FINRA
Financial Industry Regulatory Authority

Marcia E. Asquith
Senior Vice President and
Corporate Secretary

Phone: 202-728-8831

May 12, 2008

Via Electronic Transmission

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

Re: Comment Letter on File No. S7-06-08; Release Nos. 34-57427; IC-28178; IA-2712 – Notice of Filing of Proposed Rule Change to Amend Regulation S-P

Dear Ms. Morris:

FINRA staff[1] appreciates this opportunity to comment on the Securities and Exchange Commission's ("SEC" or "Commission") proposed rule change to amend Regulation S-P regarding the need to safeguard the privacy of consumer financial and personal information, as published in the *Federal Register* on March 13, 2008 (the "Proposal").[2] The Proposal, inter alia, sets forth more specific requirements for safeguarding information and responding to information security breaches and broadens the scope of the information covered by Regulation S-P's safeguarding and disposal provisions.

FINRA shares the Commission's concerns about the increasing instances of account intrusion and the importance of protecting customer information.[3] The obligation to protect customer information arises, in large part, from the broad

---

[1] The comments provided in this letter are solely those of FINRA staff; they have not been reviewed or endorsed by the FINRA Board of Governors. For ease of reference, this letter may use "we," "FINRA," and "FINRA staff" interchangeably, but these terms all refer only to FINRA staff.

[2] *See* Release Nos. 34-57427; IC-28178; IA-2712, 73 FR 13692 (Mar. 13, 2008) (File No. S7-06-08).

[3] FINRA has already taken broad-based measures to address the types of problems associated with compromised customer information and on-line brokerage accounts. For example, in addition to numerous publications aimed at educating investors about the dangers of account intrusion, in *Notice to Members 05-49*, FINRA reminded broker-dealers of their obligation to protect customer information.

1735 K Street, NW
Washington, DC
20006-1506

t 202 728 8000
www.finra.org

requirements of SEC Rule 30 under Regulation S-P. Pursuant to that rule, a broker-dealer has to create and maintain policies and procedures that are reasonably designed to, among other things, "insure the security and confidentiality of customer records and information, protect against any anticipated threats or hazards to the security or integrity of customer records and information, and protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer."

Despite the breadth of these requirements, safeguarding customer information has proven troublesome for a variety of reasons. As the Commission is aware, account intrusions can occur in numerous ways and can result from a person accessing a customer's account either directly through a breach in the firm's system (e.g., by gaining unauthorized access to the firm's network) or as a result of actions by the customer (e.g., by deceiving a customer into providing account-sensitive information).[4] FINRA supports the Commission's efforts to provide greater clarity and uniformity to this area through its proposal to use risk-based standards similar to those identified by the federal banking regulators that make up the Federal Financial Institutions Examination Council (the "FFIEC") in their guidance concerning customer authentication in an on-line environment.[5] FINRA supports the Commission's proposed approach that is technology neutral, and FINRA recommends that the Commission adopt requirements that generally mirror the FFIEC's guidance regarding "multifactor" authentication for high-risk transactions.

FINRA also believes that the SEC's proposed amendments to Regulation S-P will have the beneficial effect of bringing greater clarity to the full breadth of the application of Regulation S-P and Rule 30's requirements thereunder. Specifically, FINRA believes

---

[4] The Proposal specifically identifies the use of "keylogger" programs and "'phishing' attacks"; however, there are multiple ways in which investors can inadvertently provide access to their accounts. *See* Proposal at n.17.

[5] *See Authentication in an Internet Banking Environment* (July 27, 2006). The FFIEC is composed of the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision. According to the FFIEC's guidance, financial institutions should "conduct risk-based assessments, evaluate customer awareness programs, and develop security measures to reliably authenticate customers remotely accessing their Internet-based financial services." The guidance notes that effective customer authentication "is necessary for compliance with requirements to safeguard customer information, to prevent money laundering and terrorist financing, to reduce fraud, to inhibit identify theft, and to promote the legal enforceability of [a financial institution's] electronic agreements and transactions." Although the guidance stops short of endorsing particular technologies, it states several times that "[t]he agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties." These same concerns are obviously present in the securities industry as well.

that Rule 30 requires broker-dealers to be vigilant in protecting customer information even when their customers (and not simply the broker-dealers) inadvertently provide account information to unauthorized persons. As cited above, Rule 30 currently requires that firms protect against "anticipated threats." The facilitation of an account takeover by an investor who fails to take adequate precautions is certainly a threat that firms should anticipate occurring, and firms must take reasonable steps to prevent the misuse of any information obtained in such a manner. Indeed, as the Commission observed, some firms have taken steps to prevent this type of account intrusion by offering investors the use of pass-word generating tokens for on-line brokerage accounts.[6] In the interest of further clarity and the avoidance of any doubt, however, FINRA requests that the Commission reaffirm FINRA's interpretation of Rule 30 in this regard.

FINRA supports the proposed requirement that broker-dealers inform their designated examining authority, whether FINRA or another self-regulatory organization ("SRO"), whenever a significant event has occurred.[7] FINRA believes this information could further its ability to identify those member firms whose policies and procedures may be weak or otherwise deficient and may, in some instances, further assist in identifying the source of unusual trading activity. The Proposal requests comment on whether it would be easier or more cost-effective for firms if the rule specified the information they are required to provide rather than provide a form. For purposes of submission to an SRO, FINRA supports deference to the SRO to specify both the manner in which the information is provided and the mode in which it is delivered. In this way, the SRO will have the ability to determine a manner and mode of delivery of the information that allows for both the efficient reporting by its member firms and the receipt by the SRO in a manner that is effective for the deployment of the SRO's programmatic operations around such information.

It is important to point out, however, that an SRO's investigative and enforcement reach would remain limited in the context of account intrusions even if it receives information about significant events. An SRO's jurisdiction covers only the SRO's member firms (and their associated persons), and this limitation restricts an SRO's ability to deal with an account intrusion beyond investigating the member firm and its associated persons for potential rule violations. Only in rare instances will an SRO be able to deal with an account intrusion on a comprehensive basis. Indeed, even if an account were intruded as part of a market manipulation effort, the SRO's jurisdiction would extend only to the member firm holding the account unless the individuals engaging in the manipulation were themselves associated persons of a member firm. FINRA's understanding is that perpetrators of account intrusions are infrequently associated with broker-dealers and are often located abroad. As such, FINRA respectfully suggests that the Commission consider requiring that broker-dealers also report significant events to

---

6 *See* Proposal at n.20.

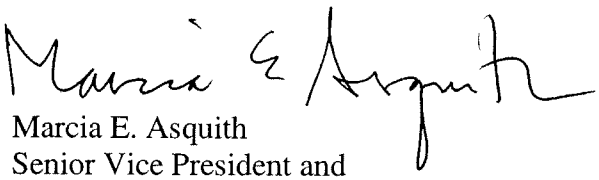
7 *See* Proposal at n.54.

the SEC or other federal agency with broader jurisdiction and subpoena powers so that a more comprehensive response to any intrusion could be undertaken if warranted. Such an approach would allow FINRA to address the significant event from a member firm compliance standpoint and the Commission or other federal agency to address it from a broader law enforcement perspective.

In all cases, FINRA believes that preventive (rather than after-the-fact) measures taken by member firms are the key to successfully protecting customer information. Chasing perpetrators and funds after a customer account has already been compromised, while important, is neither the most efficient nor the most effective method of protecting customer information or assets.[8] Preventing account intrusions before they begin through the use of reasonable policies and procedures offers the best chance of securing confidential customer information and, perhaps even more crucial, thwarting market manipulation schemes that rely on account intrusions.

For the reasons set forth above, FINRA supports the Proposal, with the noted concern about the requirements for broker-dealers to report significant events only to their designated examining authority. Please contact James S. Wrona, Associate Vice President and Associate General Counsel, at (202) 728-8270, or Brant K. Brown, Associate General Counsel, at (202) 728-6927, if you would like to discuss our concerns or have any further questions.

Sincerely,



Marcia E. Asquith
Senior Vice President and
Corporate Secretary

---

[8] Although broker-dealers generally have reimbursed customers who are victims of account intrusion, such relief does not, standing alone, alleviate other problems associated with account intrusion. For example, as the Commission noted in the Proposal, there are increasing instances involving the takeover of on-line brokerage accounts as part of a wider effort to engage in market manipulation, which can injure not only the customer whose account was compromised, but all of those investors who suffer because of the manipulation itself. In addition, once a customer's personal information has been compromised, that information may be used to access other of the customer's existing accounts or engage in other forms of identity theft. Consequently, protecting against unauthorized access to customer information and accounts in the first instance is equally, if not more, important than providing reimbursement after an account has been compromised.