U.S. DEPARTMENT OF THE TREASURY

Press Center

Remarks of Assistant Secretary for Financial Institutions Cyrus Amir-Mokri at the 2013 Securities Industry and Financial Markets Association (SIFMA) Operations Conference

4/29/2013

As prepared for delivery

BOCA RATON, FL - Good morning. Thank you for inviting me again to the SIFMA Operations Conference.

You may recall that, last year, I commented broadly on the impact of technology on financial services with a focus on our efforts at Treasury to better understand and to work on these issues. I offered some more specific thoughts on the impact of technology on our work on financial stability and consumer policy.

Today, I would like to update you briefly on our continuing efforts in these areas. But my emphasis today will be efforts to preserve and enhance the resiliency of the technological infrastructure of the financial services sector, particularly in areas such as cyber-security. Last year, the emphasis of my remarks was on the creative potential of technology, and its promise to better our lives, to inform our decisions, and to enrich our personal experiences. This year, I will shift my emphasis to urging you to focus on technology's potential for disruption and destruction. We have had important recent reminders that our financial institutions and markets are vulnerable to malicious cyber-attacks and operational failures. Working to prevent the realization of such threats and to be prepared to manage, mitigate, and recover from any harm that might occur should be a top priority for all of us.

Technology and Consumer Policy

Last year, I spoke to you briefly about our work on using data to enhance consumers' financial capability. We continue to focus on "smart disclosure," which broadly consists of releasing data in machine readable and clear, comprehensible format to allow better handling of disclosed data so that retail and institutional consumers can more easily use that data to inform their decisions in the marketplace.

Since last year, we have launched the Finance Data Initiative. We recognize that large datasets are important to entrepreneurs, businesses, and other organizations because of the potential that the productive use of large datasets has for economic growth and consumer benefits. We also recognize that the federal government is a significant repository of important data. Accordingly, we have launched the Finance Data Directory, which is a one-stop online platform for innovators to access over fifty, publicly available federal data sets.

To further our policy work in this area, we convened entrepreneurs, consumer advocates, financial institutions, and government authorities at Treasury to discuss current and potential economic benefits and uses of data made publicly available by government. We heard about numerous ideas and current services that draw on data released by the agencies such as the SEC, the Department of Labor, and the CFPB to help investors analyze market information, individuals plan for retirement, credit card holders discover suspicious charges, and small businesses obtain working capital loans. These are only a few examples of innovations made possible by use of finance data sets. We will continue to work to enable this kind of data-driven innovation through the Finance Data Initiative. As we continue our work on access to finance data, however, we must be mindful of important privacy and security issues attendant to the release of datasets.

Last year, I also spoke about the promise of mobile and other technology to empower consumers. We have continued our work in these areas, too. Recognizing the promise of today's smart phone technology as a platform to allow entrepreneurs to develop apps that may help consumers make financial decisions, we sponsored a prize challenge that asked app-developers to submit designs focused on enhancing financial capability. The winners of the challenge were announced in September of last year. We will continue to encourage app-developers to create tools that help consumers improve their financial choices.

Second, this past November, we brought together consumer advocates, financial institutions, entrepreneurs, and regulators to discuss innovation and trends in the use of mobile and information technology in the payments and retail banking areas. The development of digital wallets might allow consumers to centralize their accounts and payments tools, and to gain access to financial services companies and products directly through their smart phones.

As we monitor these developments and encourage innovations that benefit consumers, we must also remain mindful of safety and soundness concerns and other potential risks to the financial system posed by the introduction of new technologies into the financial services architecture. We must pay attention to operational risk, from fraud to money laundering, and on protecting privacy and proprietary information.

Financial Stability and the Work of the OFR

Last year, I also discussed some of the important work of the Office of Financial Research (OFR), including improving the quality of financial data, research on financial stability, and developing tools to evaluate and monitor risks to the financial system.

In the area of data standards, there has been progress on creating a global Legal Entity Identifier, or LEI, to identify—precisely and uniquely—parties to financial transactions. The governing structure for the LEI system is in place, several entities around the world are issuing pre-LEIs that are designed to be compatible with the LEI code, and the OFR's Chief Counsel has been named Chair of the Regulatory Oversight Committee that is overseeing the LEI's launch and implementation. We expect the LEI to yield significant savings for the financial industry in collecting, cleaning, and aggregating data. The LEI system also promises to reduce the regulatory reporting burden, so that industry can use the same data for its internal business operations and risk management as it uses for reporting to regulators. I know that SIFMA has been a supporter of this project, and I thank the organization for its efforts.

Threats to the Technological Infrastructure of Our Financial Sector

I noted last year that the financial services sector has been at the forefront of developing highly advanced, resilient systems infrastructure. The results of this success can be witnessed in every corner of the financial system and, in fact, on practically every street corner. Large volumes of money are transacted daily between persons and institutions through electronic means, whether it is through retail payment networks or through the institutional payment and settlement systems. The dependence of the global financial system on a rapid and accurately functioning technological infrastructure cannot be overstated. We as consumers and market participants take the seamlessness of transactions and the accuracy of our books and records for granted because of what you have accomplished. The information technology personnel at financial institutions, utilities, markets, and government authorities should be commended for their work.

But we should not take this relative success as a given. I mentioned last year that the sheer pace of technological change requires constant vigilance with respect to systems breakdown and compromise. That vigilance must be heightened even further in a world where individual actors deliberately and routinely intend to cause harm.

What are the threats to the technological infrastructure of the financial services sector? I start with systems breakdowns and disruptions that are inadvertent. These are frequently caused by software glitches or the inability of a system to handle a type of command, either because the circumstances were unforeseen or because of some other programming defect. Examples of this kind of error include entry of erroneous or destabilizing orders into a trading system, or programming glitches that could make customer access or services temporarily unavailable.

Although the ultimate cause of these mishaps may be due to inadvertence, it does not mean that the consequences will be small. Sometimes, even the solvency of a firm could be threatened. At other times, as in the case of the Flash Crash of 2010, the entire trading system could be affected, reminding us again that our systems are highly interconnected and that problems in one area could be transmitted to others.

Another category of breakdowns or disruptions are ones that result from calculated, malicious actions. Here, we have broadly seen three types of attacks: (i) defacement of web-facing pages; (ii) disruption of access to and from the website through means such as distributed denial-of-service attacks (DDoS); and (iii) intrusion and entry into systems and databases. The consequences of these types of actions are different. A DDoS attack, on its own, generally may disrupt access to a public facing website, but it does not necessarily affect the functioning of core systems, nor does it result in theft of information. Intrusion or hacking into core systems and databases, by contrast, provides an opportunity for the intruder to steal, destroy, or corrupt information or core system functions.

The foregoing threats are all man-made. Another relevant threat is natural catastrophe. Earthquakes and hurricanes can also have a disruptive effect on our technical infrastructure, as we experienced a few months ago with superstorm Sandy. I will note that SIFMA took action to help markets re-open in the wake of that storm. As we prepare for the future, it is important for us all to continue to work on improving our preparedness, resilience, and continuity planning. Such preparation will help continuity and recovery from both man-made and natural disasters.

Efforts to Protect Our Technological Infrastructure

We at Treasury, and our colleagues at the financial regulatory agencies, are focused on these operational risk and security issues in a number of ways.

We are implementing the President's Executive Order entitled Improving Critical Infrastructure Cybersecurity, which was issued on February 12 of this year. The executive order was accompanied by the Presidential Policy Directive on Critical Infrastructure Security and Resilience, which updates our nation's policy from a primary focus on protecting critical infrastructure against terrorism to protecting, securing, and making the nation's critical infrastructure more resilient to all hazards, including natural catastrophes and cyber attacks.

The Executive order is designed to enhance the security and resilience of our critical infrastructure and "to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties." It adds that "[w]e can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards."

I urge you all to study this Executive order. I would highlight, however, that one underpinning of the Executive order is the timely sharing of important and relevant information with the private sector. Often, we have heard that government can do a better job of sharing information. As the Executive order indicates, we are committed to doing so.

The order directs the National Institute of Standards and Technology (NIST) to lead the development of a cybersecurity framework (Framework) to reduce cyber risks to critical infrastructure. In doing so, NIST will rely on existing international standards, practices, and procedures. In addition to consulting with sector-specific agencies such as Treasury, the Executive order contemplates public review and comment to inform the Framework.

Once the Framework is final, the Department of Homeland Security (DHS) will establish a voluntary program to support its adoption by owners and operators of critical infrastructure. Treasury and other sector-specific agencies will coordinate with sector coordinating councils to develop implementation guidance. Moreover, with DHS coordinating, the Departments of Treasury and Commerce are contributing to the establishment of a set of incentives designed to promote participation in the voluntary program.

As chair of the Financial and Banking Information Infrastructure Committee (FBIIC), we at Treasury continue to develop means to enhance information sharing between government agencies, and between government and the financial sector. Our inter-agency coordination spans not only financial regulators, but also homeland security, law enforcement, and intelligence agencies. In recent months, in collaboration with other government agencies and private sector organizations – which have included the Financial Services Sector Coordinating Council (FSSCC), the Financial Services Information Sharing and Analysis Center (FS-ISAC), the Financial Services Roundtable's BITS division, the American Bankers' Association, the Clearing House and SIFMA – we have coordinated and held briefings for the private sector on emerging and present information security threats. A few weeks ago, a group of chief executive officers and senior executives from financial institutions visited Treasury for a briefing on cyber-security issues with the participation of both the Secretary and the Deputy Secretary. Treasury also continues to be an avenue for financial institutions to request appropriate Federal technical assistance.

Elevation of the significance of operational risk and cyber-security as emerging threats to the financial system was noted just last week by the Financial Stability Oversight Council (FSOC) in its annual report. As the annual report notes, the FSOC has been monitoring security threats in cyberspace, including the DDoS attacks against financial services companies that began in the summer of 2012. The FSOC recommends that senior management remain engaged, stresses the importance of information sharing, and adds that financial regulators should review and update their examination policies and guidance on information security.

Individual financial regulatory agencies have been taking action. The Office of the Comptroller of the Currency, for example, has issued information security alerts concerning distributed denial-of-service attacks, together with regulatory guidance to assist in mitigating risks associated with the attacks. The Securities and Exchange Commission, moreover, has proposed a regulation on systems compliance and integrity (Regulation SCI).

The Role of the Financial Sector

We recognize that government alone cannot keep our financial system safe. The responsibility of protecting our financial sector rests also with the sector itself. We are aware that you are working hard and expending resources to provide security for your information systems. But here are a few thoughts that bear repeating.

First, it is critically important for the financial sector to develop robust mechanisms for sharing information among itself. You and your firms should be actively engaged on these issues with your relevant associations. The associations, moreover, should have well-developed protocols for timely, reliable dissemination to members of actionable information they receive from government. In addition, you and your associations may even consider establishing information clearinghouses that gather information about recent threats, indicate whether these threats led to incidents, and document the manner in which the threats or incidents were addressed or mitigated, and what their after-effects were.

Second, information dissemination is important not just between organizations and institutions, but also vertically within an organization. All organizations have to work continually on improving mechanisms for information flow between junior and senior levels. It is incumbent upon the financial sector to improve such communications. Senior managers should clearly articulate to their employees that systems integrity and cyber-security are priorities. Correspondingly, information technology personnel should promptly escalate to senior managers, particularly including CEOs, important information they receive from government, from the sector, or through their reviews of systems security.

Third, develop, adopt, and maintain best practices. In addition, share and test your ideas with your peers. Some fundamental actions you can take are the following. Check for vulnerabilities, particularly for potential avenues and techniques for intrusion from the outside such as SQL injections. Stress test your core systems. Educate your users on intrusion techniques such as spear-phishing. Build, protect and test backups, including backups of unstructured data. Isolate your core transaction systems with appropriate firewalls. Establish contingency plans to prioritize critical traffic and processing. This list is obviously not exhaustive. You should develop precautions, defenses, and testing as limited only by your creativity and expertise.

Finally, maintain and develop robust communications with your various government contacts. Treasury is the financial sector's sector-specific agency, a role which we take seriously. We can help facilitate communications between you and other federal agencies whose expertise may be helpful to your issues. But, while we can and will help, it is still important for you to maintain and improve your channels of communication with other relevant authorities and expert agencies, such as your regulators and law enforcement.

Conclusion

We at Treasury are excited about the still untapped potential of information technology to empower consumers, to strengthen our economy, and to enhance our tools for safeguarding financial stability. But just as we aim to reap the benefits of technology, we must remain cognizant of its risks. Given the potential consequences, we must continue to emphasize systems integrity and cyber-security as a top priority. Thank you.

###