Christopher P. Gilkerson
Senior Vice President, Deputy General Counsel
Charles Schwab & Co., Inc.
101 Montgomery Street
San Francisco, CA 94104

tel 415.636.3667 fax 415.636.5239

charles SCHWAB

May 12, 2008

SUBMITTED VIA EMAIL

Nancy M. Morris
Secretary
United States Securities and Exchange Commission
100 F Street, N.E.
Washington, DC 20549-1090

Re: File Number S7-06-08; Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information

Dear Ms. Morris:

Charles Schwab & Co., Inc. ("Schwab") appreciates this opportunity to comment on the proposed amendments to Regulation S-P. Schwab believes in the importance of effective and diligent safeguarding of customer information, and supports the mandate of the Gramm-Leach-Bliley Act ("GLBA") to protect consumers and provide them with clear disclosure regarding the use, storage and disposal of their personal information.

The proposed amendments largely achieve the Commission's goal to provide additional industry guidance for the safeguarding and disposal of customer records and information and for responding to data security breaches. Schwab, like other firms that have banking affiliates, has developed standards consistent with the FFIEC Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice dated March, 2005 ("FFIEC Guidance") regarding the safeguarding of data and the establishment of a breach response program. We would like the Commission to consider modifications to avoid requirements that are inconsistent with banking regulatory requirements. Specifically, the definitions of "sensitive personal information" as well as the standard of "substantial harm or inconvenience" should be closely aligned with the standards in the FFIEC Guidance. With respect to these definitional issues, Schwab supports the comments and suggestions in the Securities Industry and Financial Markets Association (SIFMA) letter.

Our letter discusses three main concerns: (1) the "departing representative" proposed exception to notice and opt-out, and a customer permission-based and customer choice approach to the issue of representatives who leave one firm to join another, (2) the burdens of proposed Form SP-30 and clarification of the regulatory notice requirement, and (3) the defined term "service provider" and avoidance of unnecessarily duplicative requirements when two separate firms have direct relationships with the same customer.

A. The Proposed Exception for Departing Brokers and Customer Permission

We agree with the Commission that investors have a right to choose the firm with which they hold their accounts. We also believe that representatives of broker-dealers and investment advisers should be able to leave one firm and join another or to start their own firm without undue regulatory impediments. These important public policy goals are attainable in an approach that is based on the GLBA principles of customer permission and consent.

The Commission states that the purpose of the proposed exception is to allow (not require) a firm with a departing representative to share limited customer information with the representative's new firm. The goal is to provide a safe framework under which a firm with a departing representative can choose to disclose certain customer contact information to the representative's new firm and can supervise the information transfer. The representative would use this information to contact the customers he or she serviced to inform them of the representative's association with a new firm. This purpose applies to those firms where the representative has brought customers to the firm through her own efforts, not where a firm has obtained the clients and assigned the representative to service them. Accordingly, the exception is a voluntary one, which would not likely be of interest to firms that do not follow a "wirehouse" or independent adviser business model and have a policy prohibiting representatives from taking any customer data.[1]

Schwab is sympathetic to the rule's intended purpose, and that purpose can be met while assuring customer choice and privacy protections. Unfortunately, under the proposal as currently drafted, if a firm has elected to rely upon the proposed exception, any representative who can claim to have "personally provided a financial product or service" to a customer can download or copy that customer's contact information, account type, and products purchased and walk out of the office with it upon resignation. The only requirement is to provide the departing firm a written record of the information the representative has copied or removed. Without more guidance from the Commission, this could create a gap in privacy protection. Depending on how information transfer occurs, a departing representative may not be subject to safeguarding protocols or disposal rules unless and until he comes to work at a registered firm and that data comes to rest within the new firm.[2]

---

[1] The purpose of the proposed exception may be complementary to the "Protocol for Broker Recruiting." Under the Protocol, which has been signed by a limited number of firms, a signatory firm agrees not to file claims against another signatory firm or a representative when that representative leaves with certain limited customer information and joins the other firm. Under the Protocol, "to ensure compliance with GLBA and SEC Regulation SP, the new firm will limit the use of the Client Information to the solicitation by the [representative] of his or her former clients." For a wirehouse or independent advisor business model, the Protocol serves a legitimate business interest. Under any business model, meeting the reasonable privacy expectations of customers is important.

[2] The Commission should consider whether an exception that is not permission-based is consistent GLBA. Although GLBA permits the SEC to grant exceptions to the disclosure rules, they must be "consistent with the purposes of" the Act, 15 U.S.C 6804(b), and "consistent and comparable with the regulations prescribed by other such agencies and authorities," 15 U.S.C 6804(a)(2). The proposed exception, in its current form, runs a risk of being construed as inconsistent with various federal banking rules and state privacy laws as well as the public's demand for more privacy choices.

The Commission might better serve the customer choice purpose of the proposal consistent with customer privacy protections if, instead, it provided guidance as to how firms and their representatives can meet an already existing exception to the notice and opt-out requirements that is consistent with GLBA: Rule 15(a)(1). This customer permission exception allows disclosure "with the consent or at the direction of the consumer, provided that the consumer has not revoked the consent or direction."

To meet this exception, for example, firms which elect to do so consistent with their business models could include a provision in their account agreements reflecting an understanding with their customers that if the representative who is responsible for the customer relationship leaves to join another firm, the representative may retain contact and basic account information. A customer who signs the agreement or who maintains the account after receiving notice of the clarification of account terms provides "consent and direction." In the alternative, when consistent with a firm's policies and procedures, at the time of departure a customer should be able to provide consent or direction that allows the representative to maintain limited contact information about the customer and account in order for the representative to contact that customer at the representative's new firm.[3] This approach applies, for example, with the independent broker model where the customer essentially hired the representative, not the firm at which the representative is associated.

If the SEC is concerned about promoting investor choice or ease of account transfer to enable a customer to follow a representative to a new firm, there are more direct ways to pursue that goal. A new rule might require firms to provide the departing representative's contact information at a new firm if a customer requests it. Or a new rule might focus on removing any arbitrary delays in transferring accounts.[4]

If instead of the above alternatives the Commission moves ahead with the proposed exception, it should consider changes that would clarify the scope and better uphold customers' reasonable privacy expectations. The rule text should state as a condition that a firm's policies and procedures must expressly address and permit the customer information disclosure in order for the exception to apply. The rule should also more clearly define the representatives who appropriately may take advantage of the new exception and how they may use the information. Therefore the rule text should be revised (changes and additions underlined) to apply:

> To a broker, dealer, or investment adviser registered with the Commission, <u>provided that your policies and procedures expressly allow the transfer of limited customer contact and</u>

[3] As some firms do today, firms could simply follow Regulation S-P's notice and opt-out provision by including a short explanation of their policy relating to departing brokers in their privacy policy. The proposing release fails to explain why this is too burdensome.

[4] As FINRA recently clarified, there is no need for non-public personal information to transfer from one firm to another without customer notice for purposes of a broker and his or her new firm meeting their due diligence and suitability obligations. FINRA Regulatory Notice 07-36, <u>Supervision of Recommendations after a Registered Representative Changes Firms</u> (August 2007).

account information consistent with this exception, in order to allow one of your representatives who leaves you to become the representative of another broker, dealer, or investment adviser to contact customers whose accounts were specifically assigned to that representative.[5]

The proposed rule text should also be narrowed in terms of the information that may be transferred. It should include only the customer's name, account type, address, phone number, and email address.[6] The use of the word "including" in proposed Rule 15(a)(8)(i) implies other information could be disclosed. It therefore should be deleted. All other types of data should be excluded, which is what Rule 15(a)(8)(ii) should say without partially listing what is not allowed to be disclosed.

B. The Rule Text for Regulatory Reporting Should Be Limited to Where an Individual Has Suffered "Substantial Harm or Inconvenience."

Frequency of Reporting. The proposing release says that broker-dealers should provide written notice to the Commission (for advisers) or designated examining authority (the DEA for broker-dealers) on Form SP-30 under circumstances more limited than breach notifications to customers. The release makes clear the intention of the Commission is to "avoid notice to the [DEA] in every case of unauthorized access, and to focus scrutiny on information security breaches that present a greater likelihood of potential harm."[7]

Despite this intention, the actual language of proposed Rule 248.30(4)(v) is broader, requiring notice to the firm's DEA not only where there is "(A) a significant risk of substantial harm or inconvenience to the individual," but also where "(B) an unauthorized person has intentionally obtained access to or used sensitive personal information." To be consistent with the expressed intent, the Commission should strike subsection (B). Otherwise firms will be required to notify the Commission or DEA where there is no likelihood of substantial harm or inconvenience and, in fact, where no notice is required to be provided to customers.

Form of Reporting. Schwab also believes that Form SP-30 is unduly burdensome, overly specific, and should not be adopted. Form SP-30 unrealistically presumes accurate and complete information is available at the early stages of a potential breach and requires detailed reporting on potential losses, impacted accounts, and other specific information not readily available at the initial stages of an investigation. Dedicating resources to complying with Form SP-30 will take resources away from the ongoing internal effort to assess, respond to, and limit impact of a breach.

---

[5] Failure to narrow the definition of which representatives appropriately may take and disclose customer contact information would allow representatives who are not directly responsible for the customer relationship to take the customer's information. That would be contrary to an implied consent rationale for the exception.

[6] The list should exclude products, which along with the knowledge of where the customer's account is held, poses potential risk of identification theft. Once contacted by representative, of course, a customer could authorize transfer of additional account information to the new firm.

[7] Proposing Release, 73 *Fed. Reg*. at 13698.

Because the proposed rule requires the submission of Form SP-30 as soon as possible after becoming aware of an incident of unauthorized access to or use of personal information, there is little likelihood that a firm would have all of the information requested by the form. Accordingly, as facts regarding the situation are determined, firms would be required to submit numerous additional forms to supplement the original filing, taking resources away from the internal effort. Further, the form calls for information that is proprietary, confidential, and may be useful to potential breach violators and identity thieves. In the very least the Commission should adopt the form under its exam authority and not its regulatory reporting authority in order to preserve confidentiality and investor protection.

Instead of Form SP-30, and to be consistent with Federal banking regulations, firms should be required to provide a simple notice to their regulator,[8] keep records of their investigations, and be prepared to produce them as requested during examinations or upon special confidential inquiry. The Commission's rule could simply include examples of the types of information that firms should consider including in the report. If the Commission (or FINRA) staff deems it appropriate to follow-up with a firm, it may seek more information as it does with other types of confidential inquiry.

C. The Defined Term "Service provider" Should Be Clarified to Eliminate Duplicative Oversight Requirements Where Two Separate Firms Have Direct Relationships with the Customer.

The proposed rule provides that an information security program must require service providers by contract to implement and maintain appropriate safeguards. The definition of service provider includes any entity that is permitted access to personal information through its provision of services to the firm. Schwab believes that this defined term should be clarified in order to eliminate the potential for confusion as to the level of oversight that must be applied in those instances where two distinct firms provide services to shared customers on a concurrent basis.

By way of example, through our Charles Schwab Institutional division, we are one of the largest providers of brokerage, custody and related services to independent advisory firms ("IAs") and their clients. IAs' clients establish accounts with Schwab and appoint their IAs through limited powers of attorney to exercise trading and certain other authorities over their Schwab accounts.

In this context, both Schwab and the independent IA have concurrent relationships with the customer. Through those separate relationships, the shared customer independently and directly gives Schwab Institutional and the IA access to the customer's personal information. Neither Schwab nor the IA gains access to the customer's information through the other. Further, each has its own independent regulatory obligations under the proposed amendments. Given that both Schwab and the independent IA would each be obliged to comply with the

[8] To avoid unnecessary duplication, for firms dually registered as broker-dealers and investment advisers, the final rule should only require reporting to FINRA as the DEA.

information security requirements envisioned by the rule, it would be unnecessarily duplicative for either to be subjected to oversight by the other under the proposed service provider construct.

Accordingly, the definition of "Service provider" should be revised (changes and additions underlined) as follows:

> Service provider means any person or entity that receives, maintains, processes, or otherwise is permitted access to personal information, and is not otherwise in a direct contractual relationship with the customer, or independently required to maintain its own information security program under this Section, through its provision of services directly to a broker, dealer, investment company, or investment adviser or transfer agent registered with the Commission.
>
> * * * * * *

Thank you for your consideration of the points we have raised in this letter. Please feel free to contact me to discuss them in more detail.

Very truly yours,

Christopher Gilkerson

cc:

Chairman Christopher Cox
Commissioner Paul Atkins
Commissioner Kathleen Casey
Erik Sirri, Director, Division of Trading and Markets
Catherine McGuire, Chief Counsel, Division of Trading and Markets
Brice Prince, Special Counsel, Division of Trading and Markets
Penelope Saltzman, Acting Assistant Director, Division of Investment Management