Testimony of

William B. Nelson

On Behalf of the

The Financial Services Information Sharing & Analysis Center

Before the

United States House of Representatives

Financial Institutions and Consumer Credit Subcommittee

September 14, 2011

FS-ISAC BACKGROUND

Chairman Capito, Ranking Member Maloney, and members of the Subcommittee, my name is William B. Nelson. I am President and CEO of the Financial Services Information Sharing & Analysis Center (FS-ISAC). I want to thank you for this opportunity to address the U.S. House of Representatives Financial Institutions and Consumer Credit Subcommittee on the important issue of cyber crime, its impact to the financial services industry, and the cooperation and information sharing between government agencies and the private sector.

The FS-ISAC was formed in 1999 in response to the 1998 Presidential Decision Directive 63 (PDD63) that called for the public and private sector to work together to address cyber threats to the Nation's critical infrastructures. After 9/11, and in response Homeland Security Presidential Directive 7 (HSPD7) and the Homeland Security Act, the FS-ISAC expanded its role to encompass physical threats to our sector.

The FS-ISAC is a 501(c)6 nonprofit organization and is funded entirely by its member firms and sponsors. In 2004, there were only 68 members of the FS-ISAC, mostly larger financial services firms. Since that time the membership has expanded to over 4,200 organizations including commercial banks and credit unions of all sizes, brokerage firms, insurance companies, payments processors, and over 30 trade associations representing the majority of the U.S. financial services sector.

The FS-ISAC works closely with various government agencies including the U.S. Department of Treasury, Department of Homeland Security (DHS), Federal Reserve, Federal Financial Institutions Examination Council (FFIEC) regulatory agencies, United States Secret Service, Federal Bureau of Investigation (FBI), National Security Agency (NSA), Central Intelligence Agency (CIA), and state and local governments.

With respect to cooperation within the financial services sector, the FS-ISAC is a member of, and partner to the Financial Services Sector Coordinating Council (FSSCC) for Homeland Security and Critical Infrastructure Protection established under HSPD7. We also work closely with other industry groups and trade associations that are members of the FS-ISAC including the American Bankers Association (ABA), Securities Industry and Financial Markets Association (SIFMA), Independent Community Bankers Association (ICBA), and the BITS division of the Financial Services Roundtable. In addition, our membership includes various payments, clearing houses and exchanges such as the National Automated Clearing House Association (NACHA), Depository Trust and Clearing Corporation (DTCC), New York Stock Exchange, NASDAQ, The Clearing House (TCH), the various payment card brands and most of the card payment processors in the U.S.

The overall objective of the FS-ISAC is to protect the financial services sector against cyber and physical threats and risk. It acts as a trusted third party that provides anonymity to allow members to submit threat, vulnerability and incident information in a non-attributable and trusted manner so information that would normally not be shared is able to be provided from the

originator and shared for the good of the sector, the membership and the nation. A complete list of FS-ISAC information sharing services and activities include:

- delivery of timely, relevant and actionable cyber and physical email alerts from various sources distributed through the 24x7x365 FS-ISAC Security Operations Center (SOC);
- an anonymous online submission capability to facilitate member sharing of threat, vulnerability and incident information in a non-attributable and trusted manner preparing cyber security briefings and white papers;
- operation of email list servers supporting attributable information exchange by various special interest groups including the FSSCC, the FS-ISAC Threat Intelligence Committee, threat intelligence sharing open to the membership, the Payment Processors Information Sharing Council (PPISC), the Clearing House and Exchange Forum (CHEF), the Business Resilience Committee, and the Payments Risk Council;
- anonymous surveys that allow members to request information regarding security best practices at other organizations;
- bi-weekly threat information sharing calls for members and invited security/risk experts to discuss the latest threats, vulnerabilities and incidents affecting the sector;
- emergency threat or incident notifications to all members using the Critical Infrastructure Notification System (CINS);
- emergency conference calls to share information with the membership and solicit input and collaboration;
- engagement with private security companies to identify threat information of relevance to the membership and the sector;

- development of risk mitigation best practices, threat viewpoints and toolkits;
- Subject Matter Expert (SME) committees including the Threat Intelligence Committee and Business Resilience Committee that provide in-depth analyses of risks to the sector, provide technical, business and operational impact assessments and recommend mitigation and remediation strategies and tactics;
- special projects to address specific risk issues such as the Account Takeover Task Force (see pages 11 - 16);
- document repositories for members to share information and documentation with other members;
- development and testing of crisis management procedures for the sector in collaboration with the FSSCC and other industry bodies;
- semi-annual member meetings and conferences; and
- online webinar presentations and regional outreach programs to educate small to medium sized regional financial services firms on threats, risks and best practices.

A key factor in all of these activities is trust. The FS-ISAC works to facilitate development of trust between its members, with other organizations in the financial services sector, with other sectors, and with government organizations such as law enforcement, regulators, and intelligence agencies.

The FS-ISAC has implemented a number of programs in partnership with the Department of Homeland Security (DHS) and other government agencies. Earlier this year, the FS-ISAC, in partnership with DHS became the third ISAC to participate in the National Cybersecurity and

Communications Integration Center (NCCIC) watch floor. FS-ISAC representatives, cleared at the Top Secret / Sensitive Compartmented Information (TS/SCI) level, attend the daily briefs and other NCCIC meetings to share information on threats, vulnerabilities, incidents, and potential or known impacts to the financial services sector. While this program is relatively new, our presence on the NCIC floor has largely greatly enhanced situational awareness and information sharing between the financial services sector and the government.

As part of this partnership, the FS-ISAC set up an email listserv with U.S. CERT where actionable incident, threat and vulnerability information is shared in near real-time. This listserv allow FS-ISAC members to share directly with U.S. CERT and further facilitates the information sharing that is already occurring between FS-ISAC members and with the NCIC watch floor or with other government organizations.

In addition, FS-ISAC representatives sit on the Cyber Unified Coordination Group (Cyber UCG). This group was set up under authority of the National Cyber Incident Response Plan (NCIRP) and has been actively engaged in incident response. Cyber UCG's handling and communications with various sectors following the RSA attack in March of this year is one example of how this group is effective in facilitating relevant and actionable information sharing.

Finally, it should be noted that the FS-ISAC and FSSCC have worked closely with DHS, the U.S. Department of Treasury, FBI, U.S Secret Service and other government partners to obtain over 250 Secret level clearances and a number of TS/SCI clearances for key financial services sector personnel. These clearances have been used to brief the sector on new information

security threats and have provided useful information for the sector to implement effective risk controls to combat these threats.

PUBLIC / PRIVATE SECTOR RESPONSE TO THE CYBER CRIME ISSUE

The FS-ISAC is aware through its information sharing arrangements with both public and private sector organizations that criminal threats are targeting US financial institutions, capital markets exchanges, clearing houses, payment processors, businesses and consumers. However, research shows that losses due to cyber crime currently only account for a small percentage of the overall fraud losses incurred by financial institutions. In the last eighteen months, actual losses experienced by financial institutions and their customers as a result of cyber-related fraud has actually declined in spite of the fact that the number of attacks has increased. The FS-ISAC and its members recognize the online criminal threat both to the affected institutions and to consumer confidence posed by these criminal activities and we are taking steps to address areas of concern.

Law enforcement and a number of government agencies have taken a lead role working with the FS-ISAC, its member organizations, payments processors, and the financial services sector as a whole to combat these types of attacks. An example of a successful instance of government/financial services sector information sharing occurred on August 24, 2009, when the FBI, FS-ISAC and NACHA released a joint bulletin concerning account takeover activities targeting business and corporate customers. The bulletin described the methods and tools employed in recent fraud activities perpetrated against small to medium-size businesses that had

been reported to the FBI. The objective of the bulletin was to employ FS-ISAC and NACHA subject matter expertise and apply it to the FBI case information to identify detailed threat detection, prevention, and risk mitigation strategies for financial institutions and their business customers, whilst preserving the integrity of the FBI's ongoing investigations. The FS-ISAC and NACHA developed a comprehensive list of recommendations for financial institutions to educate their business customers on the need to use online banking services in a secure manner. The bulletin was distributed through the FS-ISAC to its over 4,200 members, which includes over 30 member associations such as NACHA, ABA, and ICBA. Subsequent releases of the bulletin were shared with the press in 2010, redacting sensitive information about the ongoing investigations.

The risk mitigation tactics that are outlined in the joint FBI/FS-ISAC/NACHA bulletin include information security best practices that are consistent with the 2005 Federal Financial Institutions Examination Council's (FFIEC's) Guidance on Authentication in an Internet Banking Environment. The joint FBI/FS-ISAC/NACHA bulletin actually moved further than the 2005 FFIEC Guidance in its recommendations. Specifically, the bulletin recommended that financial institutions implement a layered "defense in-depth" approach to information security to protect financial institutions and their customers.

FFIEC SUPPLEMENTAL GUIDANCE ON INTERNET BANKING AUTHENTICATION

The recent FFIEC Supplemental Guidance on Internet Banking Authentication released on June 28, 2011 incorporates many "defense in-depth" recommendations and include a number of very

important new regulatory provisions. The following is a summary of some of the Supplemental Guidance's key provisions.

The Guidance reinforces existing supervisory expectations for annual risk assessments by financial institutions. These risk assessments should consider changes in the internal/external threat environment, changes in the financial institution's customer base, changes in functionality to online Internet services, and the financial institution's actual fraud experiences. Authentication controls should be upgraded in response to risk assessments.

For the first time, the FFIEC distinguishes between retail and commercial accounts. It raises the bar for minimum controls for all accounts and recognizes that commercial accounts pose a higher level of risk. Commercial account controls should be consistent with increased levels of risk and stronger than controls for consumer accounts.

The FFIEC Supplemental Guidance now requires financial institutions to have layered security for consumer accounts. "Layered security" is defined as having different controls at different points in a process, so that weakness in one control is compensated by strengths in another control. At a minimum, layered security should include anomaly detection and response at initial customer login, and at initiation of funds transfers to other parties. Layered security for commercial accounts should be stronger than those implemented for consumer accounts. The Guidance specifies enhanced controls for system administrators of commercial accounts. Examples of these enhanced controls include additional authentication/verification of new payees and changes to established value threshold or time windows.

Layered security should now include anomaly detection. Changes in consumer or commercial account activity should be detected and steps taken to ensure that additional controls are in place if such activity is discovered. However, according to the FFIEC Supplemental Guidance, "simple" device identification and challenge questions are no longer deemed effective as a primary control. Instead, financial institutions will be required to implement "*Complex Device Identification."* An example of complex device ID includes use of a one-time cookie, in conjunction with other factors such as the PC's configuration, IP address, and geo-location used to create a digital "fingerprint" of the customer's personal computer. The Guidance also calls for more "*Complex Challenge Questions"* not easily found by cyber criminals on the Internet. These "out of wallet" questions should not rely on publicly available information and there should be more than one question, potentially even including a "red herring" question that only the account holder will recognize as false requiring a potentially fabricated answer.

Lastly, the FFIEC Supplemental Guidance calls for increased customer awareness/education efforts by financial institutions. The Guidance recognizes that customers have an important role to play in online banking security and that for consumers and small businesses, their financial institution is most likely the more knowledgeable party concerning online security. Financial institutions have an obligation to help customers practice good online banking security and clarify consumer rights under Regulation E. Financial institutions should also educate their commercial account holders, especially small businesses, on use of security controls that are available for their online banking services.

FFIEC regulatory agencies will begin examinations in January 2012 to assess conformance with the new FFIEC Supplemental Guidance.

FS-ISAC ACCOUNT TAKEOVER TASK FORCE

In 2010, the FS-ISAC formed the Account Takeover Task Force (ATOTF) as a result of continued concern and need for additional tools to help financial institutions and their customers combat online account takeover attacks. The ATOTF consists of over 120 individuals from thirty-five financial services firms of all sizes and types, ten industry associations and processors and representatives from seven government agencies.

The ATOTF has focused on deliverables in three areas of effective cyber defense: Prevention, Detection and Response. Deliverables for each of these subgroups include:

1. **Prevention**
   - Industry Advisories
     - Corporate & Small Business Customers
       - Fraud Advisory for Businesses: Corporate Account Take Over, co-branded with US Secret Service, FBI and Internet Crime Complaint Center (IC3) The advisory is available here: http://www.fsisac.com/files/public/db/p265.pdf
     - Financial Institutions
     - Retail Customers & Consumers

        - Fraud Advisory for Consumers: Involvement in Criminal Activity through Work from Home Scams, co-branded with FBI and IC3. The advisory is available here: http://www.fsisac.com/files/public/db/p264.pdf
        - Example of a Work-From-Home Scheme
    - J1-Visa Money Mule Advisory
    - Internet Auto Fraud
- Fraud Education and Awareness.

  Representatives and volunteers from the industry have participated in various financial services, regulatory, and corporate user events to educate the business and government community.
- Improve Information Sharing with Law Enforcement
    - Inventory information sharing portals
    - IP addresses involved in frauds, money mule accounts, attack signatures, Suspicious Activity Reports (SAR) and other fraud trends
    - First joint FBI/FS-ISAC Cyber Crime Report
- Develop Email Trust Relationship working with financial institutions and large Internet Service Providers (ISPs). The Trusted Email Registry is currently being piloted. Both BITS and FS-ISAC will announce to their members when it becomes available for general use, at which time both organizations will continue to encourage members to implement email authentication protocols.

2. Detection

- List of Vendors and Service Providers

  Smaller financial institutions use a core group of service providers and this list provide them with security offerings.

- Detection Whitepaper for financial institutions.
  - Document focused on detection of account takeover victims.
- Techniques for recovering customers from ZeuS or other keystroke logging/man-in-the-middle Trojan infections and the exploration of third-party services with the goal of gathering elements of intelligence to enable better detection methods.
- Development of Webinars and Training to enable better education of customers with the goal of aiding detection techniques while improving awareness of the issues.
- Document Standard Set of Requirements and enhancements for alerting and security requirements for core ACH/wire transfer software providers.

3. Response

- Contact List, Procedures

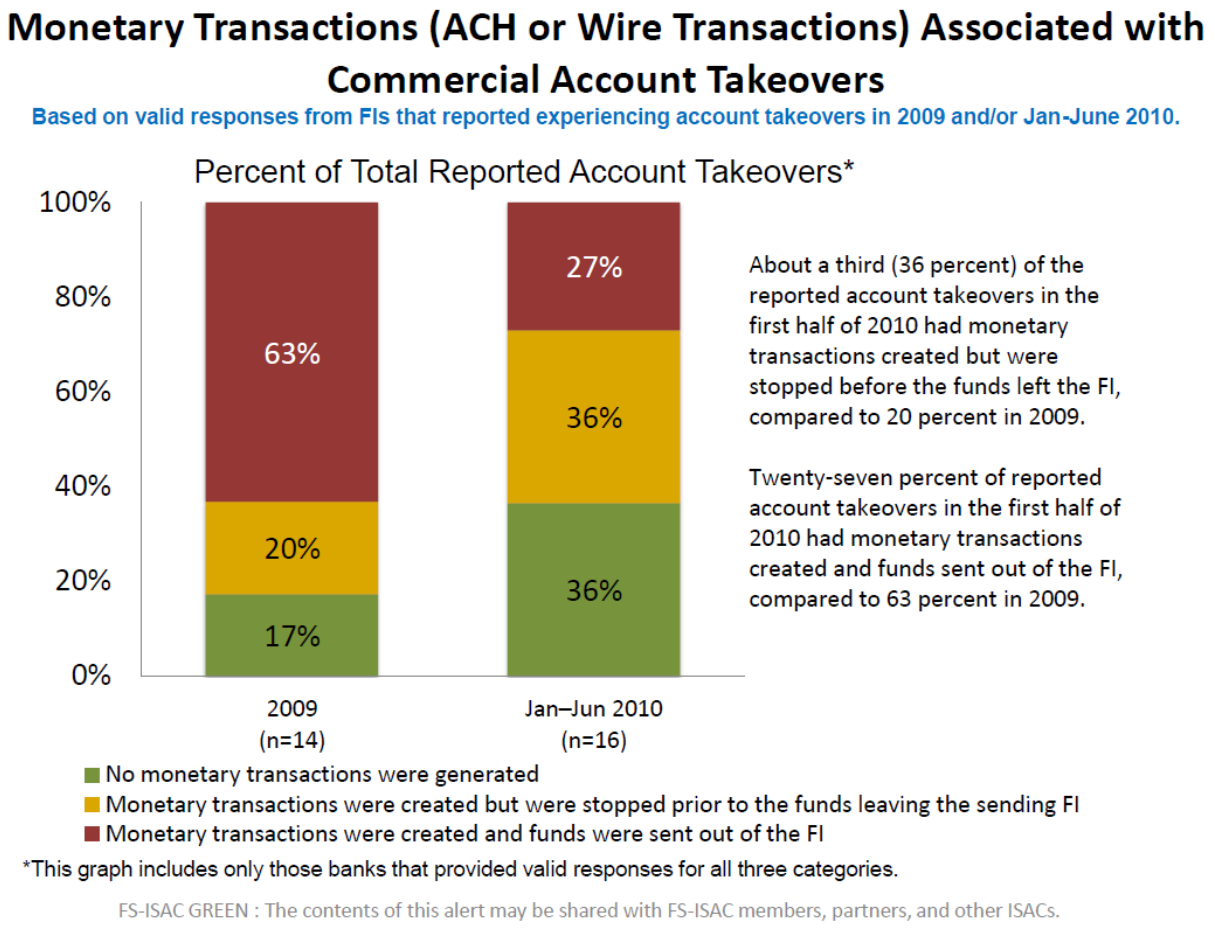
  This list provides financial institutions the information they need to report account takeover attacks via online banking to the Secret Service, FBI and other agencies, and a process for keeping the contact lists current.

- Form for Reporting account takeovers, including what should be submitted in the incident report and used for metrics to measure the success of the ATOTF.
- Actions financial institutions can take after an incident, communicated via FS-ISAC advisory notices.

- Monitor the National Cyber-Forensics & Training Alliance (NCFTA) Internet Fraud Alert service. This provides financial institutions with information for recovered credentials from the takedown of botnet command and control servers.
- List of forensic providers and forensic tool providers.
- List of Resources currently available for cyber crime and broad education so that financial institutions can leverage existing resources.
- Develop Malware Submission method and provide a process for sharing identified new malware with government/law enforcement agencies and anti-virus vendors.
- Redesign Suspicious Activity Report (SAR) Submission and Analysis Process by working with the Financial Crimes Enforcement Network (FinCEN) to give financial institutions and regulators more actionable information.
  - Recommendations for reporting an account take over attack via SARs.
- Add Fraud Contacts in FS-ISAC Membership Directory
  - FS-ISAC members updated contact information
- Conferences / Awareness—speeches by ATOTF members
  - May 2011 - Fiserv Risk Management Conference
  - June 2011 – The Clearing House Payments Forum
  - July 2011 - Advanced FFIEC Bank Secrecy Act / Anti-Money Laundering (BSA/AML) Specialists Conference
    - Continuing education to FFIEC examiners with specialized BSA/AML experience within the financial institution regulatory agencies.
    - Participants from OCC, FDIC, FBI, FS-ISAC
  - August 2011 - CERT's GFIRST conference

- August 2011 - International Association of Financial Crimes Investigators (IAFCI) conference
- August – FFIEC Bank Examination Conference
- FS-ISAC Account Takeover Workshops February to September 2011 – Twelve workshops conducted around the U.S. in cooperation with the Regional Payments Associations

- Baseline Account Take Over Survey
  - Establish baseline for Commercial Account Takeover attempts and losses for 2009 and the first half of 2010
  - 77 financial institutions responded to the survey
  - Statistics indicate financial institutions are doing a better job of stopping fraudulent transactions from being created and from funds leaving the financial institution
  - FS-ISAC will conduct another survey to capture data for all of 2010
    - Follow-up survey for 2011 data is also planned
  - The following chart illustrates one of the key findings of the Commercial Account Study (CAT). During the timeframe of the study, the trend shows that fewer monetary transactions are being created and if they are created, there are far less fraudulent payments leaving originating financial institutions.



As a result of the 2009 joint FBI/FS-ISAC/NACHA bulletin, the FFIEC Supplemental Guidance and the many deliverables of the ATOTF, financial services firms and their business, government, and consumer customers have become more aware of the online risks facing them and of the many effective layered defense practices to mitigate those risks. As a result, more financial institutions are now aware of how to detect, prevent and respond to malicious and criminal activities resulting from online attacks.

FS-ISAC EXERCISES

The FS-ISAC provides the 24x7x365 platform for its members to share information between themselves, with the government and law enforcement, and with other sectors. The FS-ISAC participates in various cyber exercises such as those conducted by DHS (Cyber Storm I, II, and III) and provides support for FSSCC exercises such as CyberFIRE.

The FS-ISAC undertook on its own a major effort to conduct a national Cyber Attack Against Payment Processes (CAPP) Exercise in February 2010. The 2010 CAPP Exercise included a variety of simulated attacks that tested the financial services industry's ability to respond and react to different types of cyber attacks. The exercise provided a forum to raise awareness regarding best practices and remediation steps to minimize the risk to the financial services firms and their customers from these various types of attacks.

Participation in the exercise was not limited to FS-ISAC members. In addition to the 634 financial services firms that participated in the exercise, 67 business/government users of payments services, 34 payment processors and 29 retailers also participated in the three day event. The CAPP Exercise had several major findings in several key areas including the ability of firms to recognize and detect attacks, security policy, response and communication, preventing future attacks and a final set of recommendations. Further information about these findings can be found in the 2010 CAPP Exercise executive Summary published on this website: http://www.fsisac.com/files/public/db/p243.pdf

LAW ENFORCEMENT SUCCESSES

From a law enforcement perspective, recent progress has been made against some cyber crime activities. The Secret Service and the FBI have made numerous arrests in the last two years of many individuals and gangs responsible for various data breaches and criminal cyber attacks. These arrests have been important in stemming the tide of rising cyber attacks by going after the criminal masterminds behind them. Arrests have been made in many cases but some of the cyber criminals indicted operate in other countries, mostly in Eastern Europe, and they remain at-large. An area where our Federal Government could help is to force better cooperation from those countries' governments that fail to cooperate in these types of cyber crime investigations and prosecutions.

CYBER SECURITY COLLABORATIVE EFFORTS BY THE FINANCIAL SERVICES INDUSTRY

The FS-ISAC is a member of the Financial Services Sector Coordinating Council (FSSCC) and is viewed as the FSSCC's operations partner. Through the FSSCC, the private sector financial service industry collaborates with Financial and Banking Infrastructure Information Committee (FBIIC) which consists of the key financial services industry regulators involved in critical infrastructure protection such as the U.S. Treasury, the Federal Reserve, the Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, and others. FSSCC and FBIIC members meet regularly and participate in classified briefings from law enforcement and the intelligence community where important vulnerability and threat information is exchanged.

Financial regulators are actively involved in developing regulations and supervisory guidance and in conducting focused examinations of information security, vendor management and business continuity controls at financial institutions and major service providers. There are nearly a dozen booklets covering these key cyber security and business continuity issues in the FFIEC handbook.

The FS-ISAC also works closely with other key financial services industry groups to protect the industry and its customers against cyber threats. Some of the key organizations have included the ABA, ICBA, FSSCC, NACHA, Regional Payments Associations, BITS and ITAC. The following is a partial list of activities that the financial services sector has undertaken to improve the industry's response to online criminal activities:

- The ABA and ICBA have been instrumental in increasing the membership levels and reach of the FS-ISAC to over 4,200 members today. Through the FS-ISAC's thirty association and processor members, the reach of the FS-ISAC is nearly universal to every regulated financial institution in the U.S., regardless of its size.

- FS-ISAC has worked closely with the Regional Payments Associations to offer regional account takeover workshops for their members. These day-long events consist of presentations from defense in-depth solution providers and include an interactive tabletop exercise that engages the participants in a simulated series of cyber attacks against their financial institutions' customers. Twelve of these workshops have been offered in 2011

and have been supplemented by numerous speaking engagements around the country by the FS-ISAC staff to various conferences.

- The nonprofit ITAC, the Identity Theft Assistance Center, which is part of the Financial Services Roundtable, provides a free recovery service to victims of identity theft. Since its inception, ITAC has helped more than 90,000 consumers recover their financial identities.

ADDITIONAL STEPS THAT INDUSTRY AND THE FEDERAL GOVERNMENT CAN TAKE TOGETHER

Rather than outline a series of recommendations that the financial services industry should take independently and a separate set of recommendations that the Federal Government should address, the following is a consolidated approach for both. This approach better illustrates the need and commitment that we must have for public/private sector cooperation in protecting the industry and the nation's citizens from the growing threat of cyber crime.

1. IMPROVE CYBER CRIME LAW ENFORCEMENT

   a. There needs to be better and more domestic and international collaboration regarding investigations and prosecutions given the origins of a significant portion of cyber crime. Countries that have not adopted the Council of Europe's Convention on Cyber Crime should be encouraged to do so. The Convention is an international, multilateral treaty specifically addressing the need for cooperation in the investigation and prosecution of computer network crimes.

b. Sufficient funding is needed for cyber crime investigations and forensics. Currently, private sector firms report that some local law enforcement agencies require minimum thresholds before they will take the case. However, evidence indicates that most of these types of attacks are directed at many firms and their customers so the cumulative dollar value of the crime committed may be many times the amount of one particular loss.
c. Law enforcement must be more responsive to cyber crimes reported by financial services firms. There needs to be improved communications at a local level between financial services firms and their cyber crime law enforcement contacts and an understanding of how to report these crimes so that action will be taken.

2. Improve Financial Institution Information Security Programs

Regulators and industry need to have a flexible and dynamic approach to cyber security so that individual financial institutions can continue to improve information security programs based on their size, scope of activities, and structure. This builds on the foundation embodied in the Gramm-Leach-Bliley Act framework and opposes prescriptive, one-size-fits-all or technology-specific approaches.

3. Implementation of Defense in-Depth Security

Financial services firms and payment processors need to implement defense in-depth security in order to protect their customers and their institutions from cyber criminal attacks. These security solutions must take into account the evolution of the changing threat landscape and will need to be updated over time. Commercially reasonable security procedures must achieve an appropriate balance between security, risk and usability. The June 28, 2011 FFIEC Supplemental Guidance

on Internet Banking Authentication goes a long way towards achieving that balance without dictating any single solution which may prove to be untenable over time.

4. IMPROVE PUBLIC/PRIVATE SECTOR COLLABORATION

Expanded information sharing between government agencies and the financial services industry is one of the FS-ISAC's primary goals. There have been improvements made but there needs to be greater private sector access to threat and intelligence from Federal intelligence and law enforcement agencies. This access must be administered in a manner that can provide broader protection without providing undue market advantage to a select group or that would compromise ongoing investigations. Specific recommendations include:

a. Provide financial institutions, networks and processors with timely, relevant and actionable information on threats, vulnerabilities, and exploits.
b. Provide the financial services industry with analysis of trends using existing data reporting requirements (e.g., FinCEN's data of Suspicious Activity Reports which includes computer crimes).
c. Support the existing National Infrastructure Protection Plan (NIPP) and its supporting organizations such as the National Council of ISACs of which the FS-ISAC belongs and the sector coordinating councils, such as the FSSCC. Also support the FSSCC's public sector partner, the Financial and Banking Information Infrastructure Committee (FBIIC) and support their joint initiatives.
d. Compile and share data on payment system fraud and security trends.
e. Fund top R&D priorities, such as the FSSCC's priority project on identity assurance.

f. Support industry exercises that relate to cyber threats. By routinely engaging in exercises and training, public and private sector participants build relationships and establish trust that is essential for sharing information.

g. Continue towards the goal of a fully integrated Joint Coordination Center for sharing cyber threat information between the public and private sectors. The embedding of financial sector personnel in the NCCIC is a positive step in that engagement process.

5. Improve the Internet Infrastructure

Use Federal procurement power to improve the security of software, hardware and services that support the Internet business infrastructure and applications (i.e., enhanced technology that is implementable and cost appropriate for the market.)

6. Education

More public/private sector collaboration is needed to support educational efforts to increase consumer and business awareness of cyber threats and risk mitigation best practices. One example of such an effort has been undertaken by the National Cyber Security Alliance in promoting a "Stay Safe Online" campaign as part of the October Cyber Security Awareness month (http://www.staysafeonline.org/).

As a result of these types of programs and the efforts of the FS-ISAC Account Takeover Task Force, financial institutions have educated their customers regarding phishing and other social engineering attacks with information on their websites, mailers and in their bank lobbies

regarding safe and secure online banking practices. Corporate and government users of online financial services products can now take advantage of these educational tools that are available.

Thank you again for this opportunity to present this testimony and I look forward to your questions.

United States House of Representatives
Committee on Financial Services

"TRUTH IN TESTIMONY" DISCLOSURE FORM

Clause 2(g) of rule XI of the Rules of the House of Representatives and the Rules of the Committee on Financial Services require the disclosure of the following information. A copy of this form should be attached to your written testimony.

1. Name:	2. Organization or organizations you are representing:
William B. Nelson	FS-ISAC

3. Business Address and telephone number:

[redacted]

4. Have you received any Federal grants or contracts (including any subgrants and subcontracts) since October 1, 2008 related to the subject on which you have been invited to testify?	5. Have any of the organizations you are representing received any Federal grants or contracts (including any subgrants and subcontracts) since October 1, 2008 related to the subject on which you have been invited to testify?
☐ Yes ☑ No	☐ Yes ☑ No

6. If you answered .yes. to either item 4 or 5, please list the source and amount of each grant or contract, and indicate whether the recipient of such grant was you or the organization(s) you are representing. You may list additional grants or contracts on additional sheets.

7. Signature: William B Nelson

Please attach a copy of this form to your written testimony.