COMMONWEALTH *financial network*®

VIA ELECTRONIC MAIL

May 12, 2008

Nancy M. Morris
Secretary
Securities and Exchange Commission
F Street NE
Washington, DC 20549-1090

RE: File Number S7-06-08 – Regulation S-P

Dear Ms. Morris:

The Securities and Exchange Commission (Commission) has proposed amendments to Regulation S-P[1] to enhance consumer protection, while promoting investor choice and account portability.

Founded in 1979, Commonwealth Financial Network (Commonwealth) is the nation's second-largest, privately owned independent broker/dealer, with offices in Waltham, Massachusetts, and San Diego, California. The firm supports more than 1,200 independent financial advisors nationwide and makes available a comprehensive array of non-proprietary financial products and services. As an independent contractor broker-dealer, our financial advisors provide investment and financial planning services primarily to individual retail clients.

Commonwealth supports the Commission's efforts and appreciates the opportunity to comment on the proposed amendments. The rule, as proposed however, fails to balance the interests of investor protection with the burdens and costs of implementing rigid, one size fits all, information security programs, the cost of which will ultimately be passed on to consumers. Furthermore, the amendments fail to take into account the wide-ranging business models of SEC registrants. A one size fits all approach is not the answer to protecting customer privacy.

Proposed Standards for Safeguarding Personal Information

The proposed amendments require firms to designate an employee to coordinate the information security program, identify in writing reasonable security risks, design and document policies and procedures to control identified risks, regularly test the effectiveness of the policies and procedures,

[1] *Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information*, Release Nos. 34-57427; IC-28178; IA 2712 (Mar. 4, 2008) (the "Release")

29 Sawyer Road
Waltham, MA 02453-3483
800.237.0081
781.736.0793 fax

110 West A Street, Suite 1800
San Diego, CA 92101-3706
877.347.1982
619.471.9701 fax

commonwealth.com

train staff, oversee service providers to ensure vendors have appropriate safeguards in place, and evaluate and adjust its information security program in response to testing.

The requirement to regularly test the effectiveness of the policies and procedures would be a significant burden to firms. The Commission however, fails to give any guidance on what they mean by "regularly test." Is it quarterly, bi-annually annually? Based on Commonwealth's experience, the estimated cost to hire an outside auditor or permanent employee to test the firm's information security program on an annual basis could easily exceed $100,000 a year.

Commonwealth proposes instead that the Commission incorporate the testing requirement as part of the testing already required by FINRA Rule 3012[2] and Investment Advisers Act Rule 206(4)-7[3]. Rather than subjecting firms to an additional testing requirement, testing the effectiveness of a firm's information security program should be an element of a firm's existing testing requirements.

Even more onerous is the requirement that firms oversee service providers to ensure they have appropriate safeguards in place. The proposed definition of a "service provider" is too broad, and as written, could include everything from technology providers to mutual fund companies to over-night shipping companies, including the U.S. Postal Service. The definition needs to be limited to those service providers "who are permitted access to personal information" and should exempt those service providers who are themselves already subject to Regulation S-P.

Even if the definition of service provider was narrowed to include only information service providers, the requirement to supervise vendors is impractical. Commonwealth, a medium-sized broker/dealer, has over 200 mission critical service providers under contract. Many of these service providers operate in industries in which SAS 70, SysTrust, and WebTrust reports are either not required, or are too costly for the service provider, small or large, to be reasonable. As an alternative, Commonwealth suggests a privacy certification that broker-dealers can use with vendors, analogous to Customer Identification Program certifications currently in place as a result of the USA PATRIOT Act.

Alternatively, Commonwealth recommends the standards be less prescriptive to provide a flexible framework in which different business models can operate. Each firm should be allowed to

---

[2] FINRA Rule 3012(a) (1) provides that members must "… test and verify that the member's supervisory procedures are reasonably designed with respect to the activities of the member and its registered representatives and associated persons, to achieve compliance with applicable securities laws and regulations, and with applicable NASD rules and (B) create additional or amend supervisory procedures where the need is identified by such testing and verification."

[3] Investment Advisers Act Rule 206(4)-7(b) requires investment advisers to "review, no less frequently than annually, the adequacy of the policies and procedures established pursuant to this section and the effectiveness of their implementation."

determine what standards are appropriate using a risk-based, principles approach based on its size, resources, and business model. A "one size fits all" approach is inappropriate as it will overburden firms without furthering the goal of investor protection.

Regarding the proposal that firms implement multifactor authentication or layered security for higher risk transactions, such as those that involve access to customer information or the movement of funds, this requirement is too inflexible. This suggestion fails to address the different contexts in which this information is accessed. The risks associated with clients accessing a firm's website versus representatives accessing systems in local branch offices or home office employees at their computer terminals are all materially different. Multi-layer security is much more appropriate for a public facing website than it would be for a mainframe system accessible only within the firm's firewall.

The Commission also requested comments on the definition of "Substantial harm or inconvenience", and while the definition is helpful, the Commission should further define or provide guidance on the phrases "trivial financial loss" and "expenditure of effort or loss of time." These terms are unclear; whether a loss is considered trivial—or how much effort or time lost is considered no longer trivial—is entirely subjective. The only guidance given is that the need to change account numbers or passwords is not substantial harm.

Data Security Breach Responses

The proposed rule requires procedures for assessing, investigating, and responding to privacy incidents. Procedures would have to include notification to affected individuals under certain circumstances, as well as notification to the Commission or designated examining authority. The rule changes would require notification if an individual has or is likely to suffer substantial harm or inconvenience, or if an unauthorized person has intentionally obtained access to or used sensitive personal information.

Commonwealth supports client notification wholeheartedly whenever there is a significant risk of unauthorized access that could lead to substantial harm or inconvenience or identity theft. The new requirement to notify the Commission or an SRO, however, could be overly burdensome without specific guidelines and de minimis exemptions. Furthermore, the final rule should include qualitative and quantitative thresholds to trigger notification to the Commission.

With regard to qualitative standards, the Commission should only require notification if there is a breach that involves a systemic breakdown of a firm's controls, for example, if a firm's computer network is breached or subjected to cybercrime. It is impractical for firms to complete Form SP-30 every time a client's account is accessed because the client's home computer falls victim to spyware

or a virus. Isolated privacy incidents are better addressed by client notification and education. In addition, there should be an exception for a breach that involves data that is encrypted or otherwise unreadable.

The proposed rule should also include a quantitative threshold before requiring firms to complete Form SP-30. If, for example, there was a compromise or unauthorized access of the sensitive personal information of numerous accounts, this would be an indicator of a potentially systemic breach requiring Commission notification. Alternatively, if there is an incident involving only a limited number of clients (Commonwealth proposes a de minimis exemption for incidents involving 50 or less households), then Commission notification would be unnecessary.

In addition, the proposed rule requires notification "… as soon as possible after you become aware of any incident of unauthorized access to or use of personal information…"[4] Commonwealth requests clarification or guidance on the definition of "as soon as possible." The final rule should provide a clearer standard that allows firms to investigate potential breaches to determine whether client or Commission notification is necessary.

Proposed Form SP-30 is relatively straightforward and easy to understand, however, question number 10 appears to impose an additional duty on firms to review policies and procedures in response to every security incident. This duty is unnecessary and burdensome in light of the proposed requirement to regularly test or otherwise monitor the effectiveness of the firm's security safeguards[5].

An additional concern with Form SP-30 is whether form submissions will receive confidential treatment or be subject to FOIA. Clearly, public interest dictates that all information submitted on Form SP-30 should remain confidential. Furthermore, firms should benefit from absolute immunity from defamation claims based on statements made in Form SP-30.

Exception for Limited Information Disclosure When Personnel Leave Their Firms

The proposed exception is a step in the right direction, but there are significant shortcomings relating to the independent broker/dealer model. The proposed exception fails to take into account the realities of the independent model where advisors develop long-term relationships with their clients that transcend the advisor's affiliation with any particular broker-dealer. In fact, unlike the wirehouse model, advisors seldom "leave" their office location when changing broker-dealers. Rather, all that changes is the signage on the front door. In the independent contractor model, the

[4] See proposed paragraph (a)(4)(v) of Section 30.
[5] See proposed paragraph (a)(3)(iv) of Section 30.

advisor maintains the relationship with their client, and their client often doesn't even recognize the name of the broker-dealer. Additionally, independent contractor advisors do not take any client information with them when they switch firms – they already possess it. Investors expect their advisor to have all of their personal information in their records, not just the client's name, address, and phone number. To promote investor choice and account portability, the Commission should revise the proposed exception as discussed further below.

The proposed rule imposes a requirement that broker-dealers supervise the information transfer. While it would be reasonable for firms with departing representatives to provide guidance to terminating representatives, it would be nearly impossible to supervise the actual transfer of information to the new firm. This requirement is impractical and unworkable. The duty of broker-dealers should be limited to putting the departing representative on notice of the firm's privacy policy as well as state and federal privacy laws.

The proposed exception also gives control over the information transfer to the delivering firm above and beyond any employment, non-compete, or non-solicitation agreements, and stymies competition. The delivering firm could effectively prohibit a departing representative from taking what is essentially public information irrespective of whether the advisor signed an agreement.

Firms are free to have non-solicitation or other agreements to prevent advisors from taking clients, but absent such agreements, the firm from which the advisor terminates their registration should not be able to prevent departing representatives from taking public information.

In the independent broker-dealer model, advisors in registered branch offices are often the custodians of client information. Independent advisors generally own or lease their own office space and the broker-dealer does not have a right to physically access the branch once an advisor terminates their registration. Requiring the former broker-dealer ensure the destruction of confidential information is impractical and unenforceable.

Commonwealth proposes that independent contractor advisors be allowed to retain information they received directly from their clients and possess locally in their branch, provided they do not upload, handover, or otherwise grant access to the information to a new broker-dealer until the client becomes a customer of the new broker-dealer by signing a new account agreement and receiving a copy of the new broker-dealer's privacy policy.

Conclusion

Commonwealth believes the proposed rule makes significant strides in the direction of investor protection and consumer choice. The proposed rule should, however, be revised to balance these

laudable goals with the realities of the many different business models in the financial services industry, including independent contractor broker-dealers. If the proposed rule is not revised, the extraordinary costs and burdens of implementing the rule as written will ultimately be passed on to consumers. More importantly, however, many of the rule's proposals are impractical and will be difficult if not impossible to enforce.

Commonwealth appreciates the opportunity to comment on the proposed rule and is grateful for the Commission's time and consideration. If you have any questions regarding our comments or concerns, please contact me at 781.529.9107.

Sincerely,

COMMONWEALTH FINANCIAL NETWORK

/s/ Brendan Daly

Brendan Daly
Compliance Manager