing practices and the ability to opt-out when applicable. In 2009, the SEC, together with seven other federal agencies published a "model" Privacy Notice to help consumers better understand how financial institutions collect and share their personal information.[4] The use of the model form is voluntary and can be used by both state and SEC registered firms. Significantly, the model form provides a safe harbor (*i.e.*, the user will be deemed to have complied with the disclosure requirements of Regulation S-P), if used consistent with the form's instructions issued by the agencies.

Additional recently adopted federal privacy regulations include:

- Amended Regulation S-P – Disposal of Consumer Report Information (January 2005)[5]
- Regulation S-AM – Limitations on Affiliate Marketing (September 2009)[6]
- Regulation S-ID – Identity Theft Red Flags Rule (May 2013)[7]

---

[1] Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338.
[2] *See* http://www.sec.gov/rules/final/34-42974.htm.
[3] 17 CFR § 248. Notably, the State of California requires businesses (including investment advisers) to obtain an "opt-in" from clients before the firm can share a client's nonpublic personal financial information with unaffiliated third party companies (with the exception of companies that offer financial products or services).
[4] *See* http://www.sec.gov/divisions/marketreg/tmcompliance/modelprivacyform-secg.htm.
[5] http://www.sec.gov/rules/final/34-50781.pdf.
[6] http://www.sec.gov/rules/final/2009/34-60423fr.pdf.
[7] http://www.sec.gov/rules/final/2013/34-69359.pdf.

While broker-dealers, SEC registered investment advisers and other federal regulated financial institutions must adhere to the above rules, state registered investment advisers are required to follow the mandates of the Federal Trade Commission's ("FTC") "Privacy of Consumer Information" rule implemented in November 2000,[8] in addition to those privacy regulations issued by the state(s) in which they are registered. The FTC rule is very similar to provisions of Regulation S-P and is comprised of examples of how to comply with the requirements. Notably, the FTC stated in the release of the rule the following:

> *"Compliance by interstate securities broker-dealers and investment advisers that are not registered with the SEC with applicable examples in the SEC rule will constitute compliance with the Commission's rule."*[9]

Importantly though, a few states have crossed over the segregation lines by releasing privacy laws with tentacles which reach beyond that state's border. For example, the State of California requires a "business[10] that owns or licenses[11] personal information about a California resident" to have procedures and controls in place that are reasonably designed to protect such information from unauthorized use, access, disclosure, or destruction.[12] Based on the State's definition of business, the location of the business and whether or not the firm is registered with the State is not relevant. Therefore, an adviser that is registered and located in another state and has less than six clients residing in California (*i.e.,* an exempt from registering in California), could be required to adhere to California's privacy regulation.

Similarly, the Commonwealth of Massachusetts requires every "person"[13] who owns or licenses personal information about a resident of Massachusetts to have a comprehensive information security program ("ISP") that has administrative, technical, and physical safeguards in place.[14] The ISP must designate at least one employee that is responsible for the oversight and maintenance of the program, which must include protocols for:

- Assessment of foreseeable risks;
- Development of security policies pertaining to storage, access and transportation of non public information outside of the business;
- Prevention of access of nonpublic information by terminated employees;

---

[8] http://www.ftc.gov/os/2000/05/65fr33645.pdf.
[9] id.
[10] The term "business" is defined by the state to mean "a sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of this state, any other state, the United States, or of any other country, or the parent or the subsidiary of a financial institution."
[11] The term "owns or licenses" is defined by the State to "include personal information that a business retains as part of the business' internal customer account or for the purpose of using that information in transactions with the person to whom the information relates."
[12] California Civ. Code §1798.82(a).
[13] **Person**, means "a natural person, corporation, association, partnership or other legal entity, other than an agency, executive office, department, board, commission, bureau, division or authority of the Commonwealth, or any of its branches, or any political subdivision thereof."
[14] 201 C.M.R. 17.00.

- Ensuring agreements with service providers contain confidentiality requirement clauses; and
- Oversight (via due diligence) of certain service providers.

Based upon these parameters, State of Massachusetts registered firms, broker-dealers, SEC registered investment advisers and other financial institutions regulated by the SEC must comply with the Commonwealth's requirements if they have consumers that reside within Massachusetts.[15]

Additionally, the majority of states have adopted security breach laws requiring firms to provide prompt (if not immediate) notification to clients of any breach involving a client's non public personal information. The states can vary in their description of what constitutes nonpublic personal information and notably, the Governor of California recently signed into law additional provisions to the State's existing privacy breach regulations (slated to take effect January 2014), which add a new category of information that triggers data security breach notifications.[16]

Advisory firms also must consider identity theft risks and whether or not they are required to implement identity theft programs. In 2007, the FTC published the "Red Flags Rule,"[17] and in 2013, the SEC released Regulation S-ID. Both rules are very similar and require broker-dealers and investment advisers (among others) that fall under the applicable rule's definition of "financial institution" and that have one or more "covered accounts" (as defined in the rules), to implement a program to identify, detect, and mitigate red flags to help prevent identity theft. Each firm also must perform an initial and annual risk assessment to determine the extent, if any, of the firm's risk of identity theft and implement and enhance its program accordingly.

Consideration also should be given to certain data protection regulations that pertain to types of information collected, such as the Portability and Accountability Act ("HIPAA"), which covers health related information, and the Fair and Accurate Credit Transactions Act ("FACTA") that protects consumer credit information. Although advisory firms may not collect this type of information from clients, it may be gathered from employees and certain independent contractors.

Practical Tips for Remaining In Compliance With Applicable Privacy Regulations

The following are practical tips for financial institutions to consider when reviewing their privacy safeguards.

1. Take inventory of the types of nonpublic data gathered by the firm, along with how it is accessed and disseminated, both internally and externally.
2. Confirm that written policies and procedures outline adequate safeguards for the gathering, maintenance, dissemination, and destruction of nonpublic data.

---

[15] To assist firms with compliance of the Commonwealth's Privacy Act, the State issued a "Compliance Checklist that may be found at http://www.mass.gov/ocabr/docs/idtheft/compliance-checklist.pdf

[16] http://oag.ca.gov/ecrime/databreach/list.

[17] 16 C.F.R. 681.1; *see* also 72 Fed. Reg. at 63,771 (Nov. 9, 2007) http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf

3. Perform testing to help ensure procedures and controls are adequately designed to safeguard nonpublic information and prevent identity theft.
4. Provide training to employees through email reminders, webinars, and/or in person meetings).
5. Consider having a third party service provider perform an independent audit.
6. Periodically review the websites of the SEC, FTC, and applicable states, and subscribe to receive newsletters and blogs from securities law firms and compliance consulting firms, to receive helpful information/tools and remain abreast of the various privacy regulations and any changes thereof.
7. Ensure privacy disclosures are adequate and meet requirements.
8. Consider using the model Privacy Notice to take advantage of the safe harbor provision.
9. Review current marketing efforts and confirm nonpublic client information is not being provided to third parties without the proper opt-in and opt-out notices.
10. Consider utilizing software that automatically encrypts and protects nonpublic information being sent and received via the internet.

For more information, or to learn about how CCLS may be of assistance, please do not hesitate to contact us at (619) 278-0020.

Author: Tina Mitchell, Lead Sr. Compliance Consultant; Editor: Michelle L. Jacko, CEO, Core Compliance & Legal Services ("CCLS"). CCLS works extensively with investment advisers, broker-dealers, investment companies, hedge funds, private equity firms and banks on regulatory compliance issues. For more information about this topic and other compliance consultation services, please contact us at (619) 278-0020, info@corecls.com or visit www.corecls.com.