

May 12, 2008

Ms. Nancy M. Morris  
Secretary  
U.S. Securities and Exchange Commission  
100 F Street, N.E.  
Washington, D.C. 20549

**Re: File Number S7-06-08  
Privacy of Consumer Financial Information and Safeguarding  
Personal Information**

Dear Ms. Morris:

The Financial Planning Association (“FPA”)<sup>1</sup> welcomes the opportunity to comment on the Securities and Exchange Commission’s (“Commission” or “SEC”) proposed amendments to Regulation S-P, concerning privacy of consumer financial information and the safeguarding of personal information.

FPA supports the proposed amendments. Safeguarding client data has long been required for financial planning practitioners by the CFP Board of Standards, Inc.,<sup>2</sup> in its *Code of Ethics and Professional Responsibility*.<sup>3</sup> On July 1, 2008, these standards are being updated to strengthen those protections. Broadly speaking, the amendments in this proposal provide better guidance and more clarity to financial planners and other registrants in applying the Commission’s safeguarding and disposal requirements under Regulation S-P. The amendments also allow for greater flexibility and efficiency in transferring client accounts from one firm to another, consistent with clients’ expectations and wishes. FPA would like to take this opportunity to comment on certain specifics of the proposed amendments that we believe need to be addressed to better ensure customer privacy and to avoid unnecessarily burdening smaller registrants.

---

<sup>1</sup>The Financial Planning Association is the largest organization in the United States representing financial planners and affiliated firms, with approximately 28,000 individual members. Most are affiliated with investment adviser firms registered with the Securities and Exchange Commission or state securities administrators, and more than one-half are affiliated with broker-dealers. FPA is incorporated in Washington, D.C., where it maintains an advocacy office, with headquarters in Denver, Colo.

<sup>2</sup> Certified Financial Planner Board of Standards Inc. (CFP Board) is a separate nonprofit organization whose goal is to benefit and protect the public by establishing and enforcing education, examination, experience and ethics requirements for persons authorized to use its certification marks. CFP Board is the largest such organization in the U.S. with more than 55,000 CFP® certificants.

<sup>3</sup> See Rule 501, Rules that Relate to the Principle of Confidentiality, and Rule 610, Rules that Relate to the Principle of Professionalism.

## I. Transferring Client Information.

### A. Generally.

As required by the Gramm-Leach-Bliley Act ("GLBA")<sup>4</sup>, the SEC promulgated regulations relating to consumer and customer privacy. Implementing GLBA, Regulation S-P provides, in part, that financial institutions regulated by the SEC inform customers about their privacy policies and practices, and limits the circumstances in which a financial institution may disclose nonpublic personal information about a consumer to a nonaffiliated third party without first giving the consumer an opportunity to "opt out" of the disclosure. Regulation S-P includes exceptions<sup>5</sup> to the notice and opt-out requirements, such as for law enforcement purposes, reporting to a consumer reporting agency, or in other limited circumstances. The proposed amendment would expand this list of exceptions to include allowing a broker, dealer or SEC-registered investment adviser to share customer information with another broker, dealer or SEC-registered investment adviser for the purpose of allowing a representative departing one firm to solicit customers to whom the representative personally provided a financial product or service. The proposed amendment recognizes that in many circumstances, clients consider their "relationship" to be primarily with an individual professional ("representative" or "principal"), rather than with the firm with which the representative is affiliated. It also recognizes the disruption caused to clients who would wish to maintain their relationship with a transferring representative when the representative is unable to take even basic customer contact information to their new firm.

FPA believes the intent of the proposed amendment - to ensure the client retains control over his or her personal account information - is fundamental to the process of financial planning. We note former NASD Chief Robert Glauber focused on the issue of customer control when the NASD announced its rule interpretation on account transfers in 2001.<sup>6</sup> As such we believe the proposed amendment strikes a proper balance between the need for a client to maintain personal control, while facilitating transfers in a manner consistent with the clients' expectations and needs. However, we suggest that the language of the proposed amendment should be modified to provide clearer protection for client information. Because this is an exception to a critical consumer protection, the information that may be shared should be limited to only that which is minimally required to assist in obtaining an affirmative consent by the client to transfer his or her account(s). Further, we must keep in mind that notwithstanding client expectations and wishes, it is

---

<sup>4</sup> 15 U.S.C. 6801 et seq.

<sup>5</sup> 17 C.F.R. § 248.15

<sup>6</sup> "It is a fundamental right of an investor to choose with whom he or she does business, and the fact that a broker changes firms should not affect an investor's ability to continue to access his or her account and to do business with that broker," said Robert R. Glauber, Chairman and CEO of the NASD. *NASD Press Release*, December 26, 2001.

<http://www.finra.org/PressRoom/NewsReleases/2001NewsReleases/P002972>

the firm, not the representative that bears the legal obligation to safeguard customer information.

That said, however, the proposal appears to address the typical scenario of a registered representative leaving a broker-dealer, or an independent contractor severing a relationship with a firm, similar situations may arise with small financial planning firms in which a firm dissolves or one equity partner leaves and whose clients prefer to remain with their personal advisor. The proposal does not seem to contemplate such a situation, where the principal has a clearer relationship with the client and an "ownership" interest in the client information. If a principal is departing a firm, it may not be appropriate for the other principals to be able to withhold information on clients with whom the principal has a relationship. FPA believes the Commission should consider a different standard if the departing "representative" is a principal or owner of a firm. Section 248.15(a)(6), which is an exemption for sales, mergers, or other business transfers contemplates an analogous situation and perhaps should be amended to address this circumstance.

*B. Scope of Client Information.*

The proposed amendment provides, in part, that the client's information that may be shared under this exception is "limited" to the client's name and contact information (phone, address and email), and "a general description of the type of account and products held by the customer." The proposed amendment further specifies certain client information that *cannot* be taken: account numbers, social security numbers and securities positions. Read together, these two provisions create uncertainty. If the information that can be taken is truly "limited," then there would be no need to specify what cannot be taken. And by specifying what cannot be taken, the Commission is inviting a broader interpretation of the "limited" information may be taken. We believe that given the record established by the Commission in the NEXT Financial case,<sup>7</sup> there is ample reason to believe that the market may indeed broadly interpret the language of this amendment, as currently drafted.

Keeping in mind the primary goal of protecting client information and secondary goal of facilitating transfers of confidential client data, we suggest that the Commission be more explicit that the information that may be taken is strictly limited to contact information (e.g., telephone, email, address) and only a very brief description of the account type(s) the customer holds. We believe this is what the Commission intended in referencing a "general description" of the account(s) and product(s) held by the client, but we are concerned that a broad interpretation of "general description" could lead to representative taking more detailed client information than would be necessary to merely facilitate a transfer of data.

---

<sup>7</sup> *In re NEXT Financial Group, Inc.*, Exchange Act Release No. 56316 (Aug.24, 2007), <http://www.sec.gov/litigation/admin/2007/34-56316.pdf>.

We also note that the proposed exception is limited to information on clients with whom the representative or principal has “personally provided a financial product or service.” Consistent with this limitation, we think it is appropriate to limit any product information that may be taken only to those accounts and products for which the representative personally provided service to the customer. So, for example, if the customer maintained an IRA account, brokerage account and advisory account with a firm, and the representative only serviced the IRA, the representative should not be permitted to take even very minimal information about the other accounts which he did not service.<sup>8</sup>

C. Independent Contractors.

In order for a firm to avail itself of the exception it must require the transferring representative to provide it with a written record of the information that will be disclosed to the representative’s new firm not later than the representative’s separation from employment with you. FPA considers this provision to be of critical importance and is pleased that the SEC is requiring such a record. However, the reference to the separation from employment is too limited, insofar as it does not seem to contemplate a transfer of an independent contractor – the circumstance most likely to involve this voluntary sharing of customer information. The proposed amendments should be modified to reflect transfer of an independent contractor.

D. Additional Safeguards.

Consistent with the intent of the proposed amendments, we believe further safeguards should be provided to protect consumer information. Specifically, the exception is simply intended to facilitate transfer of client data, if the client wishes to maintain his relationship with the principal or representative. Therefore, the new firm with whom the information is shared should be restricted from further sharing that information with either affiliated or unaffiliated parties unless and until the client affirmatively approves a transfer, establishes a client relationship with the new firm, or otherwise affirmatively consents to allowing the information to be shared. This would provide an important safeguard while still facilitating an account transfer. Similarly, there should be a time limit placed on maintaining the information if the client declines to transfer accounts or otherwise establish a relationship with the new firm. The time limitation should reflect what would be reasonably required to facilitate a transfer. After such time (e.g., 90 or 120 days), the new firm should be required to dispose of the client information unless the client establishes a relationship with the new firm or affirmatively consents to allowing the new firm to maintain the information.

E. Scope of Rule.

The proposed amendments generally cover the sharing of information between SEC registrants. We note that state-registered investment advisers are beyond the scope of the rule and SEC jurisdiction. We would strongly encourage the Commission to work with the Federal Trade Commission to adopt a similar rule to facilitate transfers for state-

---

<sup>8</sup> However, in the situation of a departing principal, discussed above, it would be appropriate to allow for the transfer of more comprehensive client information.

registered advisers and their clients. Moreover, transfers of client information could become even more complicated if the representative was changing affiliations between an SEC and state-registered investment adviser, if agencies promulgate different rules for the handling of personal client data.

Finally, the proposed amendments properly reflect that the sharing of client information contemplated by this exception is at the discretion of the firm that is responsible for safeguarding customers' nonpublic information. We believe the Commission's approach is wise. Given the firm's legal responsibilities, it would be inappropriate to establish this exception as a right of the transferring representative.<sup>9</sup> Aside from undermining the firm's legal responsibilities, to do so would create an inconsistency with legal binding and legitimate non-compete agreements that are common in the industry.

## II. Safeguarding Rule.

### A. Comprehensive Security Program

FPA supports the goals of the proposed amendment to the safeguarding rule.<sup>10</sup> Greater specificity as to what is required to provide adequate information security is helpful to financial services firms looking to protect their customers' information. Likewise, requiring notification to customers when their personal information has been compromised is not only the appropriate thing to do for the customer, but may be necessary to mitigate any harm that may come from the unauthorized use of the information (*discussed separately below*). The proposal also continues to appropriately reflect that flexibility is needed and that firms' should largely be permitted to develop programs that best fit their particular needs and those of their clients. However, we have some concern that the costs to small firms of implementing some of the mandates may be disproportionate to the risks. We suggest, therefore, that the Commissioner consider whether some of the mandates may be more appropriately put forth as guidance, allowing for more flexible application to small firms.

Currently, the SEC requires firms to maintain written safeguarding policies and procedures (administrative, technical and physical) reasonably designed to: (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 customer records and information; and (3) Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer. Though a rather broadly stated rule, it does essentially require that firms have taken reasonable steps to protect customer information.

The proposed amendment to the safeguarding rule would expand include more specific requirements in developing, implementing and overseeing a program to protect customer information. These include:

---

<sup>9</sup> Though, again, it may be appropriate to permit a principal to retain certain client information.

<sup>10</sup> 17 U.S.C § 248.30(a)

- Development, implementation and maintenance of a comprehensive information security program;
- Designation of an employee or employees to coordinate the information security program;
- Identification, in writing, of reasonably foreseeable risks and implementation of safeguards to control those risks;
- Testing/monitoring of safeguards' key controls, systems and procedures, and maintaining a record of the testing/monitoring;
- Employee training;
- Overseeing service providers; and
- Ongoing adjustment of the program.

FPA generally agrees with the SEC that these are key elements of a comprehensive information security program. For the vast majority of firms, it would be appropriate to consider these elements as essential to a program that is reasonably designed to protect customer information. As such, they should serve as a guide as to reasonable steps firms should take in developing an adequate information security program. However, for some firms, the totality of the requirements would be very burdensome and may be disproportionate to the risks they face. Put differently, some firms may spend an inordinate amount of time and money on complying with the mandates without materially enhancing protection of customer information.

FPA supports the Commission's proposal to amend the safeguarding rule to require that firms must not merely adopt written policies and procedures, but must "develop, implement and maintain a comprehensive security program." We also support the concept that the program should reflect the firm's size, complexity, scope of activity and sensitivity of the personal information. In sum, we support proposed section 248.30(a)(1) and (2).

As discussed above, FPA suggests that the specific safeguarding requirements of section 248.30(a)(3) may more appropriately serve as guidance to firms as to the elements their programs should include. As such, they can still be enforceable, as they reflect reasonable steps that should be taken to safeguard customer information in many circumstances. However, the Commission would have the flexibility to determine that each and every element may not be necessary as a minimum requirement for each and every firm. Alternatively, the proposal could be amended to recognize some circumstances in which each and every element may not be required. The flexibility reflected elsewhere in the proposal would seem appropriate to apply also to section 248.30(a)(3).

Finally, whether or not the provisions of section 248.30(a)(3) remain absolutely mandatory, all firms would benefit from guidance as to what their responsibilities would be in overseeing service providers. For example, to what extent could they rely on annual certifications from the service provider regarding compliance? Would independent audits be required of some service providers? Would on-site inspection be required? The proposal clearly contemplates that service providers have a significant

role in protecting customer information. Understanding the oversight responsibilities required is critical to firms availing themselves of these services. We urge the Commission to permit reliance on representations of these service providers to the fullest extent possible. In many instances, auditing and inspections will place an undue burden on firms and service providers alike, without an appreciable benefit. The benefits of detailed service provider oversight must be weighed against the costs and burdens of conducting that oversight.

**B. Unauthorized Access**

FPA supports requiring notification of appropriate regulatory or law enforcement authorities as well as individual customers when there has been unauthorized access to or use of personal information. The provisions of section 248.30(a)(4) and (5) are generally appropriate to safeguarding customer information and mitigating harm caused by the unauthorized access to and use of nonpublic personal information.

FPA suggests that proposed section 248.30(a)(4)(iv) be modified, however. That section requires that customers be notified “as soon as possible” when their information has been compromised and misuse is reasonably possible. The “as soon as possible” standard is too strict and taken literally will require contacting the customer while and breach is still being assessed. With incomplete information, customers are likely to benefit little from knowledge of the incident. In fact, such hasty communication could lead an individual to take unnecessarily broad precautionary measures that may lead to greater personal inconvenience (e.g., cancelling all credit and debit cards). Further, the standard seems to contradict the same paragraph that provides that a firm can delay notification if it receives a written notice from an appropriate law enforcement agency that the notice will interfere with a criminal investigation. Unless knowledge of any breach results from such a notice, this exception has no applicability because the customer will have been notified before a law enforcement agency has had an opportunity to inform the firm that such notice would interfere with a criminal investigation. FPA suggests that the notice be required within a “reasonable” time, rather than as soon as possible.

**III. Conclusion.**

FPA supports the goal of facilitating transfers, consistent with clients’ privacy rights and control over their own information. We believe the proposed amendments strike a reasonable balance and properly account for the responsibility of firms in protecting customer information. We believe, however, that additional safeguards and clarification are needed in order to fully ensure that customers control their own information and that the proposed exception is utilized only as intended – that is, to facilitate a customer’s transfer consistent with his or her wishes.

FPA believes the exception to sharing customer information generally contemplates a broker-dealer and independent contractor model. For smaller financial planning firms, with a few principals, the business model is different. We suggest that the SEC consider

an alternatives which would allow a departing principal to retain certain customer information, even if the other principals object.

FPA is concerned about the detailed safeguarding amendments that the Commission is proposing. While we support the goals of these amendments and welcome the additional guidance they provide for our members, they lack needed flexibility and would saddle firms with compliance burdens and costs that in some instances would not be justified by any commensurate enhancement of information security. The current safeguarding rule is sufficiently broad to ensure SEC oversight of safeguards, though additional guidance would be helpful for registrants and SEC staff.

If you have any questions, or if FPA can provide additional information, please contact me at 202-449-6343, or [dan.barry@fpanet.org](mailto:dan.barry@fpanet.org).

Sincerely,

A handwritten signature in black ink, appearing to read 'D. Barry', with a horizontal line extending to the right.

Daniel J. Barry  
Director of Government Relations