Testimony of

Gregory T. Garcia

On Behalf of the

The Financial Services Information Sharing & Analysis Center

Before the

United States House of Representatives

Financial Institutions and Consumer Credit Subcommittee

March 5, 2014

FS-ISAC BACKGROUND

Chairman Capito, Ranking Member Meeks, and members of the Subcommittee, my name is Gregory T. Garcia. I serve as Advisor to the Financial Services Information Sharing & Analysis Center (FS-ISAC). I want to thank you for this opportunity to address the Financial Institutions and Consumer Credit Subcommittee on the important issue of "Data Security: Examining Efforts to Protect Americans' Financial Information"**.** I appear before you today on behalf of FS-ISAC President Bill Nelson, who is on international travel and regrets his inability to take part in this proceeding.

The FS-ISAC was formed in 1999 in response to the 1998 Presidential Decision Directive 63 (PDD 63), which called for the public and private sectors to work together to address cyber threats to the nation's critical infrastructures. After 9/11, and in response to Homeland Security Presidential Directive 7 (and its 2013 successor, Presidential Policy Directive 21) 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 4,500 organizations including commercial banks and credit unions of all sizes, brokerage firms, insurance companies,

payments processors, and 24 trade associations representing virtually all of the U.S. financial services sector.

FS-ISAC PROGRAMS AND OPERATIONS – A MODEL FOR OTHER SECTORS

In light of the recent breach revelations against major retailers, this hearing puts a timely emphasis on the need to consider how commercial and critical infrastructure sectors can prevent such attacks from happening in the future.

Since its founding, the FS-ISAC's operations and culture of trusted collaboration have evolved into what we believe is a successful model for how other industry sectors can organize themselves around this security imperative. 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 share threat, vulnerability and incident information in a non-attributable and trusted manner. The FS-ISAC provides a formal structure for valuable and actionable information to be shared amongst members, the sector, and its industry and government partners, which ultimately benefits 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 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;

- operation of email listservs supporting attributable information exchange by various special interest groups including the Financial Services Sector Coordinating Council (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;
- participation in various cyber exercises such as those conducted by DHS (Cyber Storm I, II, and III) and support for FSSCC exercises such as CyberFIRE
- development of risk mitigation best practices, threat viewpoints and toolkits, and preparation of cyber security briefings and white papers;
- administration of Subject Matter Expert (SME) committees including the Threat Intelligence Committee and Business Resilience Committee, which: provide in-depth analyses of risks to the sector, conduct technical, business and operational impact

assessments; determine the sector's cyber and physical threat level; and, recommend mitigation and remediation strategies and tactics;

- special projects to address specific risk issues such as the Account Takeover Task Force
- 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 organizations, including small to medium sized regional financial services firms, on threats, risks and best practices.

FS-ISAC GOVERNMENT PARTNERSHIPS

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.

For example, in partnership with DHS, FS-ISAC two years ago 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. Our presence on the NCCIC floor has enhanced situational awareness and information sharing between the financial services sector and the government, and there are numerous examples of success to illustrate this.

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 NCCIC 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 distributed denial of service (DDOS) attacks on the financial sector in late 2012 and early 2013 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 its 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.

FS-ISAC INDUSTRY PARTNERSHIPS

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 HSPD 7 and its successor PPD-21. 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.

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.

In addition, several membership subgroups meet regularly with their own circles of trust to share information, including: the Insurance Risk Council (IRC); the Community Institution Council (CIC) with hundreds of members from community banks and credit unions; and the Community Institution Toolkit Working Group with a mission to develop a framework and series of best

practices to protect community institutions. This includes a mentoring program to assist community institutions just getting started with an IT security staff.

One operation that has achieved measurable results is our partnership with Microsoft, with whom we twice collaborated over the last 3 years to identify and take down sophisticated "botnet" operations stealing from financial services companies and their customers. A botnet is in effect a network of computers ("bots") that have been hijacked by cyber criminals who are able to steal financial credentials such as account numbers, passwords and user ID's. Because the cyber criminals were using Microsoft's infrastructure, such as their email and web servers, to deliver malware to financial customers' computers, several financial sector organizations including FS-ISAC and Microsoft were together able to share information about the source and techniques of the attacks, and work under a court order with law enforcement to cut off the "command and control" of the so-called "bot herders". This succeeded in ending this particular criminal ring's operations and disinfecting millions of computers in collaboration with internet service providers.

The FS-ISAC also works very closely with the other critical infrastructure sectors on an ISAC to ISAC basis as well as through the National Council of ISACs. Information about threats, incidents and best practices is shared daily among the ISACs via ISAC analyst calls, and a cross-sector information sharing platform. The ISACs also come together during a crisis to coordinate information and mitigations as applicable.

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.

FS-ISAC AUTOMATED THREAT INTELLIGENCE STRATEGY

While trust relationships in any sensitive activity such as cyber information sharing are essential to a successful risk management strategy, we also recognize that "human-to-human" effort can be too slow when threats and attacks are happening at internet speed. For this reason, FS-ISAC has embarked on a substantial initiative to engage more "machine-to-machine" threat intelligence exchange in a way that will more quickly inform our financial infrastructure front line operators, and aid their preventive and incident response decision making.

Over the last 18 months, we've worked with members and other industry organizations to design the industry's first Cyber Threat Intelligence Repository to automate threat intelligence sharing for our members. A first of its kind, this solution collects, analyzes, prioritizes and shares threat information in near real-time within our sector. We are well on our way to delivering the first phases of this project, are investing heavily in development resources and have a compelling multi-year roadmap that will transform how threat information is shared.

Already, initial testing with open intelligence sources has collected a total of 6 million indicators. Version 1.0 was released to pilot users last year and Version 2.0 is expected to be released later in 2014 and will include capabilities like a federated sharing model with many local repositories

as well as actionable intelligence down to a security controls level. We are working with vendors and other ISACs to extend the capability into other sectors.

Typically the time associated with chasing down any specific threat indicator is substantial. Our goal with this automation solution is to help our industry increase the speed, scale and accuracy of information sharing and accelerate time to resolution. This solution removes a huge burden of work for both large and small financial organizations, including those that rely on third parties for monitoring and incident response. With dozens of members participating in our first phase, we expect this automated solution to be a 'go to' resource to speed incident response across thousands of organizations in many countries within the next few years.

This concludes our written statement for the record. Thank you again for this opportunity to present this testimony and I look forward to your questions.