

TESTIMONY OF

GREG GARCIA

**PARTNERSHIP EXECUTIVE
for
CYBERSECURITY AND IDENTITY MANAGEMENT**

BANK OF AMERICA

Before the

HOUSE FINANCIAL SERVICES

FINANCIAL INSTITUTIONS AND CONSUMER CREDIT SUBCOMMITTEE

WASHINGTON, DC

SEPTEMBER 14, 2011

Introduction

Chairman Capito, Ranking Member Maloney, and distinguished Members of the Committee, I am Greg Garcia, Partnership Executive for Cybersecurity and Identity Management within Bank of America's Global Technology & Operations (GT&O) organization. Thank you for inviting us to share our approach to cyber security challenges facing our bank and the financial sector as a whole. My role is to coordinate Bank of America's external public private partnerships as they relate to cybersecurity and identity management so that we ensure a coherent strategy, better operationalize what we learn in the broader community, and maximize our contributions to the security of the cyber ecosystem to reduce overall risk.

Bank of America is one of the world's largest financial institutions, serving individual consumers, small- and middle-market businesses and large corporations with a full range of banking, investing, asset management and other financial and risk management products and services. The company provides unmatched convenience in the United States, serving approximately 58 million consumer and small business relationships with approximately 5,700 retail banking offices and approximately 17,800 ATMs and award-winning online banking with 30 million active users. Bank of America is among the world's leading wealth management companies and is a global leader in corporate and investment banking and trading across a broad range of asset classes, serving corporations, governments, institutions and individuals around the world. Bank of America offers industry-leading support to approximately 4 million small business owners through a suite of innovative, easy-to-use online products and services. The company serves clients through operations in more than 40 countries.

My background and contributions in cybersecurity over the past decade complement Bank of America's proactive and aggressive strategy. I was honored to have served as the nation's first Assistant Secretary for Cyber Security and Communications at the U.S. Department of Homeland Security from 2006-2008. I also had the privilege of serving as a staff member of the House Science Committee from 2001-2003 where I assisted Chairman Sherwood Boehlert in shepherding enactment of the Cyber Security Research and Development Act of 2002. Other cyber security partnership and policy roles on behalf of the technology sector have given me a unique cross-sectoral view of the challenges and opportunities from both an industry and government perspective.

We commend the committee for holding this hearing today to discuss the important issue of cybersecurity. My testimony will provide an overview of the current cybersecurity threat environment; how Bank of America manages security to protect its enterprise, customers, and shareholders; and how we partner with the rest of the financial sector, other industry sectors and the government to mitigate the risks associated with those threats.

Overview of the Threat Environment

The global financial system operates on a vast network of information and communications technology, both wired and wireless. Trillions of dollars in transactions per day flow across this network globally, from online banking and deposits, loans and credit card payments, large commercial transactions, to making payroll, raising capital and issuing debt, and securities trading, among many other services. It is our responsibility to ensure the smooth and uninterrupted delivery of those services wherever we do business around the world and to secure the data and networks that enable them and prevent unauthorized access that could lead to fraud, identity theft, data loss, or system downtime. Bank of

America's information technology infrastructure not only enables the provision of financial services, but it also guards, defends and protects those services and the data our customers entrust to Bank of America. Cyber access and the potential to disrupt these flows make the financial sector a target in the context of all threats.

It is important to note that while motivations for cyber attack differ, many of their techniques are the same, but at different levels of sophistication. We see "joy-riding", in which individuals simply want to make mischief; there are cyber criminals and criminal rings that are in it for the money, whether dealing in the credit card black market, account takeover schemes, fraudulent payments or ATM "skimming"; and there are more sophisticated threats from well organized "hacktivists" and nation states motivated to steal sensitive, strategic, or intellectual property information, disrupt services, deface websites and cause fear, loss of confidence and reputational damage.

While our emphasis has been primarily on the middle spectrum of threats – to protect our customers from fraud and identity theft, over the past few years there has been an emerging threat of greater sophistication and stealth that keeps us on alert 24x7x365.

How Bank of America Addresses the Cyber Threat

At Bank of America we are laser focused on cybersecurity. In discussing how we manage cyber security, it is useful to break it down into two interrelated components: our customer facing policies and activities, and our enterprise security.

Customer Security

Of primary importance to us is securing our customer financial information, and we deliver a range of services to secure transactions and keep our consumer customers whole. For example:

ShopSafe®

A free service that lets customers shop online without sharing their real credit number. Each time an online purchase is made, ShopSafe conveniently creates a temporary card number.

Fraud monitoring

Total Security Protection is free and automatically offered on Bank of America consumer credit and debit cards. It monitors how and where customer cards are being used. Our security systems analyze millions of transactions a day looking for patterns to help identify and stop fraud and identity theft.

Identity theft assistance

Bank of America is committed to helping victims of identity theft. We also offer the services of ITAC (Identity Theft Assistance Center) to help with identity theft recovery, prevention and education.

#1-rated safety features

Our customer safety features have ranked #1 for 5 years in a row by Javelin Strategy & Research, the nation's leading provider of research on financial institutions.

\$0 Liability Guarantee

Should any unauthorized purchases originate from Online Banking, we reimburse customer losses when reported within a reasonable time.

Secure technology

Our fraud prevention and security systems protect customers with the latest encryption technology and secured email communication.

We also offer our customers many tips online about what they can do to protect themselves. In particular, “phishing” remains one of the most widely used and effective attack methods by cyber criminals and hackers. Targeted emails that look legitimate but trick receivers into clicking on malicious links or entering personal information are difficult to prevent, and consumers, small businesses, large businesses and governments, are all at risk and must take appropriate precautions through awareness, training, up-to-date technology and strong security practices.

Enterprise Security

Our customer facing security strength relies on many of the policies and capabilities that protect and enable our broader enterprise. And at an enterprise level, we are concerned not just for our customers and employees, but for the protection of critical, nonpublic data, intellectual property, and operational availability and continuity. It is in all of these areas that we work very closely with our regulators to ensure we apply, maintain and constantly measure all the necessary security controls across the enterprise.

Fundamentally, our cybersecurity program is based on a combination of people, process and technology.

Across the company, all of our employees receive annual training on the importance of information protection, the policies and methods the bank uses, and the responsibilities of every user.

We have an information security team of advanced technology experts who have past careers in law enforcement, the military, security and high technology innovation. And we’re constantly looking to increase the pipeline of new talent.

We operate under detailed, rigorous information security policies, with a program designed to protect the security and confidentiality of customer and client information, from acquisition to use and storage to disposal.

Finally, we invest in and deploy leading-edge technology to secure data in movement and at rest. Where specific technology needs are not available off the shelf we often design and implement our own. Bank of America holds at least 140 patents in security technology so that we can deploy tools that meet our often unique requirements in a highly scalable way.

In addition, our security policy has the support and attention at the highest levels of the company. Bank of America’s Board of Directors approves the bank’s information security policy and programs, and the board is kept informed on the overall status of our information security program.

Our information security program is also subject to ongoing regulatory oversight and examination. Each of our business and support units has an executive accountable for information security, and a team of experienced associates to help implement policies, standards and baselines.

Increasing Our Investment

As an enterprise strategy, our security framework is organized along the 5 pillars of a structured cyber security operating model: Our goal is to: Deter, Prevent, Protect, Respond and Recover.

To describe each one briefly:

Deter: Discourage attacks through improved treaties, laws and increased enforcement

Prevent: Reduce incidents by better anticipating threats and addressing critical vulnerabilities

Protect: Protect our business systems through integrated controls across the stack: access, applications, information and infrastructure

Respond: Mitigate incidents through a proactive monitoring and agile incident response capability

Recover: Conduct forensics on events, work with investigations, and capture lessons learned to improve our security posture

We are investing heavily in developing a progressive standard of practice across those 5 pillars that is commensurate with the financial industry's status as critical national infrastructure. We believe that as companies across the financial sector and other critical sectors adopt the same structured methodology for managing against the sophisticated and evolving range of threats we face, we will collectively be able to stay ahead of the cyber criminals, hackers and other adversaries.

Partnership is Key to Cybersecurity Management

A critical element of a mature cyber security program is an investment in partnerships and collaboration. A mature partnership program can contribute outcomes to all elements of "people, process and technology" as well as the five pillars of a cybersecurity operating model, both within the walls of the company and externally for the broader good of the community. At Bank of America, we are bolstering our partnerships and collaboration to gain the broadest view of the threat landscape and innovative solutions, and we are sharing information and best practices so that we can collectively get smarter and better at protecting assets and critical information.

For example, among many others, we are coordinating and supporting partnerships such as the Financial Services Sector Coordinating Council, the Financial Services Information Sharing and Analysis Center (FS-ISAC), the Department of Homeland Security's cybersecurity entities and law enforcement partners globally. We consider these partnerships within the sector and across the cyber ecosystem to be essential elements of our ability to protect our customers, investors and shareholders from fraud, identity theft, cyber attack and business disruption. We treat every partnership as an opportunity to either improve our own internal security capabilities or an opportunity to extend our expertise and situational awareness to other partners.

The bottom line is: No one entity has all the information; it takes teamwork to bring all the pieces together to complete the picture.

Development of the Critical Infrastructure Partnership Model

This model of partnership has its official roots in a 2003 presidential directive – Homeland Security Presidential Directive (HSPD) 7. HSPD 7 set forth the imperative that “critical infrastructure” industry sectors are strongly encouraged to self-organize around a mission to identify and measure cyber and physical threats and vulnerabilities across the sector and work together with interdependent stakeholders such as other industries and government to mitigate those vulnerabilities.

HSPD 7 established a structure – now known as the National Infrastructure Protection Plan, or “NIPP” - that assigned sector specific agencies or “SSA’s” to each organized sector to work in partnership to address current and emerging issues. In the case of financial services and the Financial Services Sector Coordinating Council which is described below, the U.S. Department of Treasury is the assigned SSA.

In addition to these more formal public private partnerships, Bank of America participates actively in a large number of other industry to industry, company to company, and company to government efforts to quite simply get better at what we do – to exchange actionable intelligence, to adopt and share best practices, and to develop longer-term policy and strategic approaches to collectively strengthen the security of the ecosystem in which we all operate. This program is well founded on the understanding that we are all interconnected, interdependent and in this together.

The following summarize just a few of the many collaborations and initiatives that Bank of America contributes to and leverages to bolster our security posture and that of the broader ecosystem:

Industry to Government

Financial Services Sector Coordinating Council (FSSCC)

The Financial Services Sector Coordinating Council is a group of more than 45 private-sector firms and financial trade associations that reinforces the financial sector’s resilience against threats and all hazards to the nation’s financial infrastructure. Formed in 2002, FSSCC works with the Department of Treasury, which has direct responsibility for infrastructure protection and homeland security efforts for the financial services sector, while also serving under the overall guidance of the Department for Homeland Security.

I serve as co-chair of the FSSCC Cyber Security Committee where, among other activities, we are leading the effort to develop a financial sector annex to the National Cyber Incident Response Plan so that we have a uniform and coherent set of procedures for aligning sector-wide and national response to a cyber incident of significant impact.

For additional detail on the FSSCC’s perspective on cybersecurity, I refer the Committee to the April 15, 2011 testimony of FSSCC Chair Jane Carlin before the Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies of the House Homeland Security Committee.

Financial Services Information Sharing and Analysis Center (FS-ISAC)

The industry forum for collaboration on critical security threats facing the financial services sector. Bank of America serves on the FS-ISAC Board of Directors and its Threat Intelligence Committee.

Taken together, the FSSCC and the FS-ISAC serve as the primary financial industry policy and operational components under the NIPP partnership model. Both the FSSCC and the FS-ISAC maintain

a strategic role through information sharing and collaboration among stakeholders (e.g., Federal agencies infrastructure providers, and other financial services firms), education and awareness, preparedness planning, issuance of guidelines/ good practices, and developing mitigation/protection strategies against threats, incidents, and vulnerabilities. The FSSCC and FS-ISAC also maintain a cross sector coordination role based on established relationships. In this capacity, they are responsible for mobilizing interaction with critical external partners and agencies to support accurate situational awareness and resource support requirements (to and from the FS Sector and its constituents).

Financial and Banking Information Infrastructure Committee (FBIIC)

As the government partner to the FSSCC, the FBIIC is 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. Treasury's Assistant Secretary for Financial Institutions chairs the committee. The FSSCC and FBIIC hold a joint meeting semi-annually.

National Cyber Forensics Training Academy (NCFTA)

The NCFTA functions as a conduit between private industry and law enforcement with a core mission to identify, mitigate and neutralize cyber crime. Bank of America is deploying bank personnel to serve on the NCFTA on a rotational basis.

National Cybersecurity and Communications Integration Center (NCCIC) and the Unified Coordination Group (UCG)

The NCCIC provides an integrated incident response facility to mitigate risks that could disrupt or degrade critical information technology functions and services, while allowing for flexibility in handling traditional voice and more modern data networks. The NCCIC was created at the recommendation of the National Security Telecommunications Advisory Committee, the Government Accountability Office and a joint industry-government working group, which together emphasized the need for collocation, integration, and interoperability among existing cyber and communications incident response mechanisms. Bank of America and the financial sector are represented on the NCCIC watch floor by the FS-ISAC.

Cyber UCG

The Cyber UCG is an interagency and inter-organizational body that incorporates public and private sector officials ensuring unity of coordination and the facilitation of rapid collaboration in response to cyber events of national significance. It has roles and responsibilities during steady state and cyber incidents under the National Cyber Incident Response Plan. As co-chair of the FSSCC Cyber Security Committee, I serve on the UCG.

Department of Homeland Security U.S. Computer Emergency Readiness Team (US-CERT)

US-CERT leads efforts to improve the Nation's cybersecurity posture, coordinates cyber information sharing, and proactively manages cyber risks to the Nation while protecting the constitutional rights of Americans. Bank of America, the FS-ISAC and many financial institutions exchange information with US-CERT on an ongoing basis, and the relationship is maturing.

Cross Sector Cyber Security Working Group

The Cross-Sector Cybersecurity Working Group (CSCSWG), founded by the Department of Homeland Security, serves as a forum to bring government and the private sector together to collaboratively address risk across the critical infrastructure sectors. This cross-sector perspective facilitates the sharing of perspectives and knowledge about various cybersecurity concerns, such as common vulnerabilities

and protective measures, and leverages functional cyber expertise in a comprehensive forum. Bank of America serves as the financial services representative to the CSCSWG.

Government Information Sharing Framework (GISF)

The GISF is an information sharing agreement between FS-ISAC, DHS and the Department of Defense for the purpose of sharing timely, accurate, and actionable warnings of physical, operational, and cyber threats or attacks on the national financial services infrastructure.

Electronic Crimes Task Force

The ECTF network brings together federal, state and local law enforcement, as well as prosecutors, private industry and academia, for common purpose of prevention, detection, mitigation and aggressive investigation of attacks on our nation's financial and critical infrastructures. Bank of America associates participate in various ECTF events across the country throughout the year.

InfraGard

InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. InfraGard Chapters are geographically linked with FBI Field Office territories. Bank of America associates are members of and participate in various InfraGard events across the country throughout the year.

Industry to Industry

Bank of America Cyber Collaboration Program

Bank of America actively seeks out other like-minded companies that similarly find value in establishing more intimate and trusted information sharing relationships to exchange data on threats, vulnerabilities, incidents and response efforts. We have nearly 2 dozen individual partnerships with companies from within the sector and outside the sector. These more informal relationships help us not only get better and smarter now, but the fact that we are exchanging business cards now rather than when an incident occurs means we have already established a level of preparedness that could not have been achieved in isolation. The benefits from these partnerships just in the past 12 months have yielded measurable results in dollar value and improved situational awareness and preparedness.

BITS

A division of the Financial Services Roundtable, BITS was formed in 1996 by the CEOs of member institutions to foster the growth and development of electronic financial services and e-commerce for the benefit of financial institutions and their customers. BITS works to sustain consumer confidence and trust by ensuring the security, privacy and integrity of financial transactions. Bank of America serves on the Executive and Advisory Boards of BITS as well on its as numerous subject matter working groups.

Identity Theft Assistance Center

ITAC, the Identity Theft Assistance Center, is the leading consumer advocate on identity fraud and the financial services industry's identity management solution center. An affiliate of The Financial Services Roundtable, ITAC is supported by the industry as a free service for our customers. Since 2004, ITAC has helped tens of thousands of consumers restore their identity. Bank of America has served on the ITAC Board and as its chair.

National Cyber Security Alliance

NCSA's mission is to educate and therefore empower a digital society to use the Internet safely and securely at home, work, and school, protecting the technology individuals' use, the networks they connect to, and our shared digital assets. Bank of America serves on the board of NCSA.

Cyber Campaigns

Participation in Cyber Exercises and Crisis Playbooks

Bank of America has participated in multiple financial services exercises testing various perceived vulnerabilities and establishing follow-up actions as a result of lessons learned. Significant tests were run to evaluate sector preparedness related to social engineering attacks, payment processing attacks, and communication during a crisis. In particular, the 2009 Cyber Financial Industry and Regulators Exercise (CyberFIRE) and Cyber Attack against Payment Processes (CAPP) exercise were jointly executed by the FSSCC, FS-ISAC, and included many FBIIC members, the U.S. Secret Service, the Federal Bureau of Investigation (FBI), DHS, and more than 800 individual participants. Members of the FSSCC are also planning to participate later this fall in an exercise of our ability as a sector to respond to a cyber incident of national significance, testing the Financial Services annex (currently in development) to the National Cyber Incident Response Plan.

National Cyber Security Awareness Month

National Cyber Security Awareness Month (NCSAM), conducted every October since 2004, is an annual awareness-raising effort that seeks to encourage everyone to protect their networks and our nation's critical cyber infrastructure. Bank of America supports NCSAM with activities and messaging aimed internally at employees and at our millions of customers and all consumers to raise awareness about how we protect information and assets and what every individual can do to protect their own corner of cyberspace. Central to the theme is that cyber security is a shared challenge and a shared responsibility.

Stop.Think.Connect

The Stop.Think.Connect. (STC) Campaign launched in October 2010 in conjunction with National Cybersecurity Awareness Month. STC is part of a public awareness campaign effort among Federal and State governments, industry, and non-profit organizations to promote safe online behavior and practices.

National Initiative for Cybersecurity Education (NICE)

Launched by the Obama Administration last year, NICE is a national campaign to promote cybersecurity awareness and digital literacy across industry, government and academia, and to build a digital workforce for the 21st century. Bank of America supports this effort and is exploring opportunities to contribute.

Conclusion

In conclusion Chairwoman Capito, I am proud to say that Bank of America is focusing a tremendous amount of resources and energy to staying ahead of the cyber security challenge. We have come a long way as an institution and as a sector. We are developing new tools, processes and expertise for meeting the challenge of cyber crime. We are making the necessary investments and taking our regulatory compliance obligations seriously, just as we are working proactively to do more than is required by regulation. Our ultimate goal is protect our customers, our shareholders, and our enterprise.

We also have seen our working relationships with government and industry partners evolve and mature for the good in partnership initiatives that are not subject to – indeed cannot be effectively subject to – regulatory compliance. While we recognize the importance of uniform regulatory standards to set a minimum bar across the sector and hold us accountable, we also recognize that the evolving nature of cybercrime requires a resilient and evolving partnership structure that is responsive and adaptable in the kind of real time dynamic that a regulatory structure is insufficient to ensure.

But of course, this is not to say we are where we need to be. We have more work to do. We are constantly seeking ways to build trust relationships and information sharing partnerships with government that transcend concerns about secret-level classification and business sensitive information. Most acknowledge that actionable threat information that is not shared is useless information. The more we develop and populate those institutional structures such as the FS-ISAC, FSSCC, the NCCIC and others, that are designed to facilitate broad situational awareness, a common operational picture, best practices and real-time incident response, the better and more secure will be our financial infrastructure, our economy and the homeland.

Final Recommendations

As mentioned earlier, we have much to do, both in industry and in government. Let me close by making a few recommendations for additional measures we can take together:

Government can:

- Enact stronger laws against hacking with continued enhancement of enforcement capabilities
- Prioritize long-term, basic research into cyber “grand challenges” not typically undertaken by the private sector
- Simplify and streamline multiple, simultaneous and sometimes conflicting government efforts to “solve” the problem

We all can:



- Urge and support industry efforts to take cyber responsibility within the current critical infrastructure partnership structure
- Better share technology and R&D between the private sector and government labs
- Invest more in education, training and awareness
- Develop more collaborative operations and open channels for faster, better information sharing and actionable intelligence
- Increase coordination internationally
- Continue to build consumer awareness

Madam Chairman, that concludes my testimony. Thank you.

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: |
| Greg Garcia | Bank of America |
| 3. Business Address and telephone number:  | |
| 4. Have <u>you</u> 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 <u>organizations you are representing</u> 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? |
| <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No | <input type="checkbox"/> Yes <input checked="" type="checkbox"/> 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: | |

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