Wells Fargo & Company
45 Fremont Street, 27th Floor
San Francisco, CA 94105

May 12, 2008

Via Electronic Mail

Securities and Exchange Commission
c/o Nancy M. Morris
Secretary
Washington, D.C. 20549-1090

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

Subject: File Number 57-06-08
Proposed Amendment to Regulation S-P

Ladies and Gentlemen:

Wells Fargo & Company ("Wells Fargo") appreciates the opportunity to comment on the amendments proposed to Regulation S-P. Wells Fargo is one of the country's largest diversified financial services enterprises. In addition to banks, a consumer finance company, and insurance underwriters and brokers, Wells Fargo includes broker-dealers, investment advisors, funds management and stock transfer operations. Our goal is to be able to offer our customers a broad range of financial products and services to meet their needs in the most seamless way possible.

The majority of our business segments are subject to, and have considerable experience in complying with, the regulations and guidance already issued by the Federal bank regulatory agencies and the Federal Trade Commission (the "FTC") covering the same information security, breach response and records disposal concerns as the amendments now proposed by the Commission to Regulation S-P. Our corporate information security and breach response programs, which were developed to comply with the requirements of the bank regulatory agencies and the FTC, have been equally applied to those segments of our business that are regulated by the Commission. To the extent that the proposed amendments to Regulation S-P are consistent with the existing requirements of the bank regulatory agencies and the FTC, Wells Fargo firmly supports them. However, because of the high degree of integration of our banking and securities businesses and our reliance on centralized information security and breach response programs, we believe that Regulation S-P should depart from or go beyond the corresponding requirements of the banking agencies only where there are compelling reasons to do so. (Our stock transfer operations are conducted through Wells Fargo Bank, N.A. which is clearly subject regulation and oversight by the

Comptroller of the Currency so inconsistent rules would have a particularly confusing and burdensome impact in that situation.)

Our primary recommendations with respect to the proposal are:
(1) the revisions to Reg S-P should be harmonized with the Federal Banking Agencies' Guidance;
(2) the proposed expansion of the rule to cover employees, investors and security holders is beyond the scope of the Gramm-Leach-Bliley Act;
(3) securities firms should only be required to notify regulators of a breach if a significant number of customers are affected, and the method of notification should be flexible;
(4) the proposed exception permitting departing registered representatives to take their customer contact information to their new firm should be clarified;
(5) the rule should provide firms with a 12 month implementation period.
We also suggest changes to or clarifications of other sections of the proposal.

General Overview

Because many securities firms, including Wells Fargo's, are affiliated with banking organizations and have already implemented policies and procedures in accordance with standards of the banking agencies, we believe that it is critical that the Commission harmonize Regulation S-P with the guidance already provided by the Federal banking agencies to the greatest extent possible. Such consistency will enable securities firms to comply with uniform standards adopted by all of the Federal agencies more effectively and more efficiently. Imposing standards in Regulation S-P that are inconsistent with those applicable to banking organizations would prove unduly and unnecessarily burdensome for many securities firms. Accordingly, Wells Fargo supports the amendments proposed for Regulation S-P to the extent that they (a) are consistent with the guidance of the federal banking agencies or (b) are tailored to genuine differences between the banking and securities industries.

We view the proposed standard that an information security program should be appropriate to size and complexity of a firm, the nature and scope of its activities, and the sensitivity of personal information it holds, as consistent with the corresponding banking agency guidance. We believe Commission should also confirm that a diversified financial institution which includes securities firms may adopt a single information security program across all companies and business sectors within its corporate family.

In response to the Commission's inquiry, we do NOT believe Regulation S-P should try to address the issues identified in the banking agencies' guidance regarding authentication in an Internet environment or their final "red flags" regulations. It would be unnecessary and perhaps unwise for the Commission to impose such requirements at this time. Given the rapidly evolving nature of how transactions are conducted over the Internet, and the fact that banks and many other financial institutions will be implementing the banking agencies' red flags requirements over the next several months, we recommend that the Commission not take any action in this area at this time. Rather, the Commission should monitor the impact – both costs and benefits – of these requirements before taking action on these issues.

Designation of Responsible Employee

Wells Fargo believes that institutions subject to regulation by the Commission should be permitted to designate an employee or employees to coordinate their information security program either by name or

by job title. Some firms may wish to appoint a specific named employee to coordinate the information security program while others may wish to indicate a particular position, office or function. We also request that the Commission permit securities firms that are part of diversified financial services organizations to designate an employee of an affiliate or a position at an affiliate as the person responsible for coordinating the securities firm's information security program. Such flexibility will help ensure that the policies and procedures of such firms are consistent and coordinated throughout the organization as a whole.

Substantial Harm or Inconvenience

Consistent with the banking agencies' guidance, the proposal would require a firm's information security program be reasonably designed to protect against unauthorized access to or use of personal information that could result in "substantial harm or inconvenience." However the Commission's proposal goes on to define the term "substantial harm or inconvenience" as "personal injury, or more than trivial financial loss, expenditure of effort or loss of time." This would appear to represent a significant departure from the corresponding banking agency standard, since there is a wide gap between "trivial" and "substantial." Any attempt by the Commission to further define "substantial harm or inconvenience" is bound to be interpreted as intending to impose a different standard under Regulation S-P than that which applies under the banking agencies' guidance. We suggest that the existing standard of the banking agencies has provided adequate protection for consumers for the seven years it has been in effect while at the same time being workable for financial institutions. There is simply no good reason why a different threshold for securities firms should now be imposed.

We agree with the Commission that having to change an account number or password is not "substantial harm," nor is unintentional delivery of an account statement to an incorrect address if there is no reason to believe the information likely to be misused. The example of accidental access by an employee to a customer's records not constituting substantial harm or inconvenience if there is no significant risk of misuse should be expanded to include employees of affiliates and service providers of the firm, as well as "good faith acquisition" of personal information by such parties. We believe the Commission should expressly include these as well as similar examples in the final rule.

Written Determination of Likelihood of Misuse

The proposed rule requires firms to "conduct a reasonable investigation and ***determine in writing the likelihood that the information has been or will be misused***…" (Emphasis added) Where the incident is significant either because of the number of customers affected or because of other circumstances, for example criminal conduct by an employee or an apparently deliberate attempt to acquire data without authorization, we would agree that a written determination of the likelihood of harm is reasonable, especially if the firm determines that harm is not likely and that customer notification is not required. However, the vast majority of "incidents" involve only one or a small number of customers and, by their nature, entail little risk of harm. For example, a fax containing account information is mistakenly sent to the wrong number, account statements are "double stuffed" in a single envelope, or a correctly addressed statement is delivered to the wrong address and opened before the recipient realizes it was intended for someone else. In many of those cases, the firm will become aware of the incident only because the mistaken recipient of the information contacts the firm to advise it of the mistake. Having thus called

attention to him- or herself, it is inherently unlikely that the mistaken recipient will turn around and misuse the information. Conversely, the facts of some incidents make it apparent from the outset that there will not be a determination that misuse is unlikely and that notice must be given to affected customers; i.e., there is a clearly implied determination that misuse of the information is reasonably possible.

Requiring a written determination of the likelihood of misuse for each and every incident is a waste of resources that would be better spent on dealing with incidents where misuse is likely or in preventing incidents altogether. Accordingly, we suggest that written determination of the likelihood of misuse only be required (a) if more than 250 customers are affected, or (b) despite some facts which might indicate that misuse is reasonably probable, the firm determines the risk of misuse is low and that customer notification is not required.

Notice and Form SP-30

The proposed rule requires broker-dealers to provide written notice to their designated examining authority on Form SP-30 as soon as possible after becoming aware of an incident of unauthorized access to, or use of, personal information in which (1) there is a significant risk of substantial harm or inconvenience to the individual, or (2) an unauthorized person has intentionally obtained access to or used sensitive personal information. Wells Fargo believes that notice to the designated examining authority should be required only if there is a significant risk of substantial harm or inconvenience to the individual. There is no reason to require notice to regulators if an unauthorized person has obtained access to or used sensitive personal information but there is no significant risk of substantial harm or inconvenience to the individual. Such notices will serve no useful purpose and are an unnecessary administrative burden. We also believe that a notice to the designated examining authority should be required only if it appears that 250 or more individuals are or will be affected by the incident. Incidents impacting fewer than 250 are generally not a significant incident and reporting them would be an unnecessary burden on firms.

We also believe that the proposed Form SP-30 should not be adopted. The Federal banking agencies do not require financial institutions subject to their jurisdiction to use a specific form. The proposed Form SP-30 is too detailed and completing its requirements would not further the purpose intended. 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. Information submitted on the initial forms will undoubtedly change and would have to be amended as additional information is obtained. Accordingly, as facts regarding the situation are determined, firms would be required to submit numerous additional or amended forms to supplement the original filing.

A better approach would be that adopted by the Federal banking agencies, which does not specify the details or method of the report. The Commission's rule could simply include examples of the types of information that firms may wish to consider including in the report. For example, the name of the firm, dates of the incident and the filing, a brief description of the incident, a preliminary estimate of the number of persons affected and whom to contact for more information would appear to be more than sufficient information to meet the Commission's needs. If the Commission determines to require a form, a simpler form limited to this information or simply explaining the context of the incident would be more

useful to the Commission. The Commission could then request additional information if it intends to follow-up on the incident.

Finally, Wells Fargo believes that the information reported to the Commission in connection with a data breach is information that should not be available to the public. The information requested generally relates to information that is regarded by firms as confidential business information, the public disclosure of which would likely be competitively harmful. Moreover, public disclosure of this information may, in some cases, increase the risk of harm to consumers. For example, if a laptop computer with customer information is stolen, the thief is usually interested in the value of the hardware. But public disclosure that the laptop contains sensitive information pertaining to a large number of individuals could alert the thief to the potential value of the information. Rather than requiring firms to request confidential treatment of the information every time it is submitted, the Commission should indicate that filings made by firms in accordance with Rule S-P will be accorded confidential treatment under the Freedom of Information Act and the Commission's rules regarding public availability of information. If any of this information is made public, it should be done in an aggregated and summary format.

Definition of Sensitive Information

The definitions of the terms "personal information" and "sensitive personal information" as set forth in the proposed rule are unnecessarily confusing and go beyond what is authorized by the GLBA. It is proposed that "personal information" means any record containing consumer report information or nonpublic personal information as defined in Regulation S-P. Virtually all information about customers might come within this overly broad definition. See definition of "consumer report" in 15 U.S.C. § 1681a(d). The adverse consequences of a broad definition of personal information are exacerbated by the definition of "sensitive personal information," which includes "personal information." As a result, virtually all information maintained by a firm will be regarded as "sensitive personal information." Accordingly, a firm will be required to notify customers when it believes misuse of essentially any information is reasonably possible. This is a significant departure from the standards used by the other Federal agencies, which define "sensitive personal information" far more narrowly.

We suggest that the Commission define "personal information" simply as nonpublic personal information as defined in Regulation S-P. "Sensitive personal information" should then be defined in the same way the other agencies have defined it, which is substantially the same as the definition proposed in the latter portion of § 248.30(d)(10).

The Commission's proposed definition of sensitive personal information would also include a person's Social Security Number ("SSN") standing alone. This differs from the definition of the banking agencies which regards an SSN as sensitive customer information only if found in combination with the person's name, address or telephone number. A person's SSN alone should not be regarded as "sensitive personal information" unless it is obtained in combination with other information that would permit access to a customer's account. Additionally, mother's maiden name should not be regarded as sensitive personal information unless it is used as a password for access to a person's account. In the interests of consistency, the Commission should adopt the definition of "sensitive customer information" adopted by the banking agencies.

In addition, the Commission should affirmatively acknowledge that encryption is a factor that firms may take into account in determining whether an incident will result in substantial harm, inconvenience, or misuse.

Scope of Coverage

The proposal covers information about consumers, employees, investors and security holders who are natural persons. Section 501 of the GLBA (15 U.S.C. §6801(a)) provides that financial institutions have an affirmative and continuing obligation to protect the security and confidentiality of their ***customers'*** nonpublic personal information. In furtherance of this objective, §501(b) authorizes the Commission and other Federal agencies to establish appropriate standards for financial institutions to insure the security and confidentiality of customer information. There is nothing in §501 that applies the standards set forth therein to employee information. Moreover, the guidance of the banking agencies and the Federal Trade Commission does not extend to employee information. We believe that in view of the specific language of §501, and in order to be consistent with the requirements of the other Federal agencies, it would be inappropriate to expand the scope of the proposed rule to cover employee information. Because many firms maintain employee information in separate data processing systems, we believe that extending coverage to employee information will require extensive, burdensome modifications to data systems not within the scope of GLBA.

In addition, the Commission should revise the proposed rule to clarify that nonpublic personal and sensitive personal information of persons who are not customers, including investors and security holders who may not be customers, does not fall within the scope of coverage since §501 only applies to information of individuals who are customers of the financial institution.

Wells Fargo would also oppose any expansion of the proposed definition of personal information to include information identified with non-natural persons, such as corporate clients. Section 501 of GLBA authorizes the agencies to establish appropriate standards relating to safeguarding "customer" information. As used in GLBA, "customers" include only ***individuals*** who obtain financial services primarily for personal, family or household purposes. 15 U.S.C. §509(9). Regulation S-P defines the term "customer" as a consumer who has a customer relationship with the firm. §248.3(j). Accordingly, we see no legal basis to expand the scope of coverage when it is clear that Congress intended to apply §501 solely to nonpublic personal information of individuals.

Service Providers

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. Accordingly, the proposed rule appears to require firms that have services provided by affiliates to enter into contracts to implement and maintain safeguards. Wells Fargo believes that firms should not be required to enter into formal contracts with affiliates that provide services to them, especially when these firms are themselves financial institutions subject to the requirements of GLBA. Affiliates often provide services to firms on an informal basis without the need for a formal contract. Such affiliates generally are

subject to company-wide policies and standards relating to safeguarding personal information. Given the nature of these types of arrangements, there is no purpose to be served by requiring a firm to enter into a contract with an affiliate to implement and maintain safeguards.

We support the position that firms may use third-party reports, such as a review of a service provider's SAS-70 or SysTrust reports, in order to assess the adequacy of service provider information safeguards. The Commission should also indicate that other methods for evaluating service provider information safeguards are acceptable as long as they are reasonable. Similarly, we believe that if the service provider is an entity subject to GLBA, the firm should be allowed to take into account in its initial due diligence and continuing monitoring of the service provider.

Disposal of Personal Information

The proposed rule expands the current Commission rule regarding disposal of personal information by requiring firms to document in writing their proper disposal of personal information. This could be read to require a written record every time a firm disposes of any personal information. This would be a significant and unnecessary burden. The Commission should simply require that firms confirm that they have records disposal policies and procedures and reasonable processes for monitoring compliance, rather than requiring that every disposal of personal information be documented in writing.

We also believe it is inappropriate and unnecessary to impose direct personal liability on employees in the event customer information is not properly disposed of. Enforcement of such liability would inevitably be sporadic at best, perhaps arbitrary and most often triggered by publicity or the consequences of improper disposal with little or no relationship to the employee's actual culpability. Holding employees accountable for compliance with their firms' policies and procedures with employment related consequences up to an including termination is a much fairer and surer way to enforce compliance by individual employees.

Exception to GLBA for Departing Representatives

Wells Fargo appreciates the Commission's proposal for a limited exception to Regulation S-P for departing representatives that would clarify what information they may take a notice and opt-out from the prior firm to the affected customers. This proposal simply reflects the reality that sales people working on commission are likely to take at least contact information for their clients when they change firms. This has been an issue since Regulation S-P was first promulgated.

Even within Wells Fargo, different business units have divergent views and policies regarding whether departing brokers should be permitted to take customer information with them. Indeed, very different rules may be appropriate for situations in which the customer's primary loyalty is likely to be to the firm (e.g. a large wire house where the brokers are all employees) versus situations where the customer's primary loyalty is likely to run to the individual broker (e.g. a firm that does utilizes a network of independent representatives). Accordingly, we believe it needs to be clear that the proposed exception is merely permissive, and that the Commission does not require or approve of any particular practice or policy. For this reason, we recommend that the text of the rule provide that representatives are subject to

their firm's policies, and that firms may, by policy, prohibit representatives from taking any customer information, including the limited information covered by the exception. The Commission should also clarify that information that a departing representative is permitted to take is subject to the safekeeping requirements of GLBA when it is in the custody of the representative's new firm.

We also recommend that the language of the rule be slightly modified. The exception provides that no notice or opt-out is required if the information a departing representative takes is limited to a customer's name, contact information and "a general description of the type of account and products held by the customer." We believe this last is too vague. Unlike other data elements covered by the exception – name, address, telephone number and e-mail address – this language does not provide clear guidance to firms regarding precisely what types of account and product information the departing representative may take. A better approach might be to use the term "account type" as a more accurate description of the types of information that come within the exception.

Effective Date

If the Commission accepts our recommendations to conform its information security and breach response requirements to those of the banking agencies, Wells Fargo believes that its securities businesses could come into full compliance very quickly and, in fact, might already be incompliance with the exception of notice to the Commission of significant information compromises. However, based on our experience with the banking agencies' rules, we know that implementation by stand-alone firms not previously subject to such requirements can be a significant undertaking. We would therefore suggest that the Commission give firms at least 12 months to come into compliance once a final rule is published. However, we believe that the effective date of the final rule should be immediate so that firms can take advantage of the "departing representative" exception without undue delay.

Wells Fargo appreciates the opportunity to comment on the Commission's proposed amendments to Regulation S-P. If you wish to discuss these comments, please feel free to contact the undersigned.

Sincerely,

Peter L. McCorkell
Senior Company Counsel