Akin®

Administration and SIFMA Announce New Steps to Make Financial Data More Secure

Oct 21, 2014

Reading Time : **1 min**

By: Francine E. Friedman, Matthew Thomas (Senior Public Policy Specialist)

In the announcement, made during a speech at the Consumer Financial Protection Bureau, President Obama also called on Congress to pass a national data breach law to provide "one, clear national standard" to dictate how businesses should react to data breaches. The White House also announced plans to hold a Cybersecurity and Consumer Protection summit, which will bring together security experts, industry leaders and consumer advocates to discuss how companies should deal with breaches, and the best options going forward.

Coinciding with this announcement, on October 20, 2014, the Securities Industry and Financial Markets Association (SIFMA) released a series of 10 principles that it said government should follow when issuing new cybersecurity regulations. SIFMA stated that, while a public-private partnership can be beneficial when responding to data breaches or other cyber incidents, information sharing should be "limited to cybersecurity purposes."

The ten principles provided from the group are articulated under the following headings:

- Principle 1: The U.S. Government Has a Significant Role and Responsibility in Protecting the Business Community
- Principle 2: Recognize the Value of Public–Private Collaboration in the Development of Agency Guidance
- Principle 3: Compliance with Cybersecurity Agency Guidance Must be Flexible, Scalable and Practical
- Principle 4: Financial Services Cybersecurity Guidance Should be Harmonized Across Agencies

- Principle 5: Agency Guidance Must Consider the Resources of the Firm
- Principle 6: Effective Cybersecurity Guidance is Risk-Based and Threat-Informed
- Principle 7: Financial Regulators Should Engage in Risk-Based, Value-Added Audits Instead of Checklist Reviews
- Principle 8: Crisis Response is an Essential Component to an Effective Cybersecurity Program
- Principle 9: Information Sharing is Foundational to Protection, Must Be Limited to Cybersecurity Purposes, and Must Respect Firms' Confidences
- Principle 10: The Management of Cybersecurity at Critical

Categories

Cybersecurity, Privacy & Data Protection