The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

SPEECH

December 11, 2014

Welcoming Remarks, 2014 ICI Cybersecurity Forum

Welcoming Remarks
2014 ICI Cybersecurity Forum

Paul Schott Stevens
President and CEO
Investment Company Institute

December 11, 2014
Washington, DC

Good morning, and welcome to ICI's first Cybersecurity Forum.

With diverse backgrounds but a single common interest in protecting our funds and shareholders, we gather today to share our insights on matters of utmost importance. Indeed, information security is a question of enormous and understandable concern to fund executives, boards, regulators, and investors alike. So, thank you very much for joining us today. And thank you in advance for the insights and energy you will contribute to our discussions.

As I said, this is ICI's first Cybersecurity Forum—but it will not be the last. Rather, think of this as an ongoing discourse. We call this event a forum for good reason. In Latin, the term forum means, literally, what is out of doors—a place set apart, like the famous Forum Romanum, for public assembly and for discussion of the most important issues of the day.

In their time, the Romans were concerned with securing the frontiers of their empire against successive invasions by barbarian peoples. In our time, the challenge is securing our cyberspace against latter-day Goths and Vandals.

We have a rich, engaging program in store for you. I claim no technical expertise here, but before we begin I would like to share a few thoughts about information security's fundamental place in our industry…the urgency of shoring it up…and the collective responsibility we have for doing so.

First, why is information security of such fundamental importance?

Because it goes to the heart of our duty to shareholders. As fiduciaries, we of course must

be scrupulously loyal to their interests. But we also must act with due care in all the activities we undertake on their behalf. In this context, our duty of care means, for example, being diligent about protecting shareholders' personal data and market-sensitive information from unauthorized disclosure, and also about maintaining the integrity of the books and records that document our work.

Ours is an industry built on the trust and confidence of millions of shareholders. We have an exceptionally strong shared interest in maintaining that trust, and in doing our level best to address anything that could seriously undermine it. Cyber threats fall in just that category.

My second point centers on the urgency of our information security challenge.

I say "our" advisedly. This is certainly not a challenge unique to the fund industry, or to financial services, or even to the private sector. It is a daunting challenge for our nation at large, literally implicating the security of us all. And it cannot be taken too seriously—or dealt with soon enough. Indeed, the challenge isn't in the offing—it's not something we can prepare for incrementally. It's here today—frankly, it was here yesterday—and it calls for an energetic, comprehensive national response that takes that into account.

I do not underestimate the difficulty of the task. Our industry has been defending against cyber threats for decades now. Indeed, ICI's Technology Committee has made cyber security an essential part of its agenda since the Committee was formed in 1998. Nonetheless, the threats grow more numerous and sophisticated by the day.

I also know that there is no such thing here as a separate peace. The risks are common to all; so too must be our efforts to reduce the risks.

That is why I believe we have a collective responsibility to enhance our industry's information security.

Information security is far more than a concern just for IT departments, or for large, prominent fund families. It is a concern that touches every business unit of every fund complex—as well as a host of firms that provide services of every kind to our industry. And everyone in and around our industry has a role to play in addressing it.

Here is where I think ICI can play an essential role. We can help ensure that the large set of issues around cyber security have the priority for the fund industry that they deserve. We can help leaders in information security share their knowledge within and across firms. We can convene meetings of experts—like today's Forum—for a structured dialogue on cutting-edge issues and valuable personal interactions among peers. Working with our members, we can give strong support to sound public policies in the U.S. and elsewhere that are designed to enhance cyber security.

Our new Chief Information Security Officer Advisory Committee—formed by our Board of Governors earlier this year—is leading the way on this front. Though its focus will be on information security, the Advisory Committee also aims to share its work beyond the security community—to people working in compliance, risk, operations, and elsewhere—and with all ICI members, not just those who attend the committee meetings.

To that end, the committee is developing a range of information-sharing initiatives. Three stand out for me today:

- First, the committee has drawn up a new cybersecurity resource page, which will

debut before the New Year and be accessible from ICI's website. Among other material, the page will include a detailed set of questions that fund management, boards of directors, and information security practitioners should consider when evaluating their own information security program or that of a third-party service provider. The questions will help firms better secure their networks and data, and identify threats and risks with greater accuracy.

- Second, the committee is developing an anonymous survey—to be conducted next year—that will paint a more detailed picture of how ICI members are building and maintaining their information security programs. Through the survey results, the committee will be able to get a better sense of how practices are developing—and as a result, a better sense of where to direct its efforts going forward. The survey is designed to be repeatable, so that the committee can see how the industry is progressing and how defensive measures are evolving.
- Third, the committee will be collaborating with the Financial Services Information Sharing and Analysis Center, or FS-ISAC, to produce threat intelligence output geared specifically to the asset management sector. Since 1999, the FS-ISAC has collected intelligence on threats to the financial services industry at large, and delivered it to people who subscribe to their service. Now, we are working with them to create a product that addresses our needs more directly. Discussions for this project will begin in the very near future.

Be assured that ICI will continue to accord a very high priority to cyber security. We owe our shareholders nothing less, and we appreciate your support and assistance in this endeavor.

I encourage you to participate actively in this Forum. Engage in healthy debate...ask pointed questions...disagree with vigor—and courtesy...state your case confidently...entertain constructive criticism...share an unconventional perspective...acknowledge errors gracefully...and consider theories you've long rejected.

Every idea is born in response to a problem. Yours might just grow into a long-term solution for an entire industry—and the many millions of shareholders who entrust their savings to it.

Thank you kindly for your time. I look forward to a fascinating discussion throughout the day.
