Privacy Protections Required by Securities Firms: Compliance with the Evolving Regulatory Landscape

By Michelle L. Jacko

Introduction

The Gramm-Leach-Bliley Act ("GLB Act") imposes requirements upon financial institutions for safeguarding nonpublic personal information.[1] Through the GLB Act, Congress directed the Securities and Exchange Commission ("SEC" or the "Commission") and other federal agencies to adopt rules or regulations governing the protection of such information. Pursuant to this mandate, the Commission promulgated Privacy of Consumer Financial Information (Regulation S-P) ("Regulation S-P"),[2] which governs the treatment of nonpublic personal information about consumers by brokers, dealers, investment companies and SEC registered investment advisers.

Regulation S-P requires these institutions to adopt written policies and procedures to safeguard such information; provide a notice of these policies and practices to consumers upon commencement of the relationship and annually thereafter; describe the conditions under which they may disclose such information to nonaffiliated third parties; and provide a method for consumers to prevent such disclosure by "opting out" of that disclosure.

Despite Regulation S-P, there have been several incidents of information security breaches involving securities firms. These incidents have tended to fall into one of two categories. First, cyber-criminals and identity thieves have specifically targeted such firms to obtain access to nonpublic personal information. As a consequence, it has become apparent that many securities firms do not have adequate safeguards in place to prevent or detect these intrusions. Second, many firms have themselves improperly disposed of customer information, thereby unnecessarily exposing individuals to the risks of identity theft or unauthorized access to or use of their personal information.

Michelle Jacko, Managing Partner and Zachary Rosenberg, Law Clerk, Jacko Law Group, PC ("JLG"). JLG works extensively with investment advisers, broker-dealers, investment companies, hedge funds and banks on legal and regulatory compliance matters.

©2008, Michelle L. Jacko, Core Compliance and Legal Services, Inc and Jacko Law Group, PC

These incidents combined with technological and creative advances in the means of illegally accessing nonpublic personal information, have caused the SEC to propose significant amendments to Regulation S-P.[3] Many in the industry expect these proposals to be adopted in final form within the coming months and are discussed under *Overview of Proposed Changes* below.

However, before we can consider the proposed amendments in detail, it is important to understand some of the incidents that prompted the SEC to make these proposals, which highlight some of the deficiencies in Regulation S-P that the SEC is seeking to redress.

Background

As stated above, the SEC believes that many firms do not have adequate safeguards in place to prevent or detect intrusions from cyber-criminals and identity thieves. A good example of this type of breach can be seen in the alleged facts which gave rise to the SEC's recent institution of administrative proceedings against LPL Financial Corporation ("LPL").[4] Although these proceedings post date the Regulation S-P amendment proposals, the facts in question are highly illustrative of the types of security breaches the SEC wishes to prevent.

LPL, a registered broker-dealer, investment adviser, and transfer agent, allegedly detected several incidents of unauthorized access to the firm's internal online trading platform, in which the perpetrators attempted to place $700,000 worth of securities transactions in customer accounts. Prior to this, an internal audit performed by LPL had allegedly revealed significant problems in the firm's security control system which included weak passwords with no expiration, no automatic lockout feature after repeated unsuccessful attempts to login, and unreasonably long session timeout parameters.

Although the trades were either blocked or reversed, the SEC charged LPL with failing to have sufficient policies and procedures reasonably designed to protect customer records and information and failing to adequately respond to known deficiencies. Consequently, the SEC stated that LPL failed to take sufficient corrective action in response to its own audit, which ultimately led to the security breach incidents.

Although Regulation S-P requires securities firms to adopt written policies and procedures to safeguard nonpublic customer information, if such policies and procedures do not prevent or detect security breaches or are found to be insufficient, it is arguable that greater guidance should be given with stricter requirements imposed than Regulation S-P currently provides for.

Elsewhere, it has become apparent that by focusing on the relationship between a customer and a firm, Regulation S-P does not reflect the reality of many modern business relationships, where many customers consider the individuals they deal with to be their adviser or broker and not the firm that employs them. As a result, many firms have found themselves in contravention of Regulation S-P, when such individuals take customer information with them to their new firm and attempt to persuade their customers to follow them. This predicament was highlighted in the SEC's recent enforcement action against NEXT Financial Group, Inc ("NEXT").[5]

As part of its business practice, NEXT, a FINRA registered broker-dealer, recruited registered representatives from other broker-dealers in anticipation that they would bring their current customers with them. In order to facilitate the anticipated account transfers, NEXT encouraged the recruited representatives to disclose extensive nonpublic information about their customers so that NEXT could complete the necessary account transfer paperwork in advance. Such information was then disclosed to NEXT even though the customers in question had not consented to the disclosure or indeed the transfer of their accounts.

This information was indefinitely on the NEXT database, even if the customer never transferred his or her account to NEXT and even if the recruited representative who disclosed the information decided not to become a NEXT employee. In some situations, NEXT transferred information about these "non-customers" to third parties, such as its clearing firm, in expectation that the accounts would ultimately be transferred. Finally, if a representative chose to leave NEXT, NEXT openly allowed the representative to take nonpublic information about his or her customers in expectation that the customers would want to follow the representative away from NEXT.

None of these activities was disclosed in NEXT's Privacy Notice required to be provided to their customers.

In August, 2007, the SEC instituted administrative and cease-and-desist proceedings against NEXT for improperly disclosing nonpublic information about consumers to nonaffiliated third parties without providing consumers the opportunity to opt out, failing to ensure the security of customer records and information or protect against unauthorized access to such information, failing to provide customers with a clear and conspicuous notice of the firm's privacy policies, failing to disclose the categories of nonpublic personal information that will be disclosed, and aiding and abetting other broker-dealers' violations of Regulation S-P.

Although NEXT had breached the letter and arguably the spirit of Regulation S-P, the matter served to highlight an important inherent flaw: namely, its provisions make it extremely difficult for customers to transfer their accounts from one firm to another in order to stay with a trusted personal representative. This is because once that representative has transferred to a new firm, it will be hard for the representative to tell the customer about the move without using contact information obtained from the previous firm. If the representative uses such information, the previous firm will be in breach of Regulation S-P for failing to safeguard the information and the new firm will be in breach for aiding and abetting the previous firm's breach.

Overview of Proposed Changes

The proposed amendments strive to broadly address four things. First, they seek to expand the specific obligations of firms' privacy policies and procedures. Second, they broaden the scope of information covered by the safeguards and disposal rules. Third, they increase the types of entities covered by the safeguards and disposal rules. Fourth and finally, they set forth a limited exception from the notice and opt-out requirements to allow certain information-sharing in situations where representatives move from one brokerage or advisory firm to another. The specifics of these proposed changes are discussed briefly below.

Expansion of Privacy Policy and Procedures

The most significant expansion of Regulation S-P's coverage comes in the Commission's desire to impose more specific standards for safeguarding personal information and responding to security breaches. Under the proposed amendments, firms will be required to develop, implement, and maintain a "comprehensive information security program" that will consist of detailed written policies and procedures to address administrative, technical, and physical safeguards for protecting nonpublic personal information. The program should be customized so that it is "appropriate to the institution's size and complexity, nature and scope of its activities, and the sensitivity of any personal information at issue."[6]

[T]he SEC believes that many firms do not have adequate safeguards in place to prevent or detect intrusions from cyber-criminals and identity thieves.

Importantly, the proposals do not impose an absolute obligation on firms to protect customer information. Instead, a firm's program must be reasonably designed to protect against unauthorized access to personal information that could result in "substantial harm or inconvenience," which the Commission defines as "personal injury, or more than trivial financial loss, expenditure of effort or loss of time."[7]

However, in the event a security breach should occur, each program must set forth detailed written procedures for responding to incidents of unauthorized access to or use of personal information. These procedures should include providing notice to affected individuals as well as notice to the Commission or FINRA on the proposed Form SP-30, but only if the breach poses a significant risk of resulting in substantial harm or inconvenience to the affected individual or if an unauthorized person has intentionally obtained access to the information.

The proposal also provides several mandatory components for each security program, including a requirement to designate in writing one or

more employees to coordinate the program and to regularly test its effectiveness.[8] The "Privacy Officer(s)" will presumably be responsible for ensuring compliance with the other mandatory components of the program, which include, among other things, overseeing the operation, regularly testing and monitoring of the program and making any necessary adjustments and updates to the program as may be necessary following such testing and monitoring. All firms also will be responsible for training and supervising staff to implement the program, and for overseeing third-party service providers to ensure they maintain appropriate safeguards of the personal information entrusted to them.

Scope of Information Covered by the Safeguards and Disposal Rules

Current Regulation S-P safeguard rules necessitate that institutions maintain written policies and procedures to protect "customer records and information" while the disposal rule requires institutions to properly dispose of "consumer report information." In practice, applying similar types of protections with differing terminology is both confusing and potentially allows some information to be protected in one rule but not the other.

The most significant expansion of Regulation S-P's coverage comes in the Commission's desire to impose more specific standards for safeguarding personal information and responding to security breaches.

In an effort to ensure consistency in the scope of information covered by each rule, the proposed amendments will amend both rules so that they all apply to "personal information." This is defined to encompass records containing either "nonpublic personal information" or "consumer report information," both of which already are defined in Regulation S-P. In addition, this definition includes information handled by the institution that is identified with any consumer, employee, investor, or security-holder who is a natural person.[9]

Entities Covered by the Safeguard and Disposal Rules

The proposed amendments also will extend the safeguard rules, which currently applies to registered broker-dealers, investment advisers, and investment companies, to include registered transfer agents. Additionally, the disposal rule will be expanded to apply to associated persons of a registered broker-dealer, supervised persons of a registered investment adviser, and associated persons of a registered transfer agent.

Exception from the Notice and Opt-Out Requirements

The final and perhaps most controversial aspect of the proposed changes is the addition of a new exception to the notice and opt-out requirements of Regulation S-P. This exception will allow an SEC registered investment adviser or FINRA registered broker-dealer to share limited customer information with another such firm when a representative of the first firm leaves to join the second firm. The reason behind this exception is to address some of the deficiencies identified in NEXT by enabling departing representatives to contact their former customers to provide them with the opportunity to follow their representatives to the new firm. As such, only information necessary for this purpose may be shared and this is expressed to include only the customer's name, contact information and general information about the types of accounts and products held by the customer. In order to protect a customer from the risks of identity theft, account numbers, social security numbers and specific securities positions will be expressly excluded from the exception.

It is important to note that the exception can be relied upon only by the firm the representative is departing and even then, the representative must inform that firm of the information he or she wishes to share before leaving the first firm. If that firm does not want the representative to take his or her clients, it can decline to invoke the exception. Although this would appear to give no new rights to representatives, firms should consider the risk that representatives may take confidential customer information with them anyway, which could constitute unauthorized access to personal information if the customer has not granted

permission to do so and consequently, and could result in substantial harm or inconvenience to the firms. Therefore, by relying on the exception, firms can control the information that is being shared, which they would not be able to do if it is retained by a departing representative without their knowledge.

Practical Implications and Challenges for Firms

As expected, once the proposed changes are adopted in final form, compliance with the various requirements will prove to be quite costly, particularly for smaller firms.

Much of these increased costs will be due to some inherent uncertainty in the proposed changes. For example, the proposed amendments require firms to develop, implement and maintain a comprehensive information security program, a concept which implies that the programs will be all-inclusive and wide-ranging in scope. Without more objective guidance, firms may have difficulties in determining whether an adopted program is sufficiently comprehensive to satisfy the rule.

This problem may be exacerbated because the Commission goes on to say that the program should be "appropriate to the institution's size and complexity, nature and scope of its activities, and the sensitivity of any personal information at issue." This suggests that what may be comprehensive for one firm will not be comprehensive for another. Consequently, this will make it difficult for firms to purchase an off the shelf program or look to their contemporaries for potentially transferable solutions to privacy problems.

As a result, firms will need to spend a great deal of time and money just to establish what they believe to be a suitably comprehensive program, either by allocating internal resources to the task or by hiring outside consultants.

In addition to the costs incurred in establishing a privacy program, firms also will need to expend additional staff hours and more of their operating budget on training, operating, reviewing and updating their programs. For example, costs could be increased should the firm need to hire a new employee for appointment as its Privacy Officer. Similarly, a firm may need to increase compensation for a designated employee due to intensified workload and responsibilities, and/or enhance technology solutions for detecting potential privacy breaches, which will result in additional firm expenses.

Other specific elements of the proposals also will lead to increased costs. The proposed amendments to the disposal rule extends coverage to associated persons of registered institutions and requires firms to consider safeguards for those employees who maintain information on their home computers, laptops, and blackberries. These amendments could potentially impose significant costs in supervising employees' activities conducted away from the office and in documenting the proper disposal of information contained in their personal computers.

Although Regulation S-P requires securities firms to adopt written policies and procedures to safeguard nonpublic customer information, if such policies and procedures do not prevent or detect security breaches or are found to be insufficient, it is arguable that greater guidance should be given with stricter requirements imposed than Regulation S-P currently provides for.

Moreover, the requirements for providing notice to affected individuals and the Commission may result in substantial practical compliance problems for firms. The proposed rules require notice to individuals if an incident of unauthorized access has occurred or is "reasonably possible," and such a standard may give rise to notifications and warnings of non-material issues or incidents where the likelihood of misuse is theoretically possible, although extremely unlikely. Such a standard may cause firms to err on the side of caution, with increased burdens and costs and the likelihood that individuals will be over-notified and thus may not take such warnings seriously when there is a real threat of harm.

Similar concerns may arise over the proposed requirements for notification to the Commission on Form SP-30, which is required as soon as possible after the firm becomes aware of any incident of unauthorized access to or use of personal information in which there is a significant likelihood of substantial harm or inconvenience or where an unauthorized person has intentionally obtained access to sensitive personal information. The proposed form requires a significant amount of detail, which may take time to properly evaluate, giving rise to the possibility that a firm is forced to choose between notifying the Commission "as soon as possible" before all information has come to light or waiting to submit the Form until it can be substantially completed. The former may require additional costs to be incurred by the firm if material information is subsequently uncovered and Form SP-30 is thereafter required to be updated. The latter option poses the risk that the delayed notification would be a violation of the rule and potentially prevent the Commission from taking further action to protect any affected individuals.

Aside from resulting uncertainty and potentially increased costs, certain aspects of the proposed amendments also pose significant compliance obligations on firms that attempt to tailor their programs to the specific requirements of the proposed changes. Most notably, one aspect of the proposed comprehensive information security program requires firms to "regularly test or otherwise monitor and document in writing the effectiveness of the safeguards' key controls, systems, and procedures, including the effectiveness of access controls on personal information systems, controls to detect, prevent and respond to attacks, or intrusions by unauthorized persons, and employee training and supervision . . . ."[10]

One particularly effective method for testing a firm's data security systems is to employ the techniques and methods that a criminal hacker may use to break through the perimeter firewalls and gain access to nonpublic personal information. This practice is known as "ethical hacking" and is perhaps the most effective means of testing a firm's privacy protections, but such conduct may unintentionally lead to violations of other laws or contractual provisions if certain precautions are not taken.

In order to ensure the legality of ethical hacking without undermining its effectiveness, firms should take care to provide the person or persons conducting the test with specific written guidelines as to what techniques may be used, how far into the system the tester is permitted to access, and who is entitled to receive reports of the results of the tests. Any individual involved in the ethical hacking process should be carefully screened, pass a thorough background check, and otherwise prove satisfactory for such a role through a history of loyalty or trustworthiness regarding the use of potentially damaging information. It is also imperative that the terms and conditions governing the conduct of the testers remain consistent with the firm's internal privacy policies and procedures, the privacy notices delivered to customers, and any contractual limitations or specific restrictions placed on such conduct by consumers. For example, privacy notices should notify consumers that the firm may disclose information under circumstances permitted or required by law, including steps reasonably necessary to ensure the adequacy of the firm's financial records.[11]

Other Related Laws and Regulations

As if the above-enumerated complications were not enough, the privacy requirements of Regulation S-P are not the only considerations that must be taken into account in designing a firm's privacy policies and procedures. Various state laws often impose additional and sometimes conflicting obligations upon firms doing business under their jurisdiction. Regulation S-P was adopted under Title V of the GLB Act, and controls the privacy obligations of financial institutions subject to the federal jurisdiction of the SEC. However, the GLB Act specifically allows for state laws to provide greater protection than those provided under the GLB Act, so long as they are not contradictory to those set forth in the federal scheme.[12] Thus, financial institutions must be cognizant of specific protections provided for under state laws in which the firm has offices, conducts business with consumers, or otherwise engages in financial services.

One notable example of a state privacy law offering greater protections than the federal system is California's Financial Information Privacy Act, known as SB-1, which imposes upon firms af-

firmative consumer opt-in requirements before firms may share certain types of information with non-affiliated third parties.[13] Although SB-1 was recently partially preempted under the Fair Credit Reporting Act, the majority of the law's protections remain intact. Other states have similar limitations and requirements, and firms should be aware of these provisions to ensure that they are in compliance with all applicable laws.[14]

In addition to state privacy laws, securities institutions may also be affected by the Red Flag Rules of the Federal Trade Commission ("FTC").

In June, 2008, the FTC and the federal banking regulators issued joint regulations implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act ("FACT Act"). Known as the "Red Flag Rules", *financial institutions* and *creditors* with *covered accounts* are required to develop and maintain written identity theft prevention programs for the detection, prevention, and mitigation of identity theft in connection with the opening of certain accounts or certain existing accounts.[15] Enforceable in May 2009, the identity theft program must be able to detect, identify, and respond to indicators of possible fraudulent activity that, when detected, should prompt creditors to determine if there is any fraudulent activity afoot.[16]

To be subject to the FTC's rules, a securities institution must first fall within the FACT Act's definition of either a "creditor" or a "financial institution." A "creditor" is an entity that is regularly involved with the extension, renewal or continuation of credit.[17] A "financial institution" includes banks, credit unions, savings and loans, but also any other person holding a transaction account either directly or indirectly belonging to a consumer.[18] For this purpose, a "transaction account" means a deposit or account on which the depositor or account holder is permitted to make withdrawals by negotiable or transferable instrument, payment orders of withdrawal, telephone transfers, or other similar items for the purpose of making payments or transfers to third persons or others.[19]

Ordinary securities activities will not cause most institutions to fall into either category. However, if these institutions provide ancillary services or are registered as something other than a broker, dealer, investment company or investment adviser, they could still be caught by these provisions.

Certain broker-dealers may fall under the definition of a creditor if they extend credit to customers as part of their regular business by allowing them to trade on margin. Other broker-dealers may be deemed to be financial institutions if they maintain custodial accounts which allow customers to make multiple account withdrawals for the purposes of payments and transfers to third parties. Similarly, some mutual funds allow investors to direct redemption payments to be made to third parties. This too would convert the fund into a transaction account and consequently make the fund a financial institution.

As long as a securities institution conducts activities causing it to fall under the FTC's jurisdiction, all activities performed by that institution will be subject to the Red Flag Rules. For example, although most investment advisers do not maintain custody of client accounts or advance funds to clients as part of their advisory business, a true "dual registrant" (*i.e.,* a firm registered both as a registered investment adviser and broker-dealer with the SEC) may need to comply if the firm's broker-dealer business falls within the definition of a financial institution or creditor

To be subject to the Red Flag Rules, the securities institution must not only fall within the definition of a creditor or a financial institution but, also hold "covered accounts" for its customers. The term "covered account" means an account used primarily for personal, family or household purposes which allows for multiple transactions or payments and also to "[a]ny 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."[20] In practice, most accounts held by securities firms or investment companies will fall within the definition of a covered account. This is because personal and non-public information is used in opening and maintaining accounts or investment company interests and this poses a reasonably foreseeable risk of identity theft which is likely to qualify the account as a covered account for the purposes of the Rules.

Similar to the proposed revised Regulation S-P, the Red Flags Rules allow businesses great flexibility in designing an identity theft prevention program suitable to the nature of a company's business operations as well as appropriate for their size and capabilities.[21] As guidance to assist businesses in designing and implementing a written identity theft prevention program, the FTC identified 26 possible red flag indicators to serve as examples for creditors to use as a starting point. For more information regarding the possible red flag indicators, please visit http://edocket.access.gpo.gov/2007/pdf/07-5453.pdf.

Regardless of whether the firm is indeed subject to the FTC's jurisdiction, all securities firms should pay close attention to the Red Flags Rules. When considering its proposals to amend Regulation S-P, the SEC looked at the regimes imposed by its fellow regulators in an attempt to promote consistency between its rules and guidelines and those of the other federal agencies that oversee the financial services industry. Many of the proposed changes to Regulation S-P discussed above appear to resemble closely certain rules of the FTC. It is therefore possible that the SEC may take its cue from the Red Flag Rules and impose similar requirements on securities firms, either in further revisions to Regulation S-P or in future regulations.

Conclusion

Compliance with privacy laws and regulations can be a daunting task for financial institutions with varying requirements among the several states and conflicts between state and federal law. Ensuring the privacy of financial information is an important obligation of all financial institutions. As technology continues to advance, privacy considerations are becoming more prevalent than ever before as unauthorized access to nonpublic personal financial information becomes easier to accomplish and harder to detect.

ENDNOTES

1 15 U.S.C. §§ 6801-6827.
2 17 C.F.R. § 248.
3 Part 248 - Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information, Exchange Act Release No. 57427, Investment Company Act Release No. 28178, Investment Advisers Act Release No. 2712 (Mar. 4, 2008) *available at* http://www.sec.gov/rules/proposed/2008/34-57427.pdf.
4 *In re* LPL Financial Corp., Exchange Act Release No. 58515, Investment Advisers Act Release No. 2775 (Sept. 11, 2008) *available at* http://www.sec.gov/litigation/admin/2008/34-58515.pdf.
5 *In re* NEXT Financial Group, Inc., File No. 3-12738 (Aug. 24 2007), *available at* http://www.sec.gov/litigation/admin/2007/34-56316-o.pdf.
6 73 Fed. Reg. 13,695.
7 *Id.*
8 *Id.* at 13,695-96.
9 *Id.* at 13,699.
10 *Id.* at 13,696.
11 For more information regarding the legal implications of ethical hacking, see Ronald I. Raether Jr., *Data Security and Ethical Hacking: Points to Consider for Eliminating Avoidable Exposure*, 18 Bus. L. Today No. 1, (Sept.-Oct. 2008) *available at* http://www.abanet.org/buslaw/blt/2008-09-10/raether.shtml.
15 U.S.C. § 6807.
12 *Id.*
13 *See* Cal. Fin. Code §§ 4050-4060.
14 Although the extent of the Fair Credit Reporting Act's preemption provision is beyond the scope of this article, federal preemption adds additional complexity to a firm's privacy program. While the provision has the effect of minimizing burdens on firms imposed under state law, the extent of its application is far from certain.
15 16 C.F.R. § 681.2. See also, FTC Business Alert, *New 'Red Flag' Requirements for Financial Institutions and Creditors Will Help Fight Identity Theft*, *available at* http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.pdf.
16 *Id.*
17 16 C.F.R. § 681.2(b)(5).
18 15 U.S.C. § 1681a(t).
19 12 U.S.C. § 461(C).
20 16 C.F.R. § 681.2(b)(3).
21 FTC Business Alert, *supra* note 19.

This article is reprinted with permission from *Practical Compliance and Risk Management for the Securities Industry,* a professional journal published by Wolters Kluwer Financial Services, Inc. For more information on this journal or to order a subscription to *Practical Compliance and Risk Management for the Securities Industry,* go to **onlinestore.cch.com** and search keywords "practical compliance"