standards for strong encryption" is too vague; and the perception that FINRA is proposing to impose security burdens on its members but does not have or follow an information security program itself.[4]

As addressed in more detail below, FINRA believes many of these concerns are unfounded or based on a misapprehension or misconception of the design and intention of the proposed rule change. Accordingly, FINRA urges the Commission to approve the proposed rule change as submitted.

Background

The proposed rule change would require information provided via portable media device pursuant to a request under FINRA Rule 8210 be encrypted, *i.e.*, the data must be encoded into a form in which meaning cannot be assigned without the use of a confidential process or key. As stated in the proposed rule change, requiring such information to be encrypted will help ensure that such information, which in many instances includes individuals' personal information, is protected from unauthorized or other improper use.

The proposed rule change in part addresses potential issues raised by laws in some jurisdictions, including Massachusetts and Nevada, that establish minimum standards to safeguard personal information in electronic records.[5] These laws contain potential penalties against persons and entities for failures to adequately safeguard electronic information containing personal information.

To help ensure that encrypted information is secure, persons providing encrypted information to FINRA via portable media device would be required to (1) use an encryption method that meets industry standards for strong encryption, and (2) provide FINRA staff with the confidential process or key regarding the encryption in a communication separate from the encrypted information itself (*e.g.*, a separate e-mail, telephone call, fax or letter). FINRA deliberately designed the requirements broadly in order to adapt to changing technology. By referring to "industry standards for strong encryption," the rule provides for appropriate flexibility and adaptability. Currently, FINRA views industry standards for strong encryption to be 256 bit or higher encryption. It is FINRA's understanding that software is available through several vendors via the Internet at no cost or minimal cost to

---

4 *See* comment letters from Great Nation, NAIBD, Pacific Select, Triad-DeMarco (supporting NAIBD), Triad-Holland (supporting NAIBD), Wedbush and Wulff Hansen (supporting NAIBD).

5 *See, e.g.*, Commonwealth of Massachusetts, 201 CMR 17.00 (Standards for the Protection of Personal Information of Residents of the Commonwealth), effective March 1, 2010; State of Nevada, NRS 603A.215 (Security Measures for Data Collector that Accepts Payment Card; Use of Encryption; Liability for Damages; Applicability), effective January 1, 2010.

the user that will encrypt documents at this standard. Consequently, FINRA has reason to believe that the costs of encryption for members today would be de minimis. In any event, the protection of investor personal information in electronic records sets out a rational requirement for the rule and its costs.

Concerns Regarding Scope

Four commenters suggest that the application of the rule to electronic media but not paper documents is too narrow or misplaced.[6] They note that members routinely respond to requests by e-mail (presumably passing unencrypted information through e-mail) or via submission of paper copies, either in person or using courier or postal services. One of these commenters further believes the rule is unnecessary for portable media devices because they are no different than the delivery of any hard copy data other than convenience.[7] Another commenter suggests the alternative of requiring that a disc be delivered by Fed Ex or UPS instead of encryption.[8] While FINRA believes that encryption is a useful method to protect electronic data, including information communicated through e-mail, it is technically infeasible to encrypt information submitted in paper form. Perhaps in the future FINRA could require documents be submitted only electronically to ensure that information is encrypted, but currently FINRA allows the submission of information in paper form and must accept the limitations of this method of information delivery. In the future, FINRA will explore whether to require encryption of other methods of communication that may contain personal data, such as e-mail. However the argument that the difficulty of the perfect encryption of all information irrespective of the media is a reason not to protect that information which can be encrypted could be used to negate all iterative protections to investors and should not be credited as a matter of public policy.

Conversely, three commenters suggest that requiring encryption of all information sent via portable media vice is overbroad.[9] For example, one of these commenters questioned the need for encryption of documents that do not include customer-related data, such as publically available prospectuses.[10] This commenter advocated that the member producing the documents be able to make a determination as to whether the information being submitted via portable media device contains information that should be encrypted. FINRA believes it is simpler, more efficient and safer to require encryption of all information provided via portable media device pursuant to a request under the rule. This requirement obviates the need for FINRA to circumscribe and monitor, and for members to determine,

---

6 *See* comment letters from IMS, NAIBD, Pacific Select and Regal.

7 *See* comment letter from Regal.

8 *See* comment letter from Abel/Noser.

9 *See* comment letters from Great Nation, IMS and Pacific Select.

10 *See* comment letter from Pacific Select.

the types of information that should or should not be encrypted under the rule. FINRA believes that the costs of determining and monitoring whether information included on portable media devices contains the type of information would be much greater than the costs of simply encrypting all such information submitted via portable media device, currently available through low- or no-cost software available online. Such an approach also further supports compliance with the laws in some jurisdictions that establish minimum standards to safeguard personal information in electronic records.[11]

Concerns Regarding Difficulties or Costs of Compliance

Some commenters challenge the proposal's requirement that member firms assume responsibility for properly encrypting portable media devices when transmitting information to FINRA. Two commenters posit that small firms lack the technical expertise to implement the rule and would be required to hire third parties to comply with this requirement.[12] Another commenter urges that FINRA provide an exception to the requirement to encrypt material that is provided directly to FINRA staff on the firm's own premises or personally delivered to FINRA staff on FINRA's premises.[13] First, FINRA questions the burden on members given the availability of web-based encryption solutions currently available at low- or no-cost. In addition, as noted above, FINRA members may be subject to various state data protection laws that are in part the impetus for this proposal. Finally, to help educate its membership about the process of encryption, FINRA will endeavor to provide information regarding various options for encrypting data, including using low- or no-cost web-based encryption software.

Commenters argue that the proposed requirement to use an encryption method "that meets industry standards for strong encryption," is too vague, or could be a moving target.[14] Consequently, they urge FINRA to adopt some sort of (presumably more detailed) mandatory standard for the production of customer related data, or alternatively to provide members directly with an appropriate method of encryption.[15] FINRA acknowledges that, as proposed, the rule does not mandate a specific method of encryption; however, FINRA believes that such a standard, which is identical to that employed by Massachusetts and Nevada in their data protection laws, is necessary for the concept to adapt to changing technology regarding encryption. Further, FINRA believes it is not appropriate at this time to dictate a "one size fits all" approach to encryption and has designed this requirement to allow each member to choose an appropriate method of encryption that works for it.

---

11 *See supra* note 5.

12 *See* comment letters from NAIBD and Pacific Select.

13 *See* comment letter from Wulff Hansen.

14 *See* comment letters from NAIBD and Pacific Select.

15 *See* comment letter from Pacific Select.

Concerns Regarding FINRA's Information Security Policy and Related Practices

Commenters question the need for the encryption requirement, mistakenly concluding that this requirement somehow illustrates that FINRA's practices with respect to safeguarding of information provided to it by its members are inadequate or nonexistent.[16] One commenter urges FINRA to review its practices regarding information security, and only after such a review and determination of safeguards throughout FINRA should it determine whether such encryption is really necessary.[17] While such comments are beyond the scope of the proposed rule change insofar as the purpose of the proposed rule change is to safeguard information being delivered to FINRA via portable media devices, FINRA notes that, as part of its regulatory program, it has a robust and current information security policy in place that sets forth the day-to-day standards for collecting, using and sharing information throughout the organization.

Uniform Standard

Commenters suggested that FINRA work with states and other jurisdictions to provide a uniform standard for use within the securities industry prior to the implementation of this rule, if adopted.[18] Such comments are beyond the scope of the proposed rule change. While developing a uniform standard regarding information security and data protection is a sound goal, FINRA has no authority to mandate such a standard. Much of that authority, as evidenced by recent State legislation regarding data protection, is within the purview of the States. FINRA is proposing this rule in part to support compliance with such standards.

FINRA believes that the foregoing fully responds to the issues raised by the commenters to the rule filing. Please feel free to contact me at (202) 728-8056 if you have any questions.

Very truly yours,

Stan Macel
Assistant General Counsel

---

16 *See* comment letters from NAIBD and Pacific Select.

17 *See* comment letter from Pacific Select.

18 *See* comment letter from NAIBD and Pacific Select.

Exhibit A

Comments on FINRA Rulemaking

Self-Regulatory Organizations; Financial Industry Regulatory Authority, Inc.; Notice of Filing of Proposed Rule Change Relating to FINRA Rule 8210 To Require Information Provided via Portable Media Device Be Encrypted

(Release No. 34-62318; File No. SR-FINRA-2010-021)

Total Number of Comment Letters Received – 11

1. Howard Spindel, Senior Managing Director, Integrated Management Solutions, dated July 16, 2010 ("IMS")

2. S. Kendrick Dunn, Assistant Vice President, Pacific Select Distributors, Inc., dated July 16, 2010 ("Pacific Select")

3. Sis DeMarco, Director of Compliance, Triad Securities Corp., dated July 15, 2010 ("Triad - DeMarco")

4. Raymond C. Holland, Vice-Chariman, Triad Securities Corp., dated July 15, 2010 ("Triad - Holland")

5. Eric Segall, Senior Vice President, Manager, Business Conduct, and Edward W. Wedbush, President, Wedbush Securities Inc., dated July 15, 2010 ("Wedbush")

6. Byron "Pat" Treat, President/CEO, Great Nation Investment Corp., dated July 15, 2010 ("Great Nation")

7. Tamara K. Salmon, Senior Associate Counsel, Investment Company Institute, dated July 14, 2010 ("ICI")

8. Chris Charles, President, Wulff, Hansen & Co., dated July 13, 2010 ("Wulff Hansen")

9. Lisa Roth, Member Advocacy Committee Chair, National Association of Independent Brokers Dealers, Inc., dated July 9, 2010 ("NAIBD")

10. Larry Taunt, Chief Executive Officer, Regal Financial Group, dated July 7, 2010 ("Regal")

11. David M. Sobel, Esq., Executive Vice President and Chief Compliance Officer, Abel/Noser Corp., dated July 6, 2010 ("Abel/Noser")