



**Executive Director**

Joan Hinchman

**Directors**

James E. Ballowe, Jr.  
*E\*TRADE Brokerage Services, Inc.*

David Canter  
*Charles Schwab & Co., Inc.*

Richard T. Chase  
*RBC Capital Markets Corporation*

Kerry E. Cunningham  
*ING Advisors Network*

Aaron D. De Angelis  
*Spring Mountain Capital, LP*

Patricia M. Harrison  
*Simmons & Company International*

Alan J. Herzog  
*A.G. Edwards & Sons, Inc.*

Ben A. Indek  
*Morgan, Lewis & Bockius LLP*

J. Christopher Jackson  
*Deutsche Asset Management*

Michelle L. Jacko  
*Core Compliance & Legal Services, Inc.*

Deborah A. Lamb  
*STI Classic Funds and Variable Trust*

David H. Lui  
*First American Funds*

Angela M. Mitchell  
*Capital Research and Management Company*

Diane P. Novak  
*Washington Mutual*

David C. Prince  
*Stephens Investment Management Group, LLC*

Theodore J. Sawicki  
*Alston & Bird LLP*

Holly H. Smith  
*Sutherland Asbill & Brennan LLP*

M. Catherine Tuckwell  
*Scotia Cassels Investment Counsel Limited*

Kenneth L. Wagner  
*William Blair & Company, LLC*

Judy B. Werner  
*Gardner Lewis Asset Management, L.P.*

Michael K. Wolensky  
*Schiff Hardin LLP*

May 19, 2008

The Honorable Christopher Cox, Chairman  
U.S. Securities and Exchange Commission  
Attn: Nancy M. Morris, Secretary  
100 F Street, NE  
Washington, DC 20549  
Electronic Address: rule-comments@sec.gov

**Re: File No. S7-06-08 - Proposed Amendments to Regulation S-P**

Dear Secretary Morris:

The National Society of Compliance Professionals (“NSCP”) appreciates the opportunity to comment on the proposed amendments to Regulation S-P (“Proposed Amendments”) by the Securities and Exchange Commission (“Commission”).

The Proposed Amendments are of considerable interest to the NSCP and its members. NSCP is the largest organization of securities industry professionals devoted exclusively to compliance issues, effective supervision, and oversight. The principal purpose of NSCP is to enhance compliance in the securities industry, including firms’ compliance efforts and programs, and to further the education and professionalism of the individuals implementing those efforts. An important mission of the NSCP is to instill in its members the importance of developing and implementing sound compliance programs across-the-board.

Since its founding in 1987, NSCP has grown to over 1,800 members, and the constituency from which its membership is drawn is unique. NSCP’s membership is drawn principally from traditional broker-dealers, investment advisers, bank and insurance affiliated firms, as well as the law firms, accounting firms, and consultants that serve them. The vast majority of NSCP members are compliance and legal personnel, and the asset management members of NSCP span a wide spectrum of firms, including employees from the largest brokerage and investment management firms to those operations with only a handful of employees. The diversity of our membership allows the NSCP to represent a large variety of perspectives in the financial services industry.

## **General Comments on Proposed Regulation S-P**

### Preliminary Observations

NSCP submitted its first comment letter on April 30, 2008, requesting that the Commission extend the comment period for an additional 60-90 days to afford NSCP, its members, other registrants and interested persons sufficient time to study the proposed rule amendments and provide more fully considered comments to the Commission.

NSCP supports the Commission's efforts to update existing protections currently in place under Regulation S-P and to provide to entities regulated by the Commission more specific guidance for safeguarding information and responding to information security breaches. Nevertheless, we observe that breaches in information security systems come from various sophisticated sources and no matter how robust the program, the financial industry may not be able to definitively stop improper access to, and misuse of, consumer information. The proposal's objective of better protecting customer information is virtuous and beyond debate. However, within its proposal, the Commission did not provide data to quantify how any shortcomings in this industry's current systems have or will contribute to consumer harm.

Many registrants have already adopted excellent programs and procedures for information security. In addition, Commission and FINRA rules have for some years now mandated that broker-dealers, investment companies, and investment advisers adopt written supervisory policies and procedures as well as annual review and/or testing of their adequacy.<sup>1</sup> Therefore, NSCP encourages the Commission to assess more fully the cost/benefit of any incremental gains likely to be achieved from a distinct comprehensive information security program contemplated by the proposed amendments when compared to the very significant expenditures that would be necessary to design, implement, maintain and enhance such a program by each entity regulated by the Commission.

NSCP also believes that there has not been sufficient investigation into the cost/benefit of a "comprehensive program" versus one that sets minimum standards for compliance (with due consideration given to size and resource considerations of various regulated entities). While a "comprehensive" approach is ideological and subjective, contrastingly, a minimum standards regulation provides guidance and objectivity for institutions to define tools that could be best used to achieve an appropriate array of safeguards consistent with the needs and resources of smaller organizations.

NSCP continues to believe that additional time is needed to fully appreciate the implications

<sup>1</sup> Sec. Act Rel. IA-2204 and IC-26299 (December 17, 2003) requires that investment advisers and funds adopt and implement written policies and procedures reasonably designed to prevent violations of the federal securities laws, review those policies and procedures annually for their adequacy and the effectiveness of their implementation, and designate a chief compliance officer to be responsible for administering the policies and procedures. Similarly, NASD Rule IM-3013 and NYSE Rule 342.30(e) require that broker-dealers have an annual certification that: the firm has processes in place to establish, maintain, and review policies and procedures reasonably designed to achieve compliance with applicable SRO rules and federal securities laws and regulations and to modify such policies and procedures as business, regulatory, and legislative changes and events dictate.

and scope of the proposed amendments on the affected entities. Since there has been no clear indication at this time that the comment period will be extended, NSCP herewith submits additional comments to support certain aspects of the proposed amendments as well as to highlight other areas requiring clarification or additional detailed study. For ease of reference, our specific comments will track the five main areas of the proposed amendments as set forth in the Commission's notice: (1) Information Security Programs; (2) Disposal of Personal Information; (3) Recordkeeping; (4) Form SP-30; and (5) the New Exception for Information Sharing When Representatives Change Firms. We once again respectfully urge the Commission to extend the comment period so that a fuller record can be developed to address and resolve the issues presented thus far.

### **(1) General Comments on Comprehensive Information Security Programs**

Under the Proposed Amendments,<sup>2</sup> 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 consumers' non-public personal information.<sup>3</sup> The Commission would require the program to be "appropriate to the institution's size and complexity, nature and scope of its activities, and the sensitivity of any personal information at issue."<sup>4</sup>

The term "comprehensive" implies that these programs will be all-inclusive and wide-ranging in scope. While we commend the approach taken by the Commission allowing firms to customize their information security program to each firm's unique characteristics, the proposal fails to provide an objective standard for measuring whether any program put in place is sufficiently "comprehensive" to satisfy the proposed rule.

NSCP is also concerned that the burdens of such an initiative will likely fall most heavily on small to mid-sized firms which may lack the technical in-house resources to identify and address their data security risks; and also may lack sufficient resources to independently produce and support these new requirements. Given the resource and monetary costs that will have to be borne by smaller firms attempting to develop a "comprehensive" Information Security Program, NSCP urges the Commission to consider whether, from a cost benefit perspective, a minimum-standards-based regulation would adequately address legislative and regulatory requirements in this area.

#### **Program Design**

As proposed, the Information Security Program must be "reasonably designed" to: (i) ensure the security and confidentiality of personal information; (ii) protect against any anticipated threats or hazards to the security or integrity of personal information; and (iii) protect against unauthorized

2 SEC, *Part 248 – Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information*, Release Nos. 34-57427, IC-28178 and IA-2712, 73 FED. REG. 13692 (March 13, 2008) [hereinafter *Release*].

3 Proposed Rule 30(a)(1).

4 *Id.*

access to or use of personal information that could result in substantial harm or inconvenience to any consumer, employee, investor or security holder who is a *natural person*.<sup>5</sup>

The Proposed Amendments define “substantial harm or inconvenience” as a harm that can cause personal injury, or more than trivial financial loss, expenditure of effort or loss of time.<sup>6</sup> Included in this category are theft (including identity theft), fraud, intimidation, damaged reputation and impaired eligibility for credit.<sup>7</sup> NSCP concurs with the Commission’s decision to include other harms, and not merely identity theft and fraud in this definition. However, we also believe that a more objective definition, one with a precise standard for determining when harm is considered “substantial,” will better guide the industry and further achieve the intended purpose to protect against all harms that may result from failure to safeguard sensitive information about an individual.

#### Elements of a Program in Compliance with the Proposed Amendments

The Proposed Amendments mandate the regular testing and monitoring of the Information Security Program, including written documentation demonstrating the effectiveness of the safeguards’ key controls systems and procedures and the institution’s ability to detect, prevent and respond to security breaches.<sup>8</sup> NSCP recommends that the Commission consider clarifying this mandate by including the specific elements that should be present.

Furthermore, in conformance with investment adviser, investment company and broker-dealer general requirements to test compliance programs no less than annually, we recommend that the Commission specifically address whether this annual review will satisfy the proposed amendment’s requirements.

An additional facet to the Proposal is the written designation of one or more individuals who will be responsible for reviewing, maintaining and enforcing the information security program.<sup>9</sup> The new “Information Security Officer” will be required to oversee the regular testing and monitoring of the program, continually adjust and modify the policies and procedures, train staff members to implement the program and otherwise supervise the proper maintenance of the program, which may require significant expertise and training.<sup>10</sup> If the proposal is adopted as proposed without further guidance, most small firms likely will delegate this responsibility to their Chief Compliance Officer, which could create yet another “hat” to an already stretched-too-thin employee. NSCP strongly encourages the Commission to clarify its expectations for the role of the Information Security Officer.

#### Scope of Information Covered

- 
- 5 Proposed Rule 30(a)(2).
  - 6 Proposed Rule 30(d)(12).
  - 7 *Id.*
  - 8 Proposed Rule 30(a)(3)(iv).
  - 9 Proposed Rule 30(a)(3)(i).
  - 10 *See* proposed Rule 30(a)(3)(i – vii).

The scope of the current Safeguards Rule is to protect “customer records and information,” whereas the Disposal Rule requires firms to properly dispose of “consumer report information.”<sup>11</sup> While these terms may appear to overlap in many respects, the Commission’s proposal seeks to apply both rules to protect “personal information.”<sup>12</sup> In addition to harmonizing the information covered by the two provisions, the Proposed Amendments broaden the scope of the rules by defining “personal information” as any record containing either “non-public personal information” or “consumer report information.”<sup>13</sup> NSCP supports such a move toward uniformity of covered information. However, we believe that additional guidance is needed as to what safeguards firms would be required to have in place to protect institutional client information, which appears outside the scope of the proposed definition.

The Proposed Amendments further expand the definition of “personal information” to include firm employee information appearing in paper, electronic or other format.<sup>14</sup> While the NSCP concurs with this as an internal ethical standard, we do not support this vast extension in the context of Safeguard and Disposal rules. By expanding the scope of coverage to include information identified with employees, the Commission would be exceeding its authority granted to it under Title V of the Gramm-Leach-Bliley Act (the “GLB Act”).<sup>15</sup> The GLB Act states that the Commission may establish standards to protect customer information, but does not refer to employee information. Accordingly, the NSCP recommends that the Commission not incorporate employee information into the scope of Regulation S-P but rather encourage covered institutions to adopt internal policies to protect employee information. This will enable institutions to design customized security procedures to encompass payroll systems, benefit plans, human resource files and other employment records without having unnecessary implementation costs.

#### Responding to Incidents of Unauthorized Access to Personal Information

As part of the Information Security Program, the Proposed Amendments require firms to have detailed written procedures for responding to security breaches or any unauthorized access or use of a firm’s personal information about customers, employees, investors, and security holders.<sup>16</sup> Moreover, the policy must contain step-by-step procedures for assessing, investigating and containing the breaches and detail notice procedures to affected individuals if misuse of sensitive personal information has occurred or is reasonably possible.<sup>17</sup>

NSCP agrees that individuals should be notified as early as possible if they are in danger of identity theft or other harm resulting from a security breach. Conversely, we also recognize that not every instance of unauthorized access should necessitate notification, because individuals may receive excessive notices where no harm or misuse has occurred. As proposed, the rule

---

11 See 17 C.F.R. 248.30(a); 17 C.F.R. 248.30(b).

12 Release at 13699-13700.

13 Proposed Rule 30(d)(8).

14 *Id.*

15 See 15 U.S.C. 6801-6827.

16 See proposed Rule 30(a)(1).

17 Proposed Rule 30(a)(4).

would require notice if misuse has occurred or is “reasonably possible,”<sup>18</sup> yet that term is neither defined in the proposal nor is there a standard for determining when misuse should be considered reasonably possible. Due to the ambiguous and subjective nature of this concept, NSCP recommends further guidance regarding the notification triggers for the reasonably possible standard to avoid firms unduly alarming clients by notifying them of non-material events. We recommend that the Commission take into consideration the concept of reasonable security and its application in this context. We also believe the adopting release should clarify that a breach does not necessarily equate to unreasonable security efforts by that institution. Rather, the firm’s internal security controls should be reasonably designed to prevent, detect and correct security breaches.

## **(2) General Comments on Disposal of Personal Information**

The Proposed Amendments broaden the Disposal Rule to require firms to adopt written policies and procedures relating to the disposal of personal information and to take reasonable measures to ensure proper disposal techniques are used to protect against unauthorized access to or use of information in connection with its disposal.<sup>19</sup> Because of the associated costs relating to disposal measures, the NSCP urges the Commission to further evaluate and assess the impact on the industry due to the broad expansion of the information covered by the disposal rule and the hidden costs that are associated with the proposal in its current form.

### Information Covered by the Disposal Rule

NSCP believes that the scope of the Proposed Amendments to the Disposal Rule is unnecessarily expanded to include “information identified with any employee, investor or security-holder.”<sup>20</sup> We believe this description of expanded coverage is too vague and ambiguous. For example, various subsets of information may not likely be “identified” with a particular person, but when combined, may constitute identifiable information. As proposed, it is unclear as to whether the Commission expects firms to protect those subsets of information which relate to an individual or whether the Commission will offer examples of information considered to be “identified” with a consumer.

In its current form, Regulation S-P protects customers and consumers from harm resulting from unauthorized access to their personal financial information.<sup>21</sup> These protections include safeguards to prevent identity theft and other harms which may occur if an institution improperly disposes of confidential client information. Accordingly, the NSCP believes that the application of the disposal rule should remain in its current form as the safeguards already serve the public’s interest as being reasonably designed to protect against improper disposal.

### Persons Covered by the Disposal Rule

- 
- 18 Proposed Rule 30(a)(4)(iv).  
19 See proposed Rule 30(b)(1-2).  
20 Proposed Rule 30(d)(8).  
21 See 17 C.F.R. 248.3(g)(1); 17 C.F.R. 248.3(j).

Currently, the Disposal Rule applies to institutions such as broker-dealers, registered investment advisers, investment companies and registered transfer agents.<sup>22</sup> If the Proposed Amendments are adopted, the rule would also apply to natural persons who are associated persons of a broker-dealer, supervised persons of a registered investment adviser, and associated persons of a registered transfer agent.<sup>23</sup> The stated purpose of this extension is to make individuals who are associated with a covered institution directly responsible for properly disposing of personal information in accordance with the institution's written policies and procedures.<sup>24</sup> In order to achieve such a result without adversely impacting the industry, significant consideration and evaluation must be given to the matter in order to adequately understand the consequences.

This proposal poses several significant practical concerns that should be considered before extending the disposal rule to individuals associated with covered institutions. First, to what extent will institutions be required to ensure that information stored on these individuals' equipment (including home computers, laptops, blackberries, etc.) is disposed of properly and in accordance with the written disposal procedures? Because information is often stored and maintained on more than one computer including personal computers, it would be impossible to effectively and efficiently monitor the proper disposal of personal information in associated persons' homes.

Second, the proposal lacks any specificity as to what standard of liability attaches to these individuals for the failure to take reasonable measures to protect against unauthorized access to information in connection with its disposal. Are they strictly liable for any unauthorized access that results from a disposal not in accordance with the written procedures, or will they be held to a recklessness or negligence standard? More specificity and clarity is needed to ensure the intended purpose of this provision is carried out.

Another significant concern regarding the changes to the disposal rule relates to the inconsistency of the new provision and absurd results that could be read into the rule, if adopted without change. The Proposed Amendments would apply the standard set forth in paragraph (b)(1) to institutions and individuals alike, requiring both the firm and its associated persons to take reasonable measures to protect against unauthorized access to information.<sup>25</sup> Significantly, the requirement set forth in paragraph (b)(2) that firms adopt written procedures and document the proper disposal of personal information only applies to institutions.<sup>26</sup> Therefore, we believe more clarity is needed because this inconsistency could be potentially burdensome by requiring the institution to document in writing each time one of the individuals referred to in paragraph (b)(1) shreds a document or gets a new PDA.

Clearly, such an extreme result is not what is intended by the Proposed Amendments, but as written, the lack of clarity and specificity causes serious concerns on a practical level. Thus, NSCP suggests that more time is imperative in order to enhance protections of personal information in the most realistic and reasonable manner.

22 17 C.F.R. 248.30(b)(2)(i).

23 Proposed Rule 30(b)(1).

24 *Release* at 13701.

25 Proposed Rule 30(b)(1).

26 Proposed Rule 30(b)(2).

### **(3) General Guidance on Recordkeeping**

Under the Proposed Amendments, institutions will be required to maintain records and policies in accordance with the new writing requirements, including the written policies and procedures of the Information Security Program, records of responses to security breaches, and documentation of the proper disposal of consumer information.<sup>27</sup> The records will be required to be held by the various types of institutions for identical periods applicable to other records imposed upon the various institutions by regulations promulgated under the Securities Exchange Act of 1934, the Investment Company Act, and Investment Advisers Act.<sup>28</sup>

#### Duration of Record Retention

NSCP observes that the proposed time periods for record retention are consistent with current record retention requirements applicable to broker/dealers, transfer agents, investment companies and investment advisers. While adding new categories of records to be created and maintained, the proposed retention periods appear to be consistent with retention requirements for similar types of records.

In addition to the proposed amendments, the Commission has also asked whether these records should be held for the same time periods by all institutions covered by the rule. NSCP believes they should not. Such a change would further complicate the varying retention requirements now in place which are mandated by each of the four recordkeeping rules applying to affected institutions.<sup>29</sup> A change of this nature would most likely add a new major category of recordkeeping requirements for each regulated institution with yet another time period requirement. NSCP believes such a change would lead to higher costs of implementation and maintenance. Further, a change could lead to more confusion for compliance and operations personnel to sort out which record is covered by an applicable portion of new and existing rules.

Finally, NSCP requests clarification of the applicable start date of the record retention period. In proposed Rule 30(c)(2) this is said to be “when the record was made or from when the written policy or procedure was last modified.”<sup>30</sup> Perhaps some examples could be provided to help institutions determine when the recordkeeping time period begins for any new policy. NSCP is unsure if the term “record” is meant to include written policies or procedures within its scope.

#### Types of Records and Documents to be Maintained and Preserved

The adequate maintenance and preservation of records relating to personal information protection appears to be appropriate. NSCP notes that the proposed changes would add at least fifteen new categories of records to be created and preserved. The time and expense to develop an understanding of the new recordkeeping requirements and integrate those requirements into a registrant’s operational process will be extensive. NSCP believes the Commission and Self

27 Proposed Rule 30(c).

28 Proposed Rule 30(c)(2).

29 17CFR 240.171-4(b); 240.17Ad-7(b); 270.31a-2(a)(4)-(6); and 275.204-2(e)(1)

30 Proposed Rule 30(c)(2).

Regulatory Organizations should develop a focused education program to assist registrants understand their responsibilities perhaps during the CCO Outreach Programs or in a webinar format. NSCP anticipates the volume of records required to comply with the new rules will be extensive.

The establishment of a comprehensive information security program by each registrant will entail a significant amount of time and expense to design, implement, maintain and test. Managing the recordkeeping aspects alone would seem to indicate substantially more time than that suggested in the Proposing Release. Given the limited time allowed by the Commission for comments on these far ranging proposals, the ability to survey NSCP members to better identify time and cost estimates was severely limited.

Certain documentation requirements are confusing and unclear. For example, registrants would be required to adopt written policies and procedures addressing proper disposal of personal information.<sup>31</sup> Both registrants and associated or supervised persons of such registrants must properly dispose of customers' personal information.<sup>32</sup> Proper disposal is to be documented in writing.<sup>33</sup> Clarification should be provided as to the role associated or supervised persons are to perform in connection with the disposal of such information.

The language in proposed Rule 30(b)(3)(i)(Relation to Other Laws) is unclear. It states that nothing in paragraph 30(b) requires that a record pertaining to an individual be maintained or destroyed "that is not imposed under other law."<sup>34</sup> NSCP is unclear as to what this section means.

Some recordkeeping requirements will add a burdensome additional layer of records to be regularly created. Consequently, under the current proposal, firms must not only maintain written policies, procedures, and records addressing the proper disposal of information,<sup>35</sup> but each time information is disposed of, firms also would have to document how the registrant complied with the Rule.<sup>36</sup>

#### **(4) General Guidance on Form SP-30**

Under the Proposed Amendments, firms that become aware of any incident of unauthorized access to or use of personal information in which there is a significant risk that an individual identified with the information might suffer substantial harm or inconvenience, or an unauthorized person has intentionally obtained access to or used sensitive personal information will be required to utilize Form SP-30 to provide written regulatory notice to the Commission or other regulatory body "as soon as possible."<sup>37</sup> This form will summarize the nature of the

31 See proposed Rule 30(b)(2)(i).

32 See proposed Rule 30(b)(1).

33 See proposed Rule 30(b)(2)(ii).

34 Proposed Rule 30(b)(3)(i).

35 See proposed Rule 30(b)(2)(i).

36 See proposed Rule 30(b)(2)(ii).

37 Proposed Rule 30(a)(v).

unauthorized access or misuse of personal information that has occurred and will describe what the firm intends to do to respond to the incident.<sup>38</sup> The regulatory notice would include a description of the incident, when it occurred, and what part of the firm's business was affected. If a third party service provider was involved, a description of the services provided, and whether the provider is an affiliate of the firm must also be disclosed.

#### Form and Content of Proposed Form SP-30

The proposed form entitled, "Security Incident Reporting Form," requires institutions filing the form to, among other things, summarize the incident, describe the steps taken to prevent improper use of personal information, and provide an estimate of customer losses.<sup>39</sup> The expectation is that institutions will use this form to report breaches to the SEC or other appropriate regulatory body. Provided the comments and concerns below are addressed, NSCP believes the use of the proposed form will promote efficiency and consistency.

As proposed, Form SP-30 requires the respondent to provide a significant amount of information, including information that typically may take time to develop and analyze. Limiting the required information to basics, such as a concise description of the "security incident," as well as "check-the-box" type information, would facilitate a firm's ability to file Form SP-30 in a reasonable amount of time and still provide the Commission with notice regarding the "security incident." The level of detail required in the proposed form, however, appears pre-mature and perhaps inconsistent with the Commission's desire to receive the Form "as soon as possible" after an incident.

NSCP recommends a more limited summary description of the incident in order to expedite filing of the form. Relevant details relating to the incident, including steps taken or planned to be taken by the firm could be made available through the firm's Chief Compliance Officer should the Commission decide that further detail or investigation of the "security incident" is warranted. Additionally, the use of an on-line reporting mechanism would further help to build uniformity and efficiency into this process.

When multiple parties are involved, NSCP suggests that clarification is needed regarding which entity has the reporting obligation. Under the proposed rules, multiple reporting obligations could be triggered with respect to the same "security incident" when, for example, a breach involves introducing and clearing broker relationships, or third party service provider or vendor relationships.

#### Prompt Notice to the Commission

The proposal states that an institution must provide notice to the Commission "*as soon as possible*" after the institution becomes aware of "*any incident*" of unauthorized access to or use of personal information in which there is a significant risk that an individual identified with the information might suffer "substantial harm or inconvenience."<sup>40</sup>

38 See proposed Appendix A(3) to Part 248.

39 See proposed Form SP-30.

40 Proposed Rule 30(a)(4).

The Commission should make clear what purpose(s) Form SP-30 reporting is meant to serve and how much of the information regarding the incident must come to light before the Commission is required to be notified. Similarly, the proposal should make clear what to do in the event that additional information is discovered after the Form has been filed.

Each “security incident” is unique and any “security incident” that would necessitate reporting will require the firm to investigate the incident, determine which parties are involved (*e.g.*, introducing/clearing firm, third party service provider and third party vendors), analyze the potential harm, and determine what action must be taken. As currently required, each of the foregoing issues needs to be addressed before the firm is in the position to file Form SP-30. Accordingly, the Commission should give further consideration as to where the appropriate balance should be struck. The Commission should clarify whether there is more value in early regulatory notice of the occurrence of a security incident, or not requiring Form SP-30 to be filed until the firm has had sufficient time to collect the relevant information, analyze the situation and address it accordingly.

Other questions arise with respect to the act of filing this type of information. How can firms ensure that their customers’ information is transmitted securely and is properly safeguarded once this information is submitted to their regulator? NSCP would like to see a safe harbor or some other provision that addresses the confidential treatment of Form SP-30 and personal information that is provided to the regulator with respect to a Form SP-30 filing.

NSCP believes that the proposed standard of reporting “any incident” to the Commission would impose an undue burden, especially with respect to such requirements on small broker-dealers and investments advisers. NSCP suggests that thresholds be incorporated into the reporting requirements.

#### Proposed Definition of “Substantial Harm or Inconvenience”

The proposal defines these terms subjectively. For example, “Substantial Harm” is either a harm that can cause personal injury, or harm more than a trivial financial loss, expenditure of effort or loss of time.<sup>41</sup> Examples include, among other things, theft, fraud, intimidation, damaged reputation, and impaired eligibility for credit.<sup>42</sup>

NSCP concurs with the Commission’s decision to consider and address harms, other than identity theft, in regards to notifying the Commission on Form SP-30. However, as noted above,<sup>43</sup> a more objective definition, one with a precise standard for determining when harm is considered “substantial,” will better guide the industry and further achieve the intended purpose in order to provide for protection of information beyond identity theft. This is particularly relevant to the filing of Form SP-30, as there is a need for objective standards and clarification regarding what type of unauthorized access would trigger regulatory notice on Form SP-30.

---

41 Proposed Rule 30(d)(12)(i).

42 *Id.*

43 *See supra*, Part 1, page 3.

### Proposed Definition of “Sensitive Personal Information”

The proposal defines “sensitive personal information” as any combination of components of personal information that would allow an unauthorized person to use, log into, or access an individual’s account, or establish a new account using the individual’s identifying information.<sup>44</sup>

NSCP agrees that a distinction should be made between “sensitive personal information” and other information to recognize the greater potential for identity theft in the event of unauthorized access to an individual’s sensitive personal information. However, as stated in the proposal, the regulatory notice requirement is intended to focus on breaches that present a greater potential for harm,<sup>45</sup> yet the “substantial harm or inconvenience” standard is not invoked where “sensitive personal information” is involved.<sup>46</sup> In accordance with the Commission’s objectives, regulatory notice should be imposed only where harm is likely to result, and as noted above, the degree of access to such information which necessitates filing Form SP-30 should include a threshold similar to the “substantial harm or inconvenience” standard.

### Notice to Affected Individuals

If an institution has determined that an unauthorized person obtained access to or used sensitive personal information, and that misuse of the information has occurred or is “*reasonably possible*,” notification to affected individuals must be provided.<sup>47</sup>

A balance must be struck between warning individuals so that they are able to take appropriate action to protect themselves and minimizing notifications of minor, harmless incidents. In this context, a standard of “reasonably possible” is unclear and can be extremely subjective as a standard for determining when the personal notification requirement is triggered. The Commission should give additional consideration to a more objective standard and establishing distinct thresholds so as not to impose unnecessary burdens and costs on regulated entities and not “over warn” individuals of non-material issues. When multiple parties are involved, clarification is also needed as to who is responsible for detecting the unauthorized access and who is responsible for providing such notice so that there is no duplication of effort.<sup>48</sup>

NSCP recommends that the Commission consider how its notice requirements to affected individuals will apply when conflicting or inconsistent state regulations exist. Absent this harmonization, there is a substantial possibility that conflicting notice requirements may result in duplication of time and expense.

In addition to, or as an alternative to individual notice to affected individuals, the Commission should give consideration to causing information on security breaches that has been collected to be transmitted promptly to other government agencies and perhaps to credit bureaus so that the

44 Proposed Rule 30(d)(10).

45 *Release* at 13697-98.

46 *See* proposed Rule 30(a)(4)(v)(B).

47 Proposed Rule 30(a)(5).

48 *See* discussion *supra* Part 1.

wrongfully obtained information can be flagged and/or new accounts frozen, so that the value of getting and using such information can be lessened or eliminated.

## **(5) General Comments on Exceptions from Notice and Opt-Out Requirements**

The Proposed Amendments would add a new exception from the notice and opt out requirements to permit limited disclosures of investor information when a registered representative of a broker-dealer or a supervised person of a registered investment adviser moves from one brokerage or advisory firm to another.<sup>49</sup> In creating this exception, the Commission takes cognizance of some of the issues under customer privacy laws presented by common industry practices when representatives move from one firm to another. The proposed exception attempts to set forth conditions and limitations on the extent of disclosure and thereby, in the Commission's view, provides an orderly framework for transferring such information.<sup>50</sup>

Before the exception approach is adopted, NSCP believes that more thought and consideration must be given to the subject. As the Commission's Notice acknowledges, many customers consider their relationship with an investment firm to be with their registered representative or investment adviser representative. Although the Commission is obliged to regulate those within its jurisdiction who are the holders of non-public customer information, efforts should be made to find ways to do so that are consistent with most customers' choice or likely expectations.

### Limitations on the Information Disclosed

NSCP generally supports the Commission's view that in this context a customer's name, address, telephone number and e-mail information (essentially "customer contact information") present a relatively low risk of misuse.<sup>51</sup> NSCP also supports the Commission's recognition that some customer information is more sensitive and potentially more harmful. Absent opt out disclosure or customer consent, it may be reasonable to prohibit departing representatives from taking more sensitive information such as Social Security or account numbers, or specific securities positions and to limit departing representatives to having customer contact and general account information for only those customers with whom they have had personal and ongoing relationship at their existing firm. Issues arise, however, with the Commission's stance regarding the circumstances under which the exception would be available.

### Who May Rely on the Exception

As proposed, the exception would only be available if the existing firm allowed it and the departing representative met certain pre-conditions. The exception provides that a departing representative must supply to the firm, not later than the time of separation from employment, a written record of the information that will be disclosed under the exception.<sup>52</sup> The Commission notes that sharing information in these situations is important for efficiency and investor

49 Proposed Rule 15(a)(8)

50 See *Release* at 13702-03.

51 See *id.*

52 Proposed Rule 15(a)(8)(iii).

freedom, as well as for eliminating the improper and secret sharing of such information.<sup>53</sup> Yet, by placing all control in the hands of the old firm, the exception may become illusory and thus fail to facilitate the stated objectives. Thus at the very threshold, the use of an exception to accomplish the goal is problematic. Not only does the proposed exception favor the existing firm by giving it control over whether the exception will be offered;<sup>54</sup> at the same time, it creates administrative burdens and uncertainty for everyone should the type of information allowable or the conditions of the exception are overstepped.<sup>55</sup>

The current proposal views the use of customer information from the perspective of the firm that holds it. The Commission has tailored its proposed exception and recordkeeping rules from that vantage point. As a result, this analysis, in our view, creates additional issues and leads to bad results. The proposed exception would, by regulating the use of a customer's information, give the current firm the ability to control the customer's choice. The inappropriateness of this result is even clearer with an investment advisory customer because a fiduciary relationship exists.

In its desire to protect and control the improper use of customer information, the Commission apparently loses sight of the fact that it is dealing with the customer's information. The "protocol" cited in the Commission's public release may be appropriate when competing broker-dealers are negotiating their respective rights, but it is certainly not a fair model when considering where to draw the line from the customer's perspective.<sup>56</sup>

Once the customer has several simultaneous existing relationships, managing the choice process in the best interest of the customer becomes more complex. Although the Commission is obliged to promulgate rules to protect customer information, it must also represent the public interest and facilitate fair and efficient processes amongst its regulated persons and entities. The proposed exemption is hardly neutral -- it clearly favors existing firms who would prohibit their departing representatives from soliciting former customers to the new firm and, more significantly, does not fully serve the customer interests in choosing whether or not to transfer their accounts. The Commission's position should be neutral and not take sides. Its rules should assume that it is equally likely that a customer wants to go with the departing representative to the new firm as it would be for them to stay with their current firm.

Another difficulty with the Commission's proposed exemptive solution is its "one size fits all" approach. As noted above, the Commission's notice makes no distinction between broker-

53 *Release* at 13702.

54 The language is written so as to apply only if the institution "allows" a departing representative to utilize the exception. *See* proposed Rule 15(a)(8).

55 Although the departing representative is likely to be a beneficiary of the exception, as proposed, the representative would not be permitted to use the information unless the firm "allows" it and the conditions of the exception are met. Additionally, if taken without such permission, the representative could presumably be charged with violating the rule. Likewise, any information sharing outside the exception would constitute a breach of the firm's Privacy Notice disclosures and its Information Security Program. The proposed amendments are silent as to what will happen if the type of material or the conditions of the exception are breached.

56 *See* SHANE B. HANSEN, *The Price of Protecting Privacy—Proposed Regulation S-P Amendments*, NSCP CURRENTS, March/April 2008, at 5.

dealer and investment advisory situations. This approach also does not take into account that the entities providing services to the customer may do so using different business models. There is also no analysis with respect to representatives that may have more than one type of relationship with customers or whether all of the entities which they represent are subject to the Commission's rules. Likewise, the types of accounts held, services provided and consideration of distinctions such as varying levels of customer sophistication can also factor into crafting the best solution.

The Commission clearly must recognize that there may be times when the interests of the existing firm, which holds the customer's information, and the desires of customer may come into conflict. The problem is, from the customer's point of view, many customers will not appreciate any or all of the implications of what it means to have the representative with whom they've been dealing leave their current firm and go to a new one.

More time is needed to study alternative approaches that will provide adequate safeguards for customer information which will at the same time limit administrative burdens, promote efficiencies in the orderly administration and transfer of accounts, and not work to the customer's disadvantage. Recognition should be given to the fact that the customer information held by the current firm was given to the firm and its representatives voluntarily by the customer at the outset of the relationship for purposes of assisting the customer in the conduct of the customer's business through the firm. Account records and other documents were created and maintained by the firm in the ordinary course of business as that relationship continued. Regardless of what happens when a representative serving the customer and the current firm take separate paths, the customer has a continuing interest that their business will continue to be done properly, efficiently, and in their best interest. Upon separation from the existing firm, possession of the customer's information by the departing representative is not necessarily harmful and may indeed be beneficial to the customer as well as necessary to the representative for other valid purposes.<sup>57</sup> The Commission should consider whether and under what circumstances it would be preferable for it to mandate appropriate acceptable solutions for the protection of customer information in these circumstances rather than leave the customer's fate to the determination made by the regulated entity with which he/she is currently doing business.

As alternatives to the current proposed exemption, the Commission should assess under what circumstances a departing representative's possession and use of certain consumer information would be deemed to be authorized by the consumer or otherwise within the "general exceptions" under the Graham Leach Bliley Act. For example, the Commission could determine that possession and use of certain defined information for the limited purpose of soliciting a customer to the new firm is acceptable for a reasonable amount of time, even without the approval of their current firm. The Commission could mandate disclosure and an opportunity to opt in or out of account information sharing between firms in the eventuality that a representative that they have been dealing with moves to new firm in all Privacy Notices. Rather than requiring notice and recordkeeping by the existing firm, the limited information, as defined by the Commission, could be deemed properly held by departing representatives going to entities capable of providing like services to affected customers and the Commission could mandate safeguards, such as

57 See Release at 13702.

password protection, encryption, or redaction of more sensitive items, that must be applied to the storage of this information. Further, the Commission could put limits on the amount of time that such information could be held or used, put the responsibility for proper destruction on the representative, and provide standards for what that constitutes.

\* \* \* \* \*

The NSCP appreciates the opportunity to comment on this proposal. While amendments to Regulation S-P may be in order, there has not been sufficient time to assess the impact that the proposed amendments are likely to have on the industry nor to explore a balancing of the interests involved and less costly ways to achieve stated goals. We respectfully suggest that sufficient concerns have been expressed that aspects of the current proposal should be reconsidered before new amendments to Regulation S-P are adopted.

*Questions regarding our comments or requests for additional information should be directed to the undersigned at 860.672.0843.*

Sincerely yours,

A handwritten signature in black ink, appearing to read 'Joan Hinchman', with a long horizontal flourish extending to the right.

Joan Hinchman  
Executive Director, President and CEO  
*Cc: Via Postal Mail*

The Honorable Christopher Cox, Chairman  
The Honorable Paul S. Atkins  
The Honorable Kathleen L. Casey