



FINRA/SIFMA Cybersecurity Conference
New York, NY
February 4, 2015

Opening Remarks as prepared for delivery
Kenneth E. Bentsen, Jr.
President and CEO, SIFMA

Good morning. I'm Ken Bentsen, president & CEO of SIFMA. Thank you for taking time out of your busy schedules to join us for this FINRA/SIFMA joint conference on the critically important issue of cybersecurity. The idea for this conference came out of the many conversations we have had with our friends at FINRA on how best to ensure industry and market preparedness. I want to thank Steve Randich, Susan Axelrod, and their colleagues at FINRA for their continued partnership in the effort to mitigate cyber threats.

This joint conference underscores the fact that cybersecurity must be a collaborative effort between the industry, regulators and policymakers. Cyber attacks are increasingly a major threat to national security and the U.S. financial system, and we are all working hand in hand to protect the integrity of the markets and the millions of Americans who use financial services every day.

For our part, the financial services industry has been dedicating tremendous resources to protect clients and protect against the risks associated with cyber attacks. Two years ago, SIFMA's effort was kicked into high gear when we held our Quantum Dawn 2 exercise, which simulated a systemic attack on the equity markets and enabled our member firms, exchanges and regulators to come together and run through their response procedures. We took those lessons learned and developed protocols around information sharing and response, and continue to refine those over time.

Following on the Quantum Dawn 2 work, we have undertaken an enhanced effort, led by our board, and in close coordination with other industry trade groups and our regulators, to develop and promote policies and practices that can help mitigate these threats.

We are promoting use of the Cybersecurity Framework issued by the National Institute of Standards and Technology, or NIST, and working with our members to develop standards tailored to broker-dealers and asset managers. In addition, we are working with critical infrastructure and other market participants to design processes that will allow firms and their vendors to measure and attest to their use of the NIST Cybersecurity Framework. We are planning additional simulation exercises that will continue to strengthen our response protocols, and we have developed best practices for managing insider threats

Washington | New York

1101 New York Avenue, NW | 8th Floor | Washington, DC 20005-4269 | P: 202.962.7300 | F: 202.962.7305
www.sifma.org

and third party risk, and specific cybersecurity guidance for small firms. As the saying goes, we are only as strong as our weakest link, and our board has directed us to develop standards that apply across the entire industry.

In addition to these resources, we have also published our recommendations for effective cyber security regulatory guidance. These principles provide regulators with SIFMA members' insight on productive ways to harmonize and create effective guidance that will improve cybersecurity protections. We believe harmonized regulation developed via a collaborative approach will foster innovation and strengthen the efforts of the industry to protect financial operations and most importantly our clients.

The most effective way to address these threats is through a robust partnership between the private sector and government. In fact, the most important takeaway we've learned through all of our simulations and work with our members and government partners is that information sharing is essential to an effective cybersecurity defense.

We are working with our US regulators, like FINRA, and other key government entities at the highest levels to ensure the most complete level of communication and coordination between our industry, other market participants and the official sector. Just yesterday, we saw FINRA and the SEC publish reports intended to help in the collective cyber defense effort, and we will review that information closely with our members and look forward to learning more about FINRA's work over the course of today's program. We commend FINRA for their focus on this vitally important issue, and believe their report on cybersecurity practices is a comprehensive, thoughtful document that makes a number of important points on cybersecurity that will point the industry in the right direction in terms of managing an effective defense and response program. We share their goal of promoting cybersecurity practices that are grounded in risk management and informed by specific threat information, and agree that a one size fits all approach is not the most effective way to manage these threats.

While cyber security is a national priority for both the industry and the government, it is also a global issue.

Through our Global Financial Markets Association, we are engaging global regulatory coordinating bodies including IOSCO, the Basel Committee for Banking Supervision and the Financial Stability Board. Just as we must have seamless communication and coordination between the industry and the official sector in the U.S., we also need to work across borders in the same fashion.

There is also an opportunity for Congressional action to strengthen our nation's cyber defenses by codifying liability protections that promote enhanced information sharing

between the industry and government, while balancing the need for important privacy protections for individuals. We strongly encourage Congress to make cybersecurity a priority and pass legislation that facilitates improved information sharing and enables the industry and government agencies to work together in the most effective way possible.

In closing, I'd like to note that SIFMA is committed to doing our part to enhance information sharing by encouraging all of our members to join the Financial Services Information Sharing and Analysis Center, or FS-ISAC. The FS-ISAC is a vitally important industry forum for collaboration on critical security threats facing the global financial services sector. It enables firms to share relevant threat information, and when attacks occur, members of the FS-ISAC receive timely notification and authoritative information specifically designed to help protect critical systems and assets.

SIFMA has set a goal to have 100% of our members join FS-ISAC and to jump start that process, we have underwritten FS-ISAC membership for over 180 of our smaller member firms. SIFMA and its members are also joining with industry partners to underwrite enhancements to FS-ISAC's and DTCC's information sharing processes. I encourage every broker-dealer, whether a SIFMA member or not, to join FS-ISAC.

I'd like to take this opportunity to sincerely thank all of our speakers for making time to share their insight with us today. These forums where the industry, regulators and solution providers can come together are very important as we all work towards our shared goal of protecting investors and promoting a resilient marketplace.

I'd also like to recognize all of our exhibitors – we appreciate their participation in today's event and I encourage you to spend some time with them to learn more about the solutions they can provide. Our exhibitors include Decoded Technologies, Delta Risk LLC, Entreda, FS-ISAC, IBM, Nexgate and ObserveIT.

Thank you again to our partners at FINRA and to all of you for joining us today. I hope you enjoy the robust program we have planned.