Testimony of

Michele B. Cantley

Chief Information Security Officer

Regions Bank

On Behalf of the

The Financial Services Information Sharing & Analysis Center

Before the

United States House of Representatives

Capital Markets and Government Sponsored Enterprises Subcommittee

June 1, 2012

FS-ISAC BACKGROUND

Chairman Garret, Ranking Member Waters, and members of the Subcommittee, my name is Michele Cantley. I am the Chief Information Security Officer for Regions Bank and I am appearing today for 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 Services Capital Markets and Government Sponsored Enterprises Subcommittee on the important issue of corporate account takeover and its impact to the financial services industry. In addition, my written testimony includes other recommendations for improving communication between the public and private sector about cyber threats as well as the efforts that our financial services sector can take to improve our defenses and educate our customers.

First, let me provide some background on Regions and FS-ISAC. Regions Financial Corporation, with $127 billion in assets, is a multi-state regional bank and is one of the nation's largest full-service providers of consumer and commercial banking, wealth management, mortgage, and insurance products and services. Regions is the 12th largest U.S. bank by deposits and loans and serves customers in 16 states across the South, Midwest and Texas, and operates approximately 1,700 banking offices and 2,100 ATMs. Regions is a member of the FS-ISAC.

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 4,400 organizations including commercial banks and credit unions of all sizes, brokerage firms, insurance companies, exchanges and clearing houses, 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), 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 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), all of the 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 instead provided for the good of the sector, the membership and the nation. 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
- presenting 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, Compliance and Audit Council, Insurance Risk Council, 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 view points 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 10-13);
- 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;

- participation in sector, cross-sector and national exercises such as the Cyber Attacks Against Payment Processes (CAPP), National Level Exercise 2012, and the Cyber Storm series;
- 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, for example, uses a traffic light protocol (red, yellow, green) to indicate to its members how information may be disseminated to FS-ISAC members, partners, and other ISACS. This protocol has been a key component in developing a clear means for trusted distribution of information. The FS-ISAC has also built a model for sharing information without attribution to a specific institution and also uses non-disclosure agreements (NDAs) to ensure that confidentiality of non-public and sensitive information is maintained.

The FS-ISAC is an active participant in cross-sector information sharing and has engaged in a number of cross-sector information sharing programs such as the Joint ISAC BOTNET Mitigation Process Working Group and the Cross Sector Information Sharing Framework, a vehicle for real-time cyber information sharing between the sectors. FS-ISAC currently also has a leadership role in the National Council of ISACs.

The FS-ISAC has implemented a number of programs in partnership with the Department of Homeland Security (DHS) and other government agencies. 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 real-time. This listserv also allows FS-ISAC members to share directly with U.S. CERT. In June 2011, 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. Over the course of a year, our presence on the NCCIC floor has largely greatly enhanced situational awareness and information sharing between the financial services sector and the government. The FS-ISAC recently obtained funding from a member to have full-time staff on the NCCIC floor in addition to the part-time resources that are currently deployed.

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 2011 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. The FS-ISAC would like to see this process updated to efficiently and effectively provide more clearances to the private sector.

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.

I want to thank you for the opportunity to address the issue of corporate account takeover. Corporate account takeover is the unauthorized use of valid online banking credentials, typically obtained via malicious software ("malware") that infect customers' workstations, laptops or computer networks. Cyber criminals use a variety of methods to infect business customers' computers and they are constantly updating their methods to match customers' uses of technology.

In order to get account information, cyber criminals continue to attack business customers' computers by phishing (attempting to acquire information (and sometimes, indirectly, money) such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication), malicious advertisements (or "malvertisements") and fraudulent messages on social media sites.

Phishing remains the most popular attack method that criminals use to infect victims' machines. Nonetheless, emails that purport to be from a victim's bank are no longer the primary type of phishing email. Criminals now send emails purporting to be from NACHA (The National Automated Clearing House Association), EFTPS (the Electronic Federal Tax Payment System), the US Postal Service, private delivery firms, telecommunications' companies, social media providers and others in order to trick their victims into opening the email and clicking on a link. Once the user clicks on such a link, it redirects the unknowing user to a server that then downloads malicious software onto the victim's computer. This malicious software includes a key logger (a program that can record a user's keystrokes) that captures the user's online banking credentials as he types them.

Another method of attack is malicious advertisements or "malvertising." In this case, criminals have put advertisements on search engines and other prominent news-sites. Victims, believing that it is a legitimate ad, click on the link, and the malware gets downloaded on their computer(s) and fraud can occur. A more recent method involves fraudulent messages sent from social media sites. These may include bogus friend requests, for example, that include links to malicious sites.

Once the criminals have the valid online banking credentials, they can impersonate the customer by logging onto the online banking site. They then create fraudulent ACH and/or wire transactions which they submit to the bank. The fraudulent transactions are generally directed to people who have been recruited to serve as intermediaries or "mules." The mules receive

instructions from the criminals regarding how to handle the funds. The mules might be instructed to withdraw the funds in cash and then send them elsewhere via legitimate money transfer or wire methods. The mules get to keep a percentage of the funds as payment for his/her services.

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. Over the past two years, 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.

The FS-ISAC has been active in its efforts to counteract the spread of corporate account takeover. 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 recently completed a report that includes recommendations to focus on three main areas—prevention, detection and responsiveness—in order to ensure an improved and effective defense against cyber crimes, including account takeover.

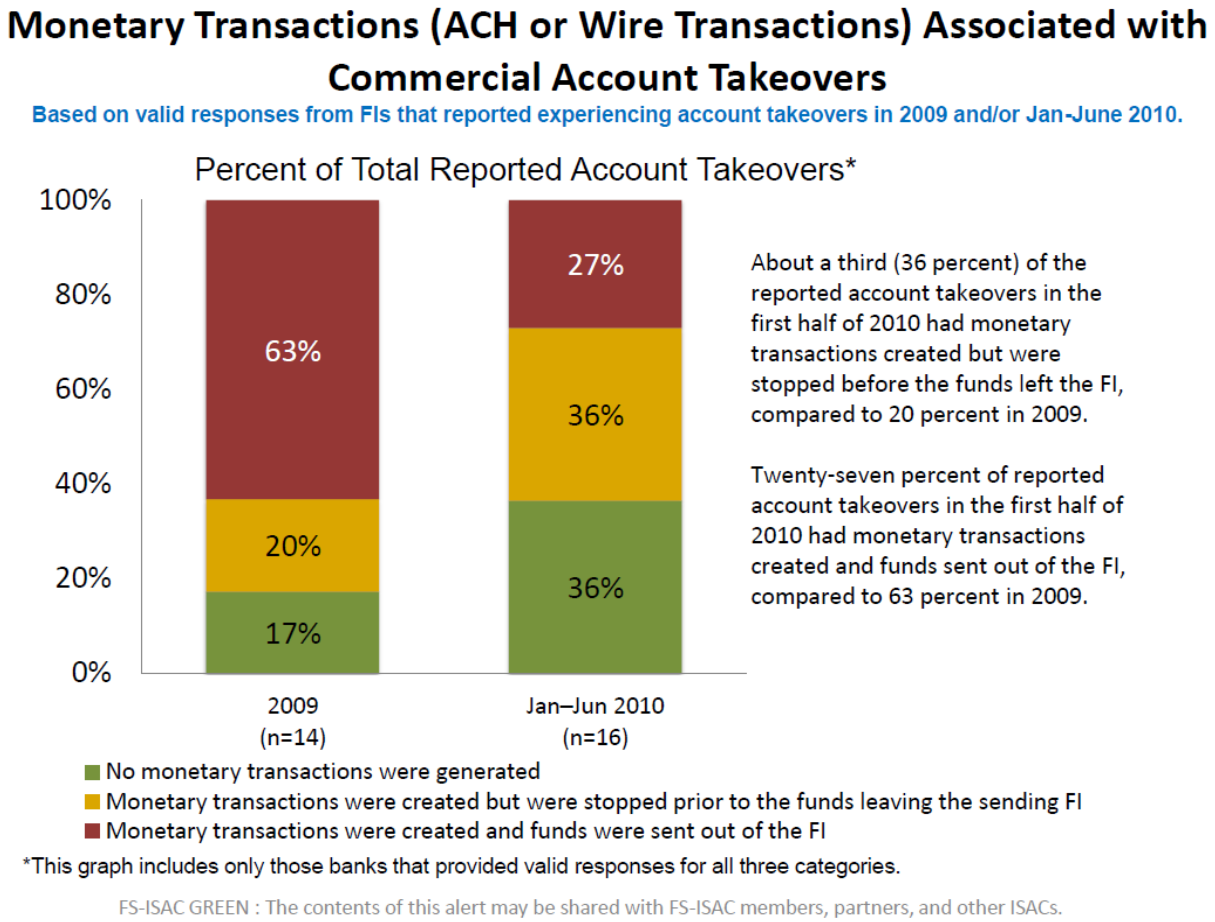
For each area, the ATOTF created work products whose purposes were to assist financial institutions of all sizes with dealing with account takeover by educating them and their customers on how account takeover works, what techniques can be used to detect and prevent account takeover, and lastly, in the event of an account takeover event, what steps financial institutions and customers should take to respond.

Examples of the work products include:

- Industry Advisories for Corporate & Small Business Customers and Financial Institutions
  - 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
- J1-visa Mule Advisory (many mules from abroad are recruited via J1-Visas)
- Fraud Advisory for consumers about Work from Home Scams (where mules are often recruited)
  - 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
- Detailed white papers on Detection, Prevention and Response Techniques
- A contact list and procedures which provide financial institutions with the information they need to report account takeover attacks to the Secret Service, FBI, and other law enforcement agencies

- A recommendation to FINCEN (since adopted) to redesign the Suspicious Activity Report (SAR) in order to appropriately capture account takeover events

Lastly, the ATOTF has undertaken, with the assistance of the FS-ISAC and the American Bankers Association, surveys of the FS-ISAC members about the scope and impact of the account takeover problem. Survey data has been obtained for 2009, 2010 and the first half of 2011. The chart which follows includes a portion of the survey data for 2009 and 2010. This chart reflects the collective work of the ATOTF and FS-ISAC members in working effectively to reduce monetary losses associated with account takeover.



In the most recent survey, members were asked about the most effective step they had taken to reduce corporate account takeover. The answer may surprise you. It was not technology or legislation; rather, it was customer education. As trusted partners, financial institutions are in the best position to educate our customers about the vectors of attack for corporate account takeover and how customers can protect themselves. This is why customer education was such an integral part of each ATOTF deliverable.

As noted above, the FS-ISAC and its membership have taken tremendous steps to limit cyber crime and corporate account takeover. Nonetheless, it is important to note that corporate account takeover attempts cannot be stopped solely by the actions of financial institutions. Beyond financial firms, our customers and participants in the broader electronic ecosystem all have roles to play to improve security.

Banks, for instance, have no direct control over the end customers' computers, nor can banks control what emails bank customers open or what websites they visit prior to accessing their online banking system(s). Nonetheless, to increase the security of our customers' accounts, we must educate our customers on the risks and monitor for anomalous transactions. Banks must continue to detect fraudulent transactions and stop them. Customers have a role to play in learning about these threats and practicing safe internet habits. Customers can also reconcile their accounts daily and review their electronic transactions for accuracy.

Others have roles to play as well. Law enforcement can assist by seeking out and arresting the criminals behind these attacks. Internet Service Providers (ISPs) can monitor traffic on their

network for much of this malicious software and alert their customers to these infections. (Collaboration is already underway with the government, ISPs, and others to reduce the number of servers and computers used to disseminate the malware and phishing emails that target financial institution customers.) ISPs and email service providers can create electronic security measures that "interrogate" phishing emails. If the senders don't authenticate the messages, they should be dumped into spam folders so they are less likely to fool users. Also, these companies can pursue civil actions to take down servers that send the phishing emails and malicious software. Finally, continued work on international legal and diplomatic levels is needed so that all countries recognize this type of cyber-crime and that there are some forms of sanctions for those countries that harbor the criminals who perpetuate the problem.

Another example of industry collaboration is the BITS / FSISAC Trusted Email Registry project, which is designed to strengthen the email delivery channel through better authentication and encryption.

Let me highlight one example of cooperation. 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, while 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 4,400 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 FFIEC Supplemental Guidance on Internet Banking Authentication released on June 28, 2011 incorporates many "defense in-depth" recommendations and includes a number of very important new regulatory provisions that fit into the larger and detailed regulatory landscape. To highlight, the financial services sector is highly regulated by international, Federal and state

authorities. Through numerous laws enacted by Congress over the past 150 years, federal financial regulators have implemented a complex regime that includes supervision of the financial institutions' operational, financial and technological systems. Regulators, such as the Federal Reserve, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency and Securities and Exchange Commission, conduct examinations to assess the adequacy of controls to address financial and other risks. These examinations focus on information security, business continuity, vendor management and other operational risks. In addition to these public sector entities, self-regulatory organizations (SROs), such as the Municipal Securities Rulemaking Board (MSRB), the Financial Industry Regulatory Authority (FINRA), the National Futures Association (NFA), and exchanges, such as the Chicago Mercantile Exchange (CME), and the New York Stock Exchange (NYSE), also play an important role in industry oversight.

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. The Guidance notes that banks must educate their customers on both the security

and protections provided to both retail and commercial clients. In doing so, it creates a regimen of clear disclosures. Commercial account controls should be consistent with increased levels of risk and stronger than the 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 strength 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, creation of new wire templates, added wire approvers, 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 (such as triggering incremental client authentication to validate questionable transactions) to ensure that additional controls are in place if such activity is discovered. Such efforts must protect customers' privacy yet should not interfere with efforts to detect fraud. 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, 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 consumers' and small businesses' financial institutions are likely more knowledgeable about online security. Financial institutions have an obligation to help customers practice good online banking security and to clarify, via customer education, the protections provided 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 have begun examinations to assess conformance with these new FFIEC Supplemental Guidance.

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 customers,

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 believes that the private sector and government can continue to work together to improve account security. Several areas of cooperation are outlined below.

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 any individual 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.

d. After a compromise is reported to law enforcement, law enforcement must allow the threat indicators from the attack to be shared with financial institutions. There are a number of instance where those indicators have not been shared and thus other financial institutions are exposed to similar attacks. We understand the sensitivity around nation state attacks and around preserving evidence for criminal cases. However, the actions of some law enforcement agencies to restrict information sharing is hampering the financial services' sector's ability to protect itself and its customers from similar attacks. This issue speaks clearly for the need for greater trust between the public and private sector.
e. In keeping with our commitment to education, it is also important for law enforcement, prosecutors and judges to have substantial cyber education and knowledge so that they can prosecute cyber criminals effectively.

2. CONTINUE TO 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. Financial institutions have comprehensive security regulations already in place. This approach 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. The House-backed Cyber Intelligence Sharing and Protection Act is a good example of strengthening information sharing in order ultimately to protect customers. 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 and is an essential building block towards a stronger trust model.

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 for the opportunity to present this testimony.