FINANCIAL SERVICES INSTITUTE

VOICE OF INDEPENDENT FINANCIAL SERVICES FIRMS AND INDEPENDENT FINANCIAL ADVISORS

VIA ELECTRONIC MAIL

March 29, 2016

Deputy Commissioner Michael Pieciak
State of Vermont
Department of Financial Regulation
89 Main Street
Montpelier, VT 05620

Re: Notice of Request for Comments Regarding Vermont Securities Regulation Rule No. S-2016-01

Dear Deputy Commissioner Pieciak:

On February 17, 2016 the Vermont Department of Financial Regulation, Securities Divisions (Department) issued regulatory proposal Securities Rule No. S-2016-01(Proposal) for public comment. The rule establishes a comprehensive set of regulations to govern the sale of securities in Vermont. The Financial Services Institute (FSI) appreciates the opportunity to comment on this important Proposal.[1]

FSI's members are strongly committed to working with all stakeholders to help ensure clarity for financial advisors and broker-dealers, when complying with state and federal securities requirements. FSI commends the Department's determination to consolidate these various regulatory requirements into one easy to read document. FSI members offer suggestions on ways to improve the provisions related to protection of vulnerable adults from financial exploitation and cybersecurity. We elaborate on our viewpoints and provide suggested potential solutions in our comments below.

Background on FSI Members

The independent financial services community has been an important and active part of the lives of American investors for more than 40 years. In the U.S., there are approximately 167,000 independent financial advisors, which account for approximately 64.5% producing registered representatives. These financial advisors are self-employed independent contractors, rather than employees of Independent Broker-Dealers (IBD).

FSI member firms provide business support to financial advisors in addition to supervising their business practices and arranging for the execution and clearing of customer transactions.

[1] The Financial Services Institute (FSI) is an advocacy association comprised of members from the independent financial services industry, and is the only organization advocating solely on behalf of independent financial advisors and independent financial services firms. Since 2004, through advocacy, education and public awareness, FSI has been working to create a healthier regulatory environment for these members so they can provide affordable, objective financial advice to hard-working Main Street Americans.

Independent financial advisors are small-business owners who typically have strong ties to their communities and know their clients personally. These financial advisors provide comprehensive and affordable financial services that help millions of individuals, families, small businesses, associations, organizations and retirement plans with financial education, planning, implementation, and investment monitoring. Due to their unique business model, FSI member firms and their affiliated financial advisors are especially well positioned to provide middle-class Americans with the financial advice, products, and services necessary to achieve their investment goals.

Discussion

A. Introduction

The Department's Proposal creates a comprehensive set of regulations for the securities industry, which aims to make operating within the securities laws in Vermont easier to understand and implement correctly. The format and language of the Proposal are drafted in a way that should make it easier for advisors and firms to understand how to comply, which strengthens their confidence that they are following all relevant rules and requirements. It is clear that the intent of drafting this Proposal was to ensure that regulatory requirements are written in plain English and are easily understood by firms and advisors in Vermont. FSI commends this undertaking and provides the following suggestions for strengthening the Proposal further.

B. FSI applauds the Department for consolidating various regulatory requirements into one easy to read document.

This Proposal consolidates FINRA, SEC, and Vermont requirements into one easy to read document. The consolidation demonstrates how various rules interact, helping to ensure compliance by advisors and firms. The consolidation also demonstrates how Vermont continues to ensure their rules are timely and updated when appropriate. The language of the consolidation is in plain English which should help firms gain confidence that they know what the rules are and what they need to do to comply with them. By writing the regulations in plain English there is also more clarity for individual advisors to understand their regulatory responsibilities.

C. FSI's comments regarding V.S.R. § 8-5 Protection of Vulnerable Adults from Financial Exploitation.

a. FSI commends the Department on the time period for holding disbursements. We request clarity as to what disbursement means and an additional provision allowing the freezing of transactions.

FSI appreciates that the Department has followed the North American Securities Association Administration's (NASAA) model act designed to protect vulnerable adults from financial exploitation. The Proposal allows a temporary hold on a disbursement for 15 business days with a renewal for another 10 business days, for a maximum of 25 business days. FSI strongly supports the Department's stance on delaying disbursements. The delay would allow firms to hold a disbursement for an adequate amount of time to dissuade any possible abuse or manipulation while also protecting account holders' rights to their funds.

FSI first suggests that the Department provide a definition of the term "disbursement." The current Proposal does not define the term and it is unclear if disbursements include the transfer of funds to another custodian or broker-dealer firm. Our members have seen examples of unscrupulous persons encouraging vulnerable adults to transfer their funds from a long-trusted financial advisor to another firm in order to facilitate their financial exploitation. As a result, we recommend asset transfers be included within the definition of disbursement. However, if the Department chooses not to include transfers in the definition of disbursement we believe it is essential that the Proposal allow firms to freeze transactions.

FSI suggests that in addition to allowing delays in disbursements, the Department should allow qualified employees to initiate a freeze on a transaction if there are reasonable suspicions that financial exploitation has occurred, is occurring, has been attempted, or will be attempted. A transaction freeze could prevent the liquidation of securities that could have serious financial consequences for a client, such as a liquidation of a variable annuity with high early termination fees and significant tax implications. An initial freeze of 15 business days would allow sufficient time for a proper internal review of the suspected financial abuse. Additionally firms could be required to notify all those involved on the account within five business days, in the event of a transaction freeze. FSI is not alone in supporting such a transaction freeze. SEC Investor Advocate Rick Fleming stated that he believes allowing firms to delay or freeze securities related transactions would be a helpful tool in the fight to prevent abuse of eligible adults.[2] FSI believes providing firms the option to freeze a transaction or disbursement would provide maximum protection to vulnerable adults.

b. <u>FSI commends the Department for providing an immunity provision. We request clarity regarding this provision and suggest an additional provision extending the immunity provision.</u>

The Proposal provides an immunity provision for qualified employees who make necessary voluntary disclosures to either government or third parties, such as Adult Protective Services (APS). FSI strongly supports this provision. Protecting financial advisors and qualified employees from liability for reporting elder abuse suspicions enables them to express their concerns without fearing repercussions. FSI requests this immunity provision clearly spell out to advisors and firms that in disclosing this important information they would not be subject to potential regulatory action for providing the necessary information to relevant agencies.

Additionally, FSI requests that the immunity provision also apply to individuals and firms who conduct a good faith investigation regarding potential abuse but do not discover instances of fraud, only to learn later that fraud had occurred. The extension of the immunity provision to cover this instance would allow firms to conduct investigations without the fear of liability in instances where they were unable to reasonably detect fraud. FSI therefore suggests adding the following language to V.S.R. § 8-5:

> (h) *<u>Immunity for Good Faith Inquiries</u>*: A qualified individual that, in good faith and exercising reasonable care, believes that financial exploitation of an eligible adult may have occurred, may have been attempted, or is being

[2] *Protecting Elderly Investors from Financial Exploitation Questions to Consider*, Feb. 5, 2015, *available at* https://www.sec.gov/news/speech/protecting-elderly-investors-from-financial-exploitation.html.

attempted, and conducts an in depth inquiry into the suspected financial exploitation is immune from any administrative or civil liability that might otherwise arise due to their failure to detect the fraud.

FSI believes that this additional provision will help prevent instances of abuse against vulnerable adults.

c. <u>FSI expresses concern over the use of a mandatory reporting standard and suggests the implementation of a permissive reporting standard.</u>

This Proposal mandates the reporting of suspected abuse to the APS in the Vermont Department of Disabilities, Aging & Independent Living. FSI appreciates the clarity as to who to report suspected fraud. FSI understands the need for firms and advisors to be vigilant and report instances of suspected financial abuse or exploitation, but FSI is concerned about the possibility of over-reporting. Under a mandatory standard, firms will feel the need to report even the slightest suspicion to avoid potential liability. FSI is concerned that over-reporting would make it more difficult to properly investigate legitimate claims due to an overabundance of claims that over-tax limited APS and state resources. FSI therefore recommends using a permissive standard. A permissive standard would better allow for qualified employees to conduct a more thorough inquiry of instances of suspected abuse without the additional strain to state resources. FSI recommends the following changes to V.S.R. § 8-5 (a) to make it a permissive standard:

> (a) <u>Governmental Disclosures.</u> If a qualified individual reasonably believes that financial exploitation of an eligible adult may have occurred, may have been attempted, or is being attempted, the qualified individual ~~must promptly~~ may notify Adult Protective Services in the Vermont Department of Disabilities, Aging & Independent Living and the commissioner (collectively "the agencies").

FSI strongly believes that this change will help prevent instances of abuse against eligible adults.

D. <u>FSI's comments regarding V.S.R. § 8-4 Cybersecurity Procedures.</u>

a. <u>FSI suggests using the NIST framework to ensure compliance conformity and clarity</u>.

FSI understands and agrees that company's cybersecurity efforts must keep pace with emerging cyber threats in order to ensure the protection of client information. Nearly every transaction of substance in the modern economy is conducted in whole or in part online. In 2014 there were a reported 79,790 security breach incidents affecting more than 700 million account records.[3] As a result, it is clear that cybersecurity threats are numerous, evolving and potentially very damaging to investors.

---

[3] *Verizon 2015 Data Breach Investigations Report* (2015), *available at* http://www.verizonenterprise.com/DBIR/2015/; see also *Symantec Internet Security Report* (2015), *available at* https://know.elq.symantec.com/LP=1542.

Under federal regulations, broker-dealers are required to have procedures and safeguards to protect client information. The Gramm Leach-Bliley Act requires the establishment of appropriate standards that ensure the security of customer records and protect against anticipated threats and unauthorized access to such information that could result in harm or inconvenience to the customer.[4] Under SEC Regulation S-P, a firm must establish reasonably-designed written policies and procedures to ensure the security and confidentially of customer records and information.[5] SEC Regulation S-ID also requires firms to create and maintain reasonably-designed policies and procedures to promote identification, detection, and response to red flags for identity theft.[6]

The Department's current Proposal requires firms to maintain reasonably designed written procedures to ensure cybersecurity. A firm's procedures are deemed reasonable based on seven specific factors that the Commissioner may take into consideration. But the factors used to determine the "reasonableness" of a plan could be improved by providing additional clarity regarding regulator expectations by instead adopting the federal National Institute of Standards and Technology (NIST) framework.[7] The framework was developed through an in depth collaboration between the private and public sectors. It consists of voluntary standards, guidelines, and practices to promote the protection of critical infrastructure. The framework is not a technical document but instead provides a holistic risk-based flexible approach that can apply to both small and large size firms. Importantly the framework provides tools to assist firms and advisors in evaluating vendors and other third-parties that have access to their networks, systems, and data. It also uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs. The NIST Framework sets out five core functions and control objectives for cybersecurity risk management and oversight. The five categories for which companies should adopt and implement protocols are: (1) Identify, (2) Protect, (3) Detect, (4) Respond, and (5) Recover. This framework was advocated by the SEC and FINRA in recent investigations regarding a firm's preparedness for cyber threats.

FSI believes that using the NIST framework not only provides all interested parties proper notice of their regulatory requirements, but also ensures that firms can take a uniform approach when developing these policies and procedures. The framework provides clear earmarks of definitions and restrictions. Additionally, adopting this framework would benefit the Department by allowing it to participate in a larger discussion with the private sector and other state and federal agencies that have adopted the framework and share experiences regarding compliance problems.

b. <u>FSI requests more clarity regarding what the mandated cybersecurity procedure requirements entail</u>.

---

[4]Gramm-Leach-Bliley Act, *available at* https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act.

[5] *Privacy of Consumer Financial Information*, 17 CFR PART 248, *available at https://www.sec.gov/rules/final/34-42974.htm*

[6] *Identity Theft Red Flag Rules*, 17 CFR Part 248, *available at* https://www.sec.gov/rules/final/2013/34-69359.pdf.

[7] The National Standards and Technology (NIST), an agency of the U.S. Department of Commerce, released the first version of the Framework for Improving Critical Infrastructure Cybersecurity on February 12, 2014. *NIST Framework available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

The Proposal requires specific provisions be part of a firm's cybersecurity procedures. FSI requests that these provisions be clearly defined in either V.S.R § 8-4 or V.S.R. § 1-2 to ensure all parties understand their compliance requirements. FSI offers the following suggestions on how to define these terms consistent with definitions used by FINRA and the NIST.

- "Cybersecurity" is "the protection of investor and firm information from compromise through the use—in whole or in part—of electronic digital media, (e.g., computers, mobile devices or Internet protocol-based telephony systems). 'Compromise' refers to a loss of data confidentiality, integrity or availability."[8]
- "Encryption" is the protection of the confidentiality of data by ensuring that only approved users can view the data.[9]
- "Authentication" or access control is the determination of "allowed activities of legitimate users, mediating every attempt by a user to access a resource in the system."[10]

FSI believes that these definitions will help ensure firms and financial advisors understand their regulatory requirements while creating greater uniformity in cybersecurity regulatory requirements.

Additionally we call on the Department to recognize the unique impact of cybersecurity requirements on the independent channel. Independent financial advisors run their own businesses and pay their own costs. This means they also own and pay for their own electronic devices, computers, Internet service, technology support, and other services. Independent firms implement policies and procedures to ensure encryption and authentication programs are loaded onto the devices and conduct surveillance to ensure advisors comply. However, independent contractor financial advisors' devices are not necessarily connected to one cohesive network creating the opportunity for failures to properly secure client data. Therefore, FSI believes there may be implementation challenges for FSI member financial advisors who are independent contractors and not employees of their firms. As a result, FSI requests that these requirements not be mandated, but instead encouraged and viewed favorably as part of a firm's overall cybersecurity plan.

The Proposal also requires a disclosure be given to clients describing potential problems that can arise from using electronic communication. FSI requests more clarity as to when this disclosure would need to be provided to a client. It is not uncommon for a client to provide personal information to an advisor prior to becoming a client. The current wording of the Proposal can be read as requiring firms to warn clients about the risks of using electronic communication even though this person is still only a potential client. This would be an unreasonable requirement fraught with significant compliance challenges. Therefore, we suggest that the Proposal be amended to state clearly that the disclosure must be provided to clients only.

---

[8] *FINRA Report on Cybersecurity Practices*, Feb. 2015, *available at* https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf.
[9] *Id.*
[10] Vincent C. Hu, David F. Ferraiolo, D. Rick Kuhn, *Assessment of Access Control Systems*, NIST, Sept. 2006, *available at* http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf.

Finally, we note that the Proposal does not specify the content of the disclosure. Firms would benefit from clear guidance from the Department on the specific risks that should be included in the disclosure. We suggest that many of these risks are already dealt with in firms' business continuity plans. Since FINRA Rule 4370(e) requires firms to disclose the details of their business continuity plan to their customers, we ask the Department to state clearly that compliance with that rule will also satisfy the requirements of the Proposal. Allowing firms the ability to meet both requirements through a single disclosure would greatly reduce compliance burdens for firms while avoiding bogging investors down with additional paperwork.

c. <u>FSI requests relief and flexibility around mandatory insurance</u>

The Proposal requires "securities professionals", meaning any person providing investment-related services in Vermont, to maintain "adequate" insurance. Adequate insurance is determined by eight specified factors: firm's size, firm's organizational structure, scope of firm's business activities, number and location of offices, nature and complexity of products and services offered, firm's volume of business, number of investment adviser representatives assigned to a location, and specification of the office as a non-branch location. FSI is concerned that these factors are too vague. This lack of clarity impacts firms' and advisors' ability to feel confident they are meeting the requirements.

Cyber liability insurance is still a new concept and premiums can be substantial and unpredictable. The market for this new insurance is suspected to grow dramatically over time. In 2014 "51% of insurers and insurance agencies d[id] not have anyone dedicated to underwriting cyber risk policies."[11] Additionally cyber risks are difficult for insurance underwriters to quantify because of the lack of actuarial data. Insurers compensate based on qualitative assessments of an applicant's risk management procedures and risk culture. As a result, policies for cyber risk are more customized than other risks insurers take on, and, therefore are more costly.[12] Premiums for cybersecurity insurance totaled $1 billion in 2012 and $1.3 billion in 2013.[13] Additionally one of the difficulties associated with the high costs of cybersecurity insurance is that it can put firms in a position where they will have to choose between spending money on cybersecurity insurance or investing in technology that will improve their cybersecurity. This would be an unfortunate outcome.

Purchasing proper coverage presents a real challenge, particularly to small businesses because it requires a thorough understanding of the organization's particular risk factors, including numbers of customers and transactions, industry regulations, value of intellectual property, and potential for lawsuits. It is difficult for insurers to know the actual frequency and extent of cyber breaches that have taken place among potential insurance purchasers. The lack of information concerning cyber threats makes it even more difficult for an insurer to assess the

---

[11] Shiela Strubel, *Here's Why You Aren't Selling More Cyber Insurance,* Western Alliance, Nov. 12, 2014, *available at* http://www.piawest.com/blogpost/1199781/202434/Here-s-Why-You-Aren-t-Selling-More-Cyber-Insurance?tag=Cyber+Breach.

[12] Russell Cameron Thomas, Total cost of security: a method for managing risks and incentives across the extended enterprise, in PROCEEDINGS OF THE 5TH ANNUAL WORKSHOP ON CYBER SEC. & INFO. INTELL. RESEARCH: CYBER SEC. & INFO. INTELL. CHALLENGES & STRATEGIES (Frederick Sheldon et al. eds., 2009), available at http://www.csiir.ornl.gov/csiirw/09/CSIIRW09-Proceedings/Abstracts/Thomasabstract.pdf.

[13] Nicole Perlroth & Elizabeth A. Harris, Cyberattack Insurance a Challenge for Business, N.Y. TIMES (Jun. 8, 2014), http://www.nytimes.com/2014/06/09/business/cyberattack-insurance-a-challenge-for-business.html?hp&_r=2.

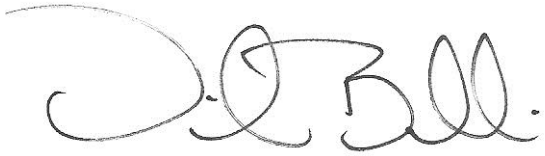
strength of a company's cybersecurity infrastructure and offer correspondingly priced premiums. The result is that these small firms could be denied insurance coverage, meaning they would be unable to comply with this regulatory requirement even with a good faith attempt. The untested waters of the cybersecurity insurance market should not be a barrier for advisors and firms to conduct business in Vermont. Therefore, FSI requests that the Department not require firms to have cybersecurity insurance at this time and perhaps revisit the requirement once the cyber insurance industry is more established.

Conclusion

We are committed to constructive engagement in the regulatory process and welcome the opportunity to work with the Department on this Proposal and other important regulatory efforts.

Thank you for considering FSI's comments. Should you have any questions, please contact me at (202) 803-6061.

Respectfully submitted,



David T. Bellaire, Esq.
Executive Vice President & General Counsel