



7705 Cresheim Road
Philadelphia, PA 19118
Actuary@icecoldmail.com
December 18, 2006

Nancy Morris
Secretary
U.S. Securities and Exchange Commission
100 F St., NE
Washington, DC 20549-9303

Via E-mail

***Re: File No. S7-10-05, Release No. 34-52926
Internet Availability of Proxy Materials***

Dear Ms. Morris,

I am writing in regard to the recent proposals for Internet Availability of Proxy Materials. My understanding is that the Commission has recently taken action and is not necessarily soliciting additional comments on the new rules. However, my comments may be helpful to the Commission.

My review of the proposals and comments indicates that a critical area of concern may have been overlooked – potential identity theft, “phishing,” and other Internet security issues.

I recently entered retired status and found that I had time to review the proxy materials that I received in the mail. Before my retirement, I tended to ignore those mailings. Analysis of the recently received materials indicates that I have received several proxies for companies for which I do not and have not owned shares. It has turned out to be difficult to determine why I am receiving these proxies. Furthermore, it seems that I could return the proxies and my votes would be recorded, even though I am not actually a shareholder.

Today’s Internet users are commonly subjected to all sorts of deliberately deceptive activity. This activity includes emails sent by unknown parties to thousands of randomly chosen recipients; the scammer hopes that a small percentage of recipients will “bite.” Some emails direct the recipient to a web site that appears to be for a legitimate company, but is actually controlled by a scammer. This scam, known as “phishing,” allows the scammer to obtain the user’s identifying information.

I noticed that the rule proposals do not consider any security issues. Perhaps the thought is that individual companies will adopt defensive measures. However, ineffective measures jeopardize both the company and the shareholder. In fact, the shareholder’s potential losses could far exceed the value of the stock. Therefore, I submit the following suggestions for your consideration:

1. Every electronic communication should clearly indicate the source of the communication and provide contact information by which the recipient may verify the validity of the communication. Any website identified in the email should be secure and clearly identified as owned by the company. Furthermore, it should be required

that the e-mail specifically state that the recipient should only visit web sites that are secure and clearly owned by the company.

2. Every electronic communication should identify the data source that has been used to determine that the recipient is a shareholder. For example, the data source might be the company's records, the registrar's records, or a stockbroker's records. This would help to validate that the email is legitimate. For example, if the email states that the data source is ABC Brokerage and the recipient does not have an account at that brokerage, suspicions would be raised.
3. In order to combat "phishing," there could be a requirement that the shareholder register ID and security codes in advance of receiving an electronic proxy.
4. A variation of the above suggestion could apply to beneficial owners. Beneficial owners could efficiently validate the company web site by connecting through their broker's web site. For example, if I signed on to ABC Brokerage web site, I could find a link that would take me to a secure web site for XYZ Company that would allow me to get proxy material or submit my proxy vote.
5. A related area of concern is that fraudulent votes could be submitted electronically. (Although the rules don't seem to deal with voting, I noticed that Commissioner Nazareth's recent speech expressed the thought that the new rules might lead more shareholders to vote online.) For example, a criminal who learns the address of the company site for voting could submit numerous attempts to "crack" the voting procedures. Although an unusually large number of votes would likely be detected, the voting fraud could easily disrupt the election, deprive legitimate shareholders of their rights, and interfere with corporate governance. Advanced attacks might affect the election results, without detection. Internet vendors have developed techniques to prevent automated computer attacks and those techniques should be required for electronic proxy voting. However, it is difficult to anticipate the future methodologies of criminals and companies need to be vigilant. It seems to me that a systemic deficiency in a company's electronic proxy voting might be the type of weakness required to be identified by Sarbanes-Oxley.
6. It is possible that security measures could be counter-productive to the overall goal of efficiency. To the extent that individual shareholders are required to register with each company, there could be a perceived burden on shareholders with many holdings. The need for multiple ID's and passwords is a well-known annoyance and security problem for Internet users. However, that concern could be mitigated by allowing shareholders to access secure voting web sites after they have logged into their broker's web site or into a centralized, secure web site serving multiple companies.

My suggested security methodologies are submitted as examples of possible approaches. I am certain that experts in the various companies and financial institutions would be able to provide effective defenses. However, I strongly recommend that companies be required to consider these issues.

Background of the Commenter

I am proud to note that I started my business career in 1967 at the Division of Investment Management of the SEC. Since then, I have worked as an actuary for a life insurance company and two actuarial consulting firms, recently retiring as a Principal of Towers Perrin.

Until recently, I had been on the Board of Governors of the Society of Actuaries and edited the Society's newsletter for actuaries interested in investments. During the course of my career, I have written numerous articles on asset allocation and selection of discount rates for pension plans.

Of course, this letter reflects my own views.

Sincerely,

A handwritten signature in cursive script that reads "Richard Q. Wendt". The signature is written in black ink on a light-colored background.

Richard Q. Wendt, FSA, CFA