

Client Memorandum

Update on Privacy Requirements Affecting Private Investment Fund Managers

February 26, 2010

Data security and privacy continue to be the subject of new legislative and regulatory proposals and requirements. A number of initiatives recently have been proposed or enacted that are designed to protect consumers and their personal information. Many of these requirements likely will be satisfied by existing information security policies and procedures, but some may not be—particularly requirements relating to the encryption of certain electronic communications.

- **Massachusetts Privacy Requirements.** A new regulation effective March 1, 2010, requires businesses, wherever located, that possess personal information of Massachusetts residents to meet specified information security requirements including encryption of electronic communications containing such information.
- **Privacy Notice Model Form.** Federal regulatory agencies, including the Securities and Exchange Commission (“SEC”), have jointly issued a Final Model Privacy Form (the “Model Form”) for financial institutions to use to comply with their privacy notice obligations. Privacy notices based upon previously issued guidance remain adequate through Dec. 31, 2010, but the Model Form will be the only safe harbor for privacy notices issued after that date.
- **Regulation S-AM.** Regulation S-AM prohibits certain financial institutions from using information provided by affiliates to solicit consumers unless the consumers have been notified of the potential use of their personal information for marketing purposes and have been given an opportunity to opt out. Regulation S-AM will become effective June 1, 2010.
- **Red Flags Rule.** The Federal Trade Commission (“FTC”), federal bank regulatory agencies and the National Credit Union Administration have issued a rule seeking to prevent and combat identity fraud (the “Red Flags Rule”). The Red Flags Rule requires “financial institutions” and “creditors” that hold “covered accounts” to develop and implement identity theft prevention programs for new and existing accounts. Many private fund managers may not have the type of account that would subject them to the Red Flags Rule. The enforcement date of the Red Flags Rule is June 1, 2010.

Massachusetts Privacy Provisions

The Massachusetts Office of Consumer Affairs and Business Regulation has issued a new regulation, effective March 1, 2010, requiring businesses that possess personal information about Massachusetts

residents to implement comprehensive information security programs to protect that information.¹ The regulation applies to any business engaged in commerce that collects and retains personal information in connection with the provision of goods and services or in connection with employment. Personal information is defined as a Massachusetts resident's first name (or initial) and last name in combination with such person's social security number; driver's license or state-issued identification card number; or financial account or credit/debit card number (with or without security access code).

The Massachusetts regulation requires businesses to have an information security program that is in writing and proscribes physical, administrative and technical safeguards, which can be found in Section 17.03 of the statute, [available here](#). Two particular new procedures are noteworthy. First, the Massachusetts regulation requires encryption of personal information transmitted over public or wireless networks or stored on unsecured portable storage devices (such as notebook computers and portable USB or other drives).² Second, the regulation requires that businesses that disclose personal information to service providers include privacy provisions to meet the regulation's encryption and service provider contract requirements.³ Ultimately, the suitability of the safeguards for a particular firm will be judged based upon the size, scope and type of business, the resources available to them, and the amount and relative need for security of the type of information owned or licensed.⁴

To comply with these requirements, firms should: (1) identify all situations in which the firm comes into possession of personal information of Massachusetts residents; (2) identify any service providers that may receive such information in any electronic form including administrators, accountants, attorneys, custodians and placement agents; (3) provide for encryption of electronic communications containing personal information where applicable; and (4) confirm that all relevant service provider agreements contain privacy protection provisions as required.⁵

At the federal level, the SEC in 2008 proposed amendments to Regulation S-P that would, to some extent, overlap with the Massachusetts requirements.⁶ The proposed amendments would expand information security requirements for covered institutions, broaden the scope of information that requires safeguards and disposal, create more specific information safeguard requirements, require documented oversight of the sufficiency of service providers' information security safeguards, establish requirements for security programs to respond to a security breach, and permit limited disclosure of investor information when an employee moves from one firm to another.

New Guidance for Fulfilling Privacy Notice Requirements

The 1999 Gramm-Leach-Bliley Act ("GLBA") required financial institutions to provide "clear and conspicuous notice" to customers to disclose the institution's privacy policies and their information sharing practices with affiliates with respect to customer information. The GLBA also required financial institutions that shared customer information with certain non-affiliated parties to provide those customers with "clear and conspicuous" notice of their right to opt out of that information being shared.⁷

The FTC and SEC adopted the "Privacy Rule" and Regulation S-P, respectively, which included "sample clauses" intended to function as guidance as to what constituted "clear and conspicuous" notice.⁸ Based on a

¹ The regulations, entitled "Standards for the Protection of Personal Information of Residents of the Commonwealth," can be found at 201 MASS. CODE REGS. 17.00 *et seq.* Schulte Roth & Zabel LLP does not practice Massachusetts law.

² 201 MASS. CODE REGS. 17.04(3), (5) (2009).

³ 201 MASS. CODE REGS. 17.03(2)(F)(2) (2009).

⁴ 201 MASS. CODE REGS. 17.03(1) (2009). Nevada also requires encryption of personal information but the law only applies to firms doing business in that state. S.B. 227, 2009 Leg., 75th Sess. (Nev. 2009).

⁵ New contracts entered into after March 1, 2010, must have these provisions but contracts entered into before that date have until March 1, 2012, to comply.

⁶ 73 Fed. Reg. 13692 (March 4, 2008).

⁷ The affiliate sharing rule and opt out requirements are now treated more fully in Regulation S-AM.

⁸ 17 C.F.R. § 248 (2009) or "Regulation S-P" applies to registered investment advisers while unregistered advisers must comply with analogous requirements under the FTC's "Privacy Rule," 16 C.F.R. § 313 (2009).

concern that the notice under the “sample clauses” guidance was still insufficiently clear for consumers, Congress passed the Financial Services Regulatory Relief Act of 2006, amending the GLBA and requiring the agencies to issue a more comprehensive and succinct model notice.

The Model Form was issued on Nov. 17, 2009, by several federal regulatory agencies. The form will not be mandatory but will be the only safe harbor available for privacy notices issued after Dec. 31, 2010.⁹

The Model Form attempts to address concerns about consumer comprehension of privacy notices by using a table format with a standardized style. As a result of this standardization, the Model Form allows less flexibility in the content and format of the privacy notice document. In response to concerns over the inflexibility of the Model Form format, the joint agencies have stressed that the Model Form is not mandatory. Firms may elect to use other formats for privacy notices, including notices using the previously issued sample clauses or simplified notice, as long as the notice complies with the Privacy Rule and Regulation S-P.¹⁰ However, the previously issued sample clauses will be eliminated from the regulations and will no longer constitute a safe harbor.

Regulation S-AM

Effective June 1, 2010, Regulation S-AM will prohibit “covered persons,” (including investment advisers) from using “eligibility information” provided by affiliates to solicit consumers using a “marketing solicitation” unless the consumer: (1) has previously received notice of the potential use of the information for marketing purposes; (2) was provided with a simple method and reasonable amount of time to opt out of allowing their information to be used for marketing purposes; and (3) did not opt out.¹¹

“Eligibility information” includes credit or other information about the consumer that is used to determine eligibility for credit or insurance. A “marketing solicitation” means marketing of a product or service to a consumer based on eligibility information communicated by an affiliate of a “covered person” that is intended to encourage the consumer to obtain goods or services.

There are several exceptions that permit affiliates to use eligibility information to solicit consumers, including, among others, where a marketing solicitation is made to a consumer with whom the affiliate has a pre-existing business relationship. For situations not falling within an exception, the SEC has indicated that Regulation S-AM requirements for a “clear and conspicuous” notice and a “reasonable opportunity” for consumers to opt out from information sharing will be satisfied by using the privacy notice Model Form.

Red Flags Rule

The FTC’s Red Flags Rule requires certain entities to develop and implement policies and procedures to detect, prevent and mitigate identity theft.¹² To determine whether the Red Flags Rule applies, a firm must first determine whether it is a “financial institution” or a “creditor.”¹³ Many private fund managers will not fall

⁹ The SEC does not technically offer a safe harbor but only “guidance.” The SEC uses a “facts and circumstances” test for each individual situation to determine compliance with Regulation S-P. 17 C.F.R. § 248.2(a) (2009).

¹⁰ “Simplified notice” is reserved for financial institutions that do not disclose, and do not wish to reserve the right to disclose, nonpublic personal information about its customers or former customers to affiliates or nonaffiliated third parties except as authorized under the standard exceptions, Regulation S-P, 17 C.F.R. § 248.14-15; Privacy Rule, 16 C.F.R. §§313.14-15 (2009). Simplified notice consists of simply stating that fact, in addition to the information required under paragraphs (a)(1), (a)(8), (a)(9), and (b) of the Rule 6 of Regulation S-P (17 C.F.R. § 248.6 (2009)) or §§313.6 of the Privacy Rule (16 C.F.R. §§313.6 (2009)), respectively.

¹¹ The rule explicitly allows opt out notices to be delivered concurrently with annual privacy notices required under Regulation S-P, and one version of the new Model Form includes an attached marketing affiliate opt-out form.

¹² As noted in our *Alert* dated Nov. 18, 2009, [available here](#), the enforcement date for the Red Flags Rule has been extended until June 1, 2010. In our *Alert* dated Sept. 25, 2008, [available here](#), we described the guidelines of the written identity theft prevention program required under the Red Flags Rule.

¹³ A “financial institution” is defined as a “State or National Bank, a state or federal savings and loan association, a mutual savings bank, a State or Federal credit union, or any other person that, directly or indirectly holds a transaction account belonging to a consumer.” 15 U.S.C. § 1681a(t). A “transaction account” is an account that supports payments or transfers to third parties. 15 U.S.C. § 1681a(t) (citing 12 U.S.C. § 461(b)(1)(c)). The definition of “creditor” is “any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit.” 15 U.S.C. § 1681a(r)(5) (citing 15 U.S.C. § 1691a(e)).

within the category of a financial institution as they do not maintain accounts for the purpose of making payments or transfers to third persons. However, an investment firm may be considered a creditor if it extends credit to its investors by, for example, billing retrospectively for advisory services.¹⁴

Even if a firm is a financial institution or a creditor, the Red Flags Rule does not apply unless the firm also maintains a "covered account." There are two types of covered accounts. The first is a consumer account that is primarily for personal, family or household purposes to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan or bank account.¹⁵ Accounts used by private fund managers would not fall into this category.

The second type of covered account is any other account for which there is a reasonably foreseeable risk to the customer, or to the safety and soundness of the financial institution or creditor, of identity theft.¹⁶ The examples given by the FTC include small business accounts, sole proprietorship accounts or single transaction consumer accounts that may be vulnerable to identity theft. In determining whether any accounts would fall under this second type of covered account, firms should consider how accounts can be accessed (e.g., whether information can be obtained or funds transferred via the telephone or the Internet) and actual incidents of identity theft. Because there is often a low risk of identity theft at firms that only manage private investment funds, the Red Flags Rule may not typically apply to private fund managers.

Where the Red Flags Rule does apply, the FTC requires that the firm develop and implement a written Identity Theft Prevention Program designed to detect, prevent and mitigate identity theft in connection with covered accounts.¹⁷ The program must be specifically tailored to the risks of the firm and approved by the firm's board of directors or other governing body. The rule also requires financial institutions and creditors to periodically reassess their accounts to ensure that new accounts or new risks have not created new "covered accounts" subject to the Red Flags Rule.

* * *

The business of private investment fund management may present relatively low risk of identity theft or other misuse of personal information, but there are important federal and state requirements that may apply. In the past year the SEC has increased enforcement of Regulation S-P, bringing four cases charging violations of data security requirements.¹⁸ Compliance with these requirements should be part of every manager's regularly updated policies and procedures.

Authored by Marc Elovitz, Jason Kaplan, Jessica Sklute and J.R. Morgan.

¹⁴ See "Frequently Asked Questions: Identity Theft Red Flags and Address Discrepancies," available at <http://www.ftc.gov/os/2009/06/090611redflagsfaq.pdf>. There is legislation currently before Congress that would reclassify low-risk entities as exempt from "creditor" status. Amending Fair Credit Reporting Act, H.R. 3763, 111th Cong. (2009).

¹⁵ 16 C.F.R. § 681.1(b)(3)(i) (2009).

¹⁶ "Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks." 16 C.F.R. § 681.1(b)(3)(ii) (2009).

¹⁷ 16 C.F.R § 681.1(d)(1).

¹⁸ Two cases brought charges under Rule 30(a) of Regulation S-P (the "Safeguards Rule") for failure to institute procedures reasonably designed to protect customer information. *In the Matter of Stephen Cheryle Bauman*, Exchange Act Release No. 60326, Admin. Proc. File No. 3-13551 (July 17, 2009) (CCO of broker-dealer failed to adopt or implement safeguard procedures); *In the Matter of Commonwealth Equity Services*, Exchange Act Release No. 60733, Admin. Proc. File No. 3-13631 (Sept. 29, 2009) (broker-dealer and investment advisor fined \$100,000 for failure to require installation of anti-virus software). In two other cases, the SEC charged violations of Rule 10(a) of Regulation S-P, for failure to limit disclosure of nonpublic customer information to nonaffiliated third parties. *In the Matter of Woodbury Financial Services*, Exchange Act Release No. 59740, Admin. Proc. File No. 3-13437 (Apr. 9, 2009); *In the Matter of Merriman Curhan Ford*, Exchange Act Release No. 60976, Admin. Proc. File No. 3-13681 (Nov. 10, 2009).

If you have any questions concerning this Memorandum, please contact:

Stephanie R. Breslow	+1 212.756.2542	stephanie.breslow@srz.com
Josh Dambacher	+44 (0) 20 7081 8044	josh.dambacher@srz.com
Ida Wurczinger Draim	+1 202.729.7462	ida.draim@srz.com
David J. Efron	+1 212.756.2269	david.efron@srz.com
Marc E. Elovitz	+1 212.756.2553	marc.elovitz@srz.com
Steven J. Fredman	+1 212.756.2567	steven.fredman@srz.com
Kenneth S. Gerstein	+1 212.756.2533	kenneth.gerstein@srz.com
Udi Grofman	+1 212.756.2298	udi.grofman@srz.com
Peter J. Halasz	+1 212.756.2238	peter.halasz@srz.com
Christopher Hilditch	+44 (0) 20 7081 8002	christopher.hilditch@srz.com
Daniel F. Hunter	+1 212.756.2201	daniel.hunter@srz.com
Jason S. Kaplan	+1 212.756.2760	jason.kaplan@srz.com
Eleazer Klein	+1 212.756.2376	eleazer.klein@srz.com
Kelli L. Moll	+1 212.756.2557	kelli.moll@srz.com
David Nissenbaum	+1 212.756.2227	david.nissenbaum@srz.com
Omoz Osayimwese	+1 212.756.2075	omoz.osayimwese@srz.com
Paul N. Roth	+1 212.756.2450	paul.roth@srz.com
Phyllis A. Schwartz	+1 212.756.2417	phyllis.schwartz@srz.com
George M. Silfen	+1 212.756.2131	george.silfen@srz.com
Marc Weingarten	+1 212.756.2280	marc.weingarten@srz.com
Jessica Sklute	+1 212.756.2180	jessica.sklute@srz.com

New York

Schulte Roth & Zabel LLP
919 Third Avenue
New York, NY 10022
+1 212.756.2000
+1 212.593.5955 fax

Washington, DC

Schulte Roth & Zabel LLP
1152 Fifteenth Street, NW, Suite 850
Washington, DC 20005
+1 202.729.7470
+1 202.730.4520 fax

London

Schulte Roth & Zabel International LLP
Heathcoat House
20 Savile Row, London W1S 3PR
+44 (0) 20 7081 8000
+44 (0) 20 7081 8010 fax

www.srz.com

U.S. Treasury Circular 230 Notice: Any U.S. federal tax advice included in this communication was not intended or written to be used, and cannot be used, for the purpose of avoiding U.S. federal tax penalties.

This information has been prepared by Schulte Roth & Zabel LLP ("SRZ") for general informational purposes only. It does not constitute legal advice, and is presented without any representation or warranty as to its accuracy, completeness or timeliness. Transmission or receipt of this information does not create an attorney-client relationship with SRZ. Electronic mail or other communications with SRZ cannot be guaranteed to be confidential and will not (without SRZ agreement) create an attorney-client relationship with SRZ. Parties seeking advice should consult with legal counsel familiar with their particular circumstances. The contents of these materials may constitute attorney advertising under the regulations of various jurisdictions.