



May 31, 2016

NASAA Legal Department
Mark Stewart, Counsel
NASAA
750 First Street NE, Suite 1140
Washington, DC 20002

VIA EMAIL

Michael Pieciak, Chair of the Corporation Finance Section
(Michael.Pieciak@vermont.gov)

Dan Matthews, Chair of the Business Organizations and Accounting Project Group
(Dan.Matthews@dfi.wa.gov)

Mark Stewart, Counsel
(nasaacomment@nasaa.org)

**RE: NASAA Proposed Statement of Policy Regarding the Use
of Electronic Offering Documents and Electronic Signatures**

Dear Chair Pieciak, Chair Matthews and Mr. Stewart,

Franklin Square Capital Partners thanks NASAA and its Corporation Finance Section (the “CFS”) for the opportunity to comment on the proposed Statement of Policy Regarding Use of Electronic Offering Documents and Electronic Signatures (the “Proposed SOP”).

Founded in Philadelphia in 2007, Franklin Square’s mission is to enhance mainstream investors’ portfolios by combining access to asset classes, strategies and asset managers typically available only to wealthy individuals and institutions with strong investor protections and industry-leading best practices. We applaud the efforts of NASAA and the CFS in formulating the Proposed SOP. We particularly appreciate your recognition of the tremendous efficiencies, reduced environmental impact, and cost-savings that the use of electronic documents and signatures represents to Franklin Square and other program sponsors, broker-dealers, registered investment advisors and, most importantly, investors. Franklin Square fully supports NASAA in this endeavor and intends the comments that follow to be entirely constructive.

(For purposes of this letter, “e-signatures” means electronic signatures, “e-prospectuses” means the delivery of prospectuses and offering related documents through an electronic medium, “e-offering” means an offering that makes use of e-signatures and/or e-prospectuses, and “paper-based offering” means an offering that does not make use of e-signatures or e-prospectuses. We also refer to electronic documents generally as “e-documents.”)

Our comments below are divided into two sections: Section I is focused entirely on Part One B.4 of the Proposed SOP – security breaches – while Section II addresses several other provisions of the Proposed SOP.

I. The Final SOP Should Define “Security Breach” and Should Conform an Issuer’s Obligations in the Event of a Security Breach to Standards Established in Other Commercial Contexts

A. Statement of Policy

Part One B.4 of the Proposed SOP states as follows:

“Subscription agreements may be provided electronically for review and completion, provided: . . . in the event of discovery of a security breach at any time in any jurisdiction, the electronic subscription process will be suspended and notification will be made to the Administrator and all investors.”

B. Definition of “Security Breach”

NASAA should define “security breach” so that sponsors, broker-dealers, and state regulators will not be left to establish their own definitions of this critical term. Otherwise, the range of possible definitions is extremely broad. A broad interpretation of this term may, in effect, be punitive to issuers that conduct e-offerings and nullify many of the efficiencies and cost-savings e-offerings promise. Conversely, too narrow an interpretation of this term may compromise the reasonable investor protections intended by NASAA. For these reasons, the Final SOP should define “security breach” and provide guidance around this definition so that an appropriate balance of investor protection and offering efficiencies is achieved.

We believe the definition of “security breach” should convey two essential concepts:

- First, a “security breach” should consist of the unauthorized acquisition or disclosure of unencrypted data that compromises the security or confidentiality of an investor’s confidential personal information; and
- Second, a “security breach” should relate only to the systems and technology that are introduced into the securities offering process in order to implement an e-offering. A breach or mishandling of information that occurs in systems or technologies that are used currently in paper-based offerings should not constitute a security breach under the Final SOP.

Fundamentally, we believe the Final SOP should address new risks created by the use of e-offerings and should not impose new regulation on old risks that exist in current practice. Proposed Guideline Part One B.1 embodies this notion – that “the subscription process is administered in a manner that is equivalent to the administration of subscription agreements in paper form.” And while we agree that the electronic subscription process should mirror the paper process as closely as possible, we also believe that the Final SOP should govern e-offerings as closely as possible to the manner in which paper-based offerings are governed under existing statements of policy. The second concept – that a security breach must be limited to those systems and technologies added to the securities offering process in order to execute an e-offering – is necessary to ensure that the Final SOP does not impose new regulation beyond the scope of e-offerings and thereby create differing regulatory schemes in a manner punitive to e-offering issuers. Otherwise, participants in

an e-offering would be placed at a disadvantage relative to participants in a paper-based offering. For example:

1. In paper-based offerings, subscription agreements and other confidential client information are maintained by broker-dealers as part of their books and records in accordance with various FINRA and SEC regulations. Those regulations allow broker-dealers to maintain their records through the use of electronic storage systems and related technologies. Also in paper-based offerings, transfer agents maintain investor data through the use of electronic storage systems in accordance with various SEC regulations. A security breach that occurs within a broker-dealer's existing books and records system, or within a transfer agent's existing document management system, should not be treated as a security breach under the Final SOP. The possibility of a security breach in such systems exists now and would not be created by or specific to e-offerings. In addition, a security breach within such systems in the context of a paper-based offering would not trigger the suspension or notification obligations contemplated by the Proposed SOP, resulting in different and unjust outcomes between paper-based and e-offerings;
2. The risk of human error or misconduct in handling data, regardless of the format or medium of such data, exists in all securities offerings. As a result, human error or misconduct that does not relate specifically to a failure or vulnerability of the systems and technology used to implement an e-offering should not be treated as a security breach under the Final SOP; and
3. All other breaches involving the execution, delivery, handling and retention of subscription agreements and other confidential client information that are inherent in a paper-based offering and do not arise directly from the implementation of an e-offering should be excluded from the definition of "security breach" in the Final SOP.

If the limitations described above are not contained in the Final SOP, then an issuer that engages in an e-offering would become subject to suspension and notification obligations flowing from conduct unrelated to, and likely preexisting, the new technologies and systems introduced to execute an e-offering. Furthermore, such regulations would not be imposed on issuers conducting paper-based offerings, despite the presence of the same risks. This disparate treatment of the same risks would create a disincentive for issuers to utilize technologies that have the potential to provide a significant savings to their shareholders.

If the restrictions described above are adopted, however, then the Final SOP's treatment of a security breach will be properly focused on those risks that are created by the technologies, systems and processes specific to the execution of an e-offering. These technologies, systems and processes will relate primarily to the use of e-signatures and the transmission of electronic records between the various parties in the completion-of-sale chain (i.e., from the registered representative or investment adviser representative, to the broker-dealer home office or custodian, to the issuer, and finally to the transfer agent). Each of these parties already maintains electronic records pertaining to individual investors in accordance with FINRA and SEC regulations; e-offerings will simply link these parties together so that records may be transferred through the chain electronically rather than by mail. Accordingly, the Final SOP's definition of "security breach"

should be limited to breaches that occur in the use of an e-signature and in the transmission of electronic records solely for the purpose of conducting an e-offering, and should not apply to breaches that may occur in the storage of electronic records.

We believe the following definition would give effect to the important concepts described above:

“Security breach” shall mean the unauthorized acquisition or disclosure of unencrypted data that compromises the security or confidentiality of confidential personal information maintained by the person or business; provided, however, that for this purpose a “security breach” shall relate only to a system, technology or process that is introduced into a securities offering in order to implement the use of e-signatures or e-prospectuses. A breach or mishandling of information that occurs in any other system, technology or process utilized by market participants shall not constitute a “security breach.”

C. Response to a Security Breach

In the event of a security breach at any time in any jurisdiction, the Proposed SOP would require an issuer to suspend the use of e-signatures and e-prospectuses and provide notice to each Administrator and every investor in the offering. In practice, this “full stop and notify everyone” requirement would likely be a lengthy and costly process that goes beyond the actual or potential risk or harm to investors.

We believe the actions an issuer should be required to take in response to a security breach should be commensurate with the nature and scope of the breach. In particular, the response should focus on identifying and locating the breach, taking prompt action to secure the affected information, and taking action to remedy the breach before resuming use of the compromised device or technology. As discussed below, we believe such a response is consistent with federal standards established in other industries and commercial settings.

For example:

1. A breach may be isolated to a single participating broker in an e-offering. In that event, the required response should be limited to the participating broker that experienced the breach, and the issuer should be permitted to continue accepting e-signatures from, and distributing e-documents through, all non-affected intermediaries.
2. If the breach can be further isolated to a particular device or technology, then the response should likewise be limited to that particular device or technology.
3. If the breach can be isolated to an e-signature technology or process, but e-prospectus technologies or processes remain unaffected, or vice-versa, then the unaffected technologies and processes should be permitted to continue.
4. The required response should consist of promptly identifying and locating the breach, taking steps to secure confidential information, and taking steps to remedy the breach.

5. Any “suspension” imposed in connection with a security breach should be limited to the particular entity, system, technology or device that experienced the breach.
6. Any requirement to provide notice of a security breach to investors should be limited to (i) those investors whose data was compromised or affected by the breach and (ii) the state securities administrators located in the state(s) in which affected investors reside.
7. Upon curing the conditions that gave rise to the security breach and restoring system integrity and/or information security, use of the suspended technology, system or device should be permitted to resume.

We believe a response based on these concepts is consistent with guidance provided by the Cybersecurity Unit of the U.S. Department of Justice. (See “Best Practices for Victim Response and Reporting of Cyber Incidents” at: <https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf>).

Because confidential personal information is gathered, transmitted and stored electronically in myriad other commercial environments, uniform standards and practices have been developed in those environments to govern the protection of electronic data. We believe that the Final SOP should be consistent with the regulations and standards developed in other contexts. For example, the regulations and standards that have been developed in the financial services and healthcare industries are instructive as those are both highly regulated environments in which the protection of an individual’s personal information is extremely important.

Standards that apply in the financial services industry include:

- The Gramm-Leach-Bliley Act (the “GLB Act”) requires that companies defined as “financial institutions” protect customer confidential information. As part of its implementation of the GLB Act, the Federal Trade Commission (“FTC”) published the Safeguards Rule and an accompanying set of guidelines to assist companies in complying with the Safeguards Rule. In the guidelines regarding security breaches, the FTC requires that financial institutions “take immediate action to secure any information that has or may be compromised” and “notify customers if their personal information is subject to a breach that poses a significant threat of identity theft or related harm.” (<https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying#how>)
- In addition, the Department of the Treasury, Federal Reserve, and Federal Deposit Insurance Corporation issued Interagency Guidance (the “Interagency Guidance”) clarifying the responsibilities of financial institutions under the GLB Act. In the Interagency Guidance, the agencies state that a financial institution, upon becoming aware of a security breach, should “conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused” and, if so, “notify the affected customers as soon as possible.” (<http://www.occ.treas.gov/news-issuances/news-releases/2005/nr-ia-2005-35a.pdf>)

Standards that apply in the healthcare industry include:

- The Health Information Technology for Economic and Clinical Health Act (the “HITECH Act”) provides that all “covered entities” under the Health Insurance Portability and Accountability Act (“HIPAA”), upon “discovery of breach of unsecured protected health information,” shall “notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed” as a result of the security breach. (<https://www.law.cornell.edu/cfr/text/45/164.404#c>)
- The FTC’s Health Breach Notification Rule (the “HBN Rule”) requires vendors of personal health records (“PHR”) and related entities that are not covered by HIPAA to notify an affected person when “there has been an unauthorized acquisition of PHR-identifiable health information that is unsecured and in a personal health record.” Under the rule, health information is only considered “unsecured” if it is not encrypted or destroyed at the time of the breach. (<https://www.ftc.gov/system/files/documents/plain-language/bus56-complying-ftcs-health-breach-notification-rule.pdf>)

The financial services and healthcare regulations described above are instructive on these important concepts:

1. Upon discovery of a security breach, notice should be given only to those individuals whose confidential information has been accessed or disclosed. Notice to individuals whose confidential information was not accessed or disclosed should not be required.
2. If personally-identifiable information that is accessed or disclosed in a security breach is encrypted, destroyed, or otherwise secure at the time of the breach, then notice of the breach should not be required.
3. Suspension of the system in which a security breach occurred is not required under any of the federal regulations summarized above. Instead, steps to investigate the breach and secure confidential information should immediately be taken.

We believe each of these concepts should be reflected in the Final SOP.

D. Recommendations

For the reasons discussed above, we believe that the Final SOP should define “security breach,” and should provide for an issuer response to a security breach, which are substantially as follows:

“Security breach” shall mean the unauthorized acquisition or disclosure of unencrypted data that compromises the security or confidentiality of confidential personal information maintained by the person or business; provided, however, that for this purpose a “security breach” shall relate only to a system, technology or process that is introduced into a securities offering in order to implement the use of e-signatures or e-prospectuses. A breach or mishandling of information that occurs

in any other system, technology or process utilized by market participants shall not constitute a “security breach.”

In the event of discovery of a “security breach” at any time in any jurisdiction, the issuer or its agents, as appropriate, will take prompt action to (i) identify and locate the breach, (ii) secure the affected information, (iii) suspend the use of the particular device or technology that has been compromised until information security has been restored, and (iv) provide notice of the security breach to any investor whose confidential personal information has been improperly accessed in connection with the security breach and to the securities administrator of each state in which an affected investor resides.

II. Other Comments

A. Part One A.1.c

Part One A.1.c of the Proposed SOP requires all offering documents to be “delivered as a single, integrated document or file.” The single-document-delivery requirement appears to assume that e-document delivery will be conducted by one of two means: (1) emailing offering documents from the issuer to the prospective investor, or (2) physical delivery of an electronic storage device containing the offering documents to the investor. However, other means of delivering e-documents exist now and likely will be developed in the future. For example, another method currently utilized entails directing prospective investors to a secure website where the issuer’s electronic offering documents may be accessed. We believe it is beneficial for investors to be able to see (and download) the e-documents available to them separately rather than as a single, large file where individual documents run together and become difficult to distinguish.

We believe the single-document requirement of Part One A.1.c would restrict the delivery of e-documents to one or two methods that may be less user-friendly for investors than other current and future methods of delivery and, therefore, NASAA should consider removing this requirement from the Final SOP. Alternatively, NASAA should specify the documents which must be delivered as a single, integrated document or file. Otherwise, an ambiguity exists that could make compliance with this guideline challenging. Specifically, it would be impossible for an e-offering issuer to comply with this provision if “offering documents” in this context include subsequently produced and disseminated materials, such as prospectus supplements and amendments, and advertising and sales literature.

B. Part One A.1.d

Part One A.1.d would prohibit electronic offering documents from containing a link to or from external documents or content. The prospectuses of virtually all DPP offerings, including those filed electronically on EDGAR and those currently available in PDF format on issuer websites, contain hyperlinks. For example, the prospectuses of Franklin Square’s non-traded BDCs contain links to three websites of interest to those funds’ investors and prospective investors: www.franklinsquare.com; <http://ir.blackstone.com>, the website of The Blackstone Group, the

funds' sub-adviser; and www.sec.gov. Moreover, disclosure of the issuer's website and the SEC's website on offering documents may be required under various SEC regulations.¹

C. Part One A.2

Part One A.2 sets out four conditions an issuer must satisfy in order to deliver electronic offering documents under the Proposed SOP. In the context of a paper-based offering, however, many or all of those functions are currently performed by intermediaries, which likely will continue to be the most appropriate parties to perform such functions in the context of an e-offering. Regarding Part One A.2.d, for example, both paper and e-prospectus kits are often handed from advisor to prospective investor, making it impossible for the issuer to document such deliveries.

NASAA should clarify that the conditions required in Part One A.2 may be satisfied by or through agents on behalf of the issuer, such as a selling broker-dealer or investment adviser. Considerable precedent for this sort of division of labor exists in other NASAA statements of policy.² Furthermore, Part One I of the Proposed SOP specifically contemplates that contractors and agents of an issuer may have custody and possession of e-offering documents, including subscription agreements.

D. Part One B.1

Part One B.1 requires that “the subscription process is administered in a manner that is equivalent to the administration of subscription agreements in paper form.” While we agree with this provision and support even broader application of the concept of equivalency of the administration of paper-based and e-offerings generally, we are concerned that potential ambiguity in this guideline may lead to varying interpretations. For example, some may read “equivalent” to mean “identical,” while others may read it as “similar.” Guidance on the application of this provision would benefit all market participants.

E. Parts One E, Two A.2, and Two C

Parts One E and Two C require an issuer to obtain informed consent to receive and sign offering documents electronically “in connection with each new offering.” This offering-by-offering approach to obtaining investor consent is currently used by some DPP issuers and should be permitted under the Final SOP. However, outside the non-traded DPP context, an investor's election to receive documents electronically is typically handled on a relationship basis or account basis rather than on an investment-by-investment basis. Parts One E and Two C should be expanded in the Final SOP to also permit account-based or relationship-based consent, consistent with SEC guidance.

An example of an account-based-election could be a 401(k) account holding multiple mutual fund investments. The investor would typically be able to elect to receive all documents related to that

¹ See, e.g., 17 C.F.R. 229.101(e)(4) (Regulation S-K), 17 C.F.R. 230.482(b)(3), and Items 1.1.d, 18.16, and 24.6-8 of the Form N-2.

² See, e.g., NASAA REIT Guidelines III.C.2-4, “The SPONSOR or each PERSON selling SHARES on behalf of the SPONSOR or REIT shall . . .” (emphasis added).

account electronically rather than having to make separate elections for each fund held in the account. Similarly, an example of a relationship-based-election could be where an investor has multiple accounts with the same institution, such as a 401(k), an IRA, a 529 plan, and a standard brokerage account. The institution may offer that investor the opportunity to make an election that covers the investors' entire relationship with the institution, i.e. to receive electronically all communications from the institution related to any of the accounts or any of the investments held within each account.

The SEC specifically permitted relationship-based consent, which they refer to as "global consent," in Securities Act Release No. 7856, "Use of Electronic Media," dated April 28, 2000. In this release, the Commission stated, "We believe that an investor may give a global consent to electronic delivery -- relating to all documents of any issuer -- so long as the consent is informed."³ Even in the case of global consent, we agree that investors should be able to change their election at any time should they prefer to receive or sign paper documents. However, we do not believe it is necessary or as efficient for the investor to be required to re-sign-up to receive or sign e-documents for each public, non-traded investment in their account when account-based or relationship-based elections suffice for all other investments. NASAA should expand Parts One E and Two C in the Final SOP to also permit global consent to participate in e-prospectus and e-signature programs consistent with SEC guidance.

Finally, the Proposed SOP provides that an investor may revoke his or her consent to participate in an e-signature or e-document program at any time. We agree with this requirement, but request clarification as to whom such revocation should be delivered. In a series of interpretive releases, the SEC suggests that electronic delivery consents and revocations should both be directed to intermediaries rather than issuers.⁴ We suggest that Parts One E and Two A.2 be revised to provide that, "The investor may revoke this consent at any time by informing the party to whom the consent was given, or, if such party is no longer available, the issuer."

F. Part One I

Part One I places on issuers and their contractors and agents storage and maintenance requirements relating to "all documents." NASAA should clarify that this provision pertains only to the electronic offering documents that are the subject of the Proposed SOP. Additionally, the requirement that parties "maintain secure offsite backups" should apply to e-documents only to the same extent that such requirement applies to paper documents. Part One B.1 requires that "the subscription process is administered in a manner that is equivalent to the administration of subscription agreements in paper form." Similarly, if secure offsite backups of paper subscription agreements are not required to be maintained, then secure offsite backups should not be required of electronic subscription agreements. Furthermore, the establishment and maintenance of such

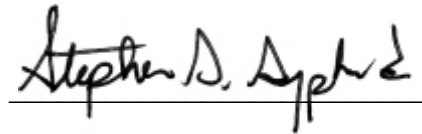
³ Use of Electronic Media, Securities Act Release No. 7856 (Apr. 28, 2000)

⁴ *See, generally*, Use of Electronic Media for Delivery Purposes, Securities Act Release No. 7233 (Oct. 6, 1995); Use of Electronic Media by Broker-Dealers, Transfer Agents, and Investment Advisers for Delivery of Information, Securities Act Release No. 7288 (May 9, 1996); and Use of Electronic Media, Securities Act Release No. 7856 (Apr. 28, 2000).

secure offsite backups may come at significant expense to shareholders in exchange for comparatively little benefit.

Franklin Square sincerely thanks NASAA and the CFS for the opportunity to comment on the Proposed SOP. We hope this letter helps the CFS strike an appropriate balance between investor protection and the realization of significant efficiencies through the use of reliable technologies. We stand ready to assist NASAA and the CFS in any other way we are able.

Sincerely,



Stephen S. Sypherd
General Counsel



Seth Hertlein
Senior Counsel

Franklin Square Capital Partners