STATEMENT OF

BITS PRESIDENT PAUL SMOCER
ON BEHALF OF THE FINANCIAL SERVICES ROUNDTABLE

BEFORE THE

SUBCOMMITTEE ON CAPITAL MARKETS AND
GOVERNMENT SPONSORED ENTITIES
OF
THE UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON FINANCIAL SERVICES

CYBER THREATS TO CAPITAL MARKETS AND CORPORATE ACCOUNTS

JUNE 1, 2012

TESTIMONY OF PAUL SMOCER, BITS PRESIDENT

Thank you Chairman Garrett, Ranking Member Waters, and Members of the Committee for the opportunity to testify before you today.

My name is Paul Smocer and I am president of BITS, the technology policy division of The Financial Services Roundtable. BITS addresses issues at the intersection of financial services, technology and public policy, on behalf of its one hundred member institutions, their millions of customers, and all of the stakeholders in the U.S. financial system.

First, I would like to recognize the Members for their focus on cybersecurity as illustrated by the House's recent Cyber Week and, more importantly, by its passage of legislation that will enhance public/private information sharing, augment funding for cybersecurity research and development, and provide for broader citizen awareness and education regarding cybersecurity. These bills address three key issues in our collective effort to secure cyberspace and fight cybercrime.

The financial services industry recognizes the serious and constantly evolving nature of cyber threats to its customers, its institutions, and the broader economic wellbeing of the United States. The industry and its institutions have historically had and continue to have a strong focus on this subject and we have been leaders in partnering with others to address the challenges.

Today, I will address cybersecurity efforts at both the institutional and industry levels, collaborations within and beyond the industry, and efforts underway to improve information sharing, and discuss how both industry and government can be supportive in protecting key economic infrastructures, such as capital markets, and in protecting customers.

At the individual institution level, every new or developing product is subject to a risk assessment that the institution uses to identify potential institutional and customer threats and risks as well as to identify mitigations to limit these risks. Likewise, when institutions consider new product delivery channels, they too are subject to an in-depth risk review. The risk management practices and processes institutions use to conduct such reviews and their general efficacy is also the subject of

reviews by numerous regulatory agencies that are part of the Federal Financial Institutions Examination Council.[1]

Individual institutions also bear a serious responsibility for understanding the cyber risks and controls of their key service providers. This is an important consideration as we consider cyber threats to both the capital markets and, to a more limited extent, commercial customers. In the context of capital markets, individual institutions often rely on external providers for many of the services that support this market such as clearings, settlements and accounting services. Institutions, both because of their innate risk management policies and regulatory expectations under the federal regulators' guidelines, regularly either examine the cyber and resiliency risks and controls of these providers or request the providers supply them with independently produced evaluations such as those produced under the American Institute of CPA's Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization. These reviews both help assure that the underlying infrastructure that supports capital market security remains intact by forcing providers of services to employ effective cybersecurity protections and assures those using the services that they will remain available. Interestingly, many of the providers of those services are, in fact, themselves, financial institutions. As both a service provider and a financial institution, those institutions are both internally focused and externally focused on cyber issues.

Institutions recognize, however, that in the battle over cybersecurity, no one institution can fight alone. Consequently, at the sector level, a number of collaborative efforts exist. Through associations such as BITS and others such as the Financial Services – Information Sharing and Analysis Center (FS-ISAC) and the Securities Industry and Financial Markets Association (SIFMA) represented today on this panel, member companies band together to identify collectively institutional and customer risks in emerging areas such as mobile financial services, cloud computing and social media usage, as well as identify and share information on new threats and threat methods. They develop best practices guidelines for the industry to improve cybersecurity and reduce fraud. In many cases, these associations band together and work with all of their members on key issues. Two recent examples of these efforts include the work led by the FS-ISAC to address fraud occurring against commercial accounts through the Account Take Over Task Force and the work of

[1] See FFIEC IT Examination Handbook "Risk Management of E-Banking Activities" at http://ithandbook.ffiec.gov/it-booklets/e-banking/risk-management-of-e-banking-activities.aspx

the American Bankers Association and BITS toward building a more secure Internet environment in which to conduct financial services.

The largest of these industry collaborations is perhaps the sector's Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC). This group consists of over 20 financial trade associations, ten of the largest US-based financial institutions (many of whom are integral to providing services within the capital markets infrastructure) and ten key participants operating in the financial infrastructure such as the Depository Trust and Clearing Corporation (DTCC). Through the Council, these organizations come together to focus on key policy areas, threat and vulnerability, research and development and resiliency. One current focus of the group is a pilot program underway between the Council and the DHS Science and Technology Directorate's Cyber Security Division to utilize available government agency data to enhance customer identity verification – an effort that would be helpful in protecting consumers.

In the spirit of public-private partnerships, this Council works closely with the public sector partner Financial and Banking Information Infrastructure Committee (FBIIC), which was chartered under the President's Working Group on Financial Markets, and is charged with improving coordination and communication among financial regulators, enhancing the resiliency of the financial sector, and promoting the public/private partnership. Chaired by the Treasury Department, this Committee includes sixteen government agencies with oversight for the entire financial sector including regulators within the capital markets. Working together, the Council and the Committee members focus on key cybersecurity issues affecting the industry and how to address them. This focus includes the critical question of the industry's ability to recover from an incident – whether cyber or physical – that might affect the availability of vital industry infrastructure. Under their leadership, the two groups have sponsored numerous industry-wide resiliency exercises. The latest of these, called "Quantum Dawn," had as one of its two objectives to exercise operational risk practices across the equities clearing and trading processes. The cybersecurity scenarios tested by this exercise included corruption of publicly reported stock prices, corruption of trades (changing of *buys* to *sells),* and substantial loss of availability of the National Market System and resulted in identifying both effective processes and areas for improvement.

While the industry and its regulators are investing significant effort to work symbiotically to improve cybersecurity for financial services, the effort continues even beyond those groups. Recognizing that our ability to maintain confidence in financial services relies on other key constituencies, the industry has formed collaborations with other key parties. One example is the development of the Cyber Operational Resiliency Review (CORR) currently being piloted. This pilot, organized by BITS, allows financial institutions to request, through The Department of the Treasury, a review by a team of specialists supplied by The Department of Homeland Security of an institution's cyber practices and networks. In addition, BITS, FS-ISAC and other associations have formed collaborative relationships with various law enforcement agencies including the Federal Bureau of Investigation, United States Secret Service and US Postal Inspectors to coordinate industry and law enforcement efforts to prevent and prosecute cybercrime. Law enforcement was a key participant in the efforts led by the FS-ISAC toward mitigating issues with commercial account takeover.

Understanding that it is important to strengthen every link in the infrastructure chain, the industry has also affected outreach efforts to other key sectors. One recent example was showcased this past Wednesday in a White House-sponsored event that announced the Principles for Voluntary Efforts to Reduce the Impact of Botnets in Cyberspace developed by the Industry Botnet Group. This multi-industry group, committed to working together to combat cyber threats, is a voluntary group of corporations, trade associations, and non-profit organizations, led by a steering committee composed of BITS, Business Software Alliance, Online Trust Alliance, Software Information Industry Association, National Cyber Security Alliance / StaySafeOnline, StopBadWare, TechAmerica, U.S. Internet Service Provider Association, and the U.S. Telecommunications Association. Recognizing that botnets have a serious impact to the security and privacy of both individuals and businesses as they facilitate the delivery of malicious software by the cybercrime community, this multi-stakeholder group is acting collaboratively to mitigate the problem. Another recent example was the successful effort undertaken by Microsoft's Digital Crimes Unit – in collaboration with the FS-ISAC and NACHA – The Electronic Payments Association, to take down the command and control center of a major botnet ring operating within the US.

These types of efforts recognize a key factor – today's Internet and electronic world is highly integrated and relies on multiple organizations and providers to effectively mitigate security risks. That is why the industry has been and continues to be supportive of efforts to assure a more

consistent level of security within other critical sectors in the cyber environment. That is also why the industry has invested in educating consumers on cybersecurity. Consumers and businesses play a key role in cybersecurity and have a responsibility to protect themselves as well. The financial services industry and others have recognized that consumers and businesses often lack the skills and awareness to fully protect themselves. As a result, significant investments have been made in education efforts by financial institutions and associations and we applaud the House's passage of H.R. 2096 The Cybersecurity Enhancement Act of 2012 sponsored by Representative Michael McCaul, which will help with this effort.

The industry's efforts start with individual institutions that provide educational materials via websites, mailings and community educational events. Financial associations also publish educational material and offer education directly to their communities through community outreach efforts. These efforts have often been done in collaboration with other parties such as law enforcement, as was the case with educating businesses about account takeovers, or with entities focused on citizen education such as the National Cyber Security Alliance and its StaySafeOnline campaign.

As these efforts show, the financial services industry understands cybersecurity is a critical issue, and that the best success in improving security comes from collaborative efforts and not just the work of financial institutions. Clearly financial institution work is significant in terms of resources, cost and commitment. Institutions willingly undertake these security and awareness efforts and recognize their necessity to safeguarding customers and their accounts, and the overall financial system. These protections are critical to maintaining customer trust and confidence in the industry, and are a highly important investment. Individual institutions also recognize success depends on investing in broader, collaborative efforts beyond financial services to ensure a resilient economic system.

I would be remiss, however, if I did not mention one other key area of collaboration – that is, the area of threat information sharing. Like all cybersecurity defenses, information sharing exists at multiple levels. Individual institutions monitor their own threats and in the financial services sector, we do an effective job of sharing threats through the FS-ISAC. But, there remains much opportunity to exchange threat information more broadly. Most of the efforts to date have involved intra-industry efforts in the financial services sector and in the defense industry sector, through its

Defense Cyber Information Sharing Environment (DCISE) program. Inter-industry and public/private information sharing opportunities remain to be developed. BITS, in cooperation with the FSSCC and the FS-ISAC, is nearing the end of a study to assess existing and potential collaboration programs between the US Government's national security agencies and the financial services sector. The study focuses on threat information sharing, cyber security capacity building and cyber-related crisis management.

Threat data and threat analysis are very often industry agnostic. Viruses, Trojans and other malicious software are sometimes written to attack the users of a particular sector, such as those that attempt to steal login credentials from banking customers. In many cases, however, they are not aimed at a particular sector. For example, malicious software that attempts to take over a user's computer or other device to make it part of a botnet[2] that will be subsequently used by cybercriminals simply does not care who or for what purpose one is using their device. Botnets, however, create the risk of establishing large numbers of endpoints available to criminals to commit cybercrime. Likewise, cyber anarchists who use denial of service attacks in attempts to disrupt the availability of systems, websites and other technology resources use these techniques to target entities in virtually all private and public sectors. The more information shared across a broad swath of sectors about the sources of attacks, the nature of attacks and the pattern of attacks, the more ultimate improvement will occur in the responsiveness and the defense of all sectors. Frankly, however, organizations are often hesitant to share this type of information. Some are concerned that information exchanged will not be protected and will subsequently be revealed. While true even with private-to-private sharing, this is especially true with private companies sharing information with public entities. Private organizations are concerned that revelation of the information will impact their reputation and the confidence of their customers – regardless of their industry. That is why the financial services industry along with other industries was supportive of the passage of HR 3523, the Cyber Intelligence Sharing and Protection Act, which, if enacted, offers additional protections and assurances to the confidentiality of shared information.

[2] The term *bot* is short for robot. Criminals distribute malicious software (also known as malware) that can turn your computer into a bot (also known as a zombie). When this occurs, your computer can perform automated tasks over the Internet, without you knowing it. Criminals typically use bots to infect large numbers of computers. These computers form a network, or a *botnet*. Criminals use botnets to send out spam email messages, spread viruses, attack computers and servers, and commit other kinds of crime and fraud. (As defined by Microsoft ® Safety & Security Center at http://www.microsoft.com/security/resources/botnet-whatis.aspx)

It is important to recognize that the information sharing generally done with regard to cyber attacks seldom involves non-public, private information regarding individuals. We recognize that as HR 3523 was debated, the concern about protecting individuals' information and privacy was a legitimate concern raised by several Members of the House. As you consider future cybersecurity legislation, however, we do urge you to consider solutions to allow sharing of this type of information under certain circumstances in a manner that protects the rights of individuals, but facilitates their protection as well. There are legitimate reasons to share this information that benefits citizens. For example, a breach occurring at a payroll processor can result in cybercriminals obtaining the checking account information of individuals. Today, sharing that information with the financial institutions that hold those accounts is difficult at best. Sharing it, however, and sharing it quickly, would allow those institutions to take action to prevent fraud against their commercial and retail customers.

In closing, please accept my thanks for the opportunity to testify to the Committee. Cybersecurity is a vitally important issue for both the private and public sectors. Protecting companies, and more so, protecting their customers and our citizenry in general must remain key imperatives for us all. Further, protecting the infrastructures that support our economy is crucial to maintaining confidence and an operating global financial system. We commend the Committee for recognizing the importance of this subject and for your attention in supporting the strongest cyber defense for our nation.

###