Kevin F. Streff
Associate Professor of Information Assurance – Dakota State University
Director – National Center for the Protection of the Financial Infrastructure
Faculty – University of Wisconsin, Graduate School of Banking

Written Testimony of
Kevin F. Streff
Associate Professor of Information Assurance
Dakota State University Information Assurance Center

Before the
United State Senate
Committee on the Banking, Housing, and Urban Affairs

Hearing on:
Cybersecurity and Data Governance in the Financial Services Sector
June 21, 2011

WITNESS STATEMENT

Kevin Streff, Ph.D. is an Associate Professor at Dakota State University in Madison, SD and performs information assurance research in the financial services sector, with a particular focus on understanding the security issues of small and medium-sized financial institutions. Dr. Streff works with the banking associations all across the United States to understand rural banking vulnerabilities and solutions to mitigate. Dr. Streff has over 20 years of experience working in insurance, banking and credit operations.

Professor Streff teaches managerial elements of information assurance, including risk management, security policy, information security management systems, disaster recovery, business continuity planning, and incident response planning. Dr. Streff has numerous publications in peer-reviewed journals such *Journal of Information Warfare, Journal of Computer Information Systems, Journal of Autonomic and Trusted Computing Journal of Computing Sciences in Colleges,* and *Issues in Information Systems.* He is the recipient of over $4 million in grants and contracts over the past five years. Dr. Streff serves on several conference program committees, including International Conference on Information Warfare, and Information Assurance, Network, Database and Software Security. Dr. Streff was session chair at several prestigious systems science conferences over the past several years, including organizing and chairing a mini-track on Information Assurance and Computer Security at the International Conference on Information Warfare. Dr. Streff was a keynote speaker at several national security conferences, presented over one hundred times at state, regional and national banking conferences, and published in both *America's Banker* and *Community Banker.*

Dr. Streff is Director of the National Center for the Protection of the Financial Infrastructure, which is missioned to fortify the resiliency of the electronic critical infrastructure of the financial sector. He is also founder and President of InfraGard South Dakota, an outreach program to promote the protection of critical infrastructure in SD, ND and MN. He is also founder and managing partner of Secure Banking Solutions, an information security consulting firm focused on improving information security in community banks and credit unions in the U.S. SBS assists over 400 small and medium-sized financial institutions in 44 states with their information security and compliance needs. Dr. Streff is on faculty at the Graduate School of Banking at the University of Wisconsin where he helped develop the recently launched Bank Technology Management School.

Introduction

Chairman Johnson, Ranking Member Shelby and Members of the Senate Committee on Banking, Housing, and Urban Affairs, I am pleased to appear before you today on behalf of the National Center for the Protection of the Financial Infrastructure (NCPFI) at Dakota State University to share our views on the current state of data/cyber security as relating to small and medium-sized financial institutions and what they do well/or not so well. These comments will be made within the context of the President's recent proposal regarding The Comprehensive National Cybersecurity Initiative (CNCI) which is vital to increase America's detection, planning, and response capabilities as it relates to attacks on our nation's critical electronic infrastructure.

My name is Dr. Kevin Streff and I am Director of NCPFI from Madison, South Dakota. The NCPFI's mission is to "*advance the security and safety of the nation's financial infrastructure through research, education and outreach.*" Started in 2009, the NCPFI has worked with academia, the private sector and government to bring attention to the homeland security, critical infrastructure and cyber risks associated with the electronic infrastructure which runs the financial industry. The work of NCPFI is funded by the State of South Dakota, NSF, DoD, DHS, Cheneega Logistics and other federal and private entities. We appreciate the invitation to appear before the committee on this important issue, and thank the committee for their leadership and foresight in dealing with these issues before a crisis state.

Background

Every day cyber criminals are scanning government, academic and industry networks for non-public information they can steal. Large corporations have in-house I.T. departments to protect their systems and customer data. Small and medium-size financial institutions (SMFIs) and small and medium-sized businesses (SMEs) businesses do not.

Furthermore, Presidential Decision Directive 63 deemed the financial services sector a critical cyber infrastructure which America depends upon every day; however, small and medium-sized financial institutions are under heavy cyber attack and lack the requisite skills and resources to combat these cyber threats. Without an understanding of the risks each institution incurs and a capability to deploy solutions to mitigates these risks, it is unlikely decision-makers in these SMFIs will win the battle against cyber thieves.

In this testimony, we will review the current legal and regulatory environment in which small and medium-sized financial institutions must operate (SECTION I), discuss security and privacy experiences in the financial services sector that have impacted small and medium-sized financial institutions (SECTION II), and discuss how the Administration's cybersecurity bill will interact with existing regulation and affect SMFIs. Some additional

ideas and concerns are noted for the President to consider as it relates to the Comprehensive National Cybersecurity Initiative (SECTION III).

SECTION I. Overview of Current Data Protection Laws, Regulation, and Policy Statements in Financial Services

A. Financial Industries Modernization Act of 1999 (Gramm-Leach-Bliley)

The Gramm-Leach-Bliley Act (GLBA) 15 U.S.C. §§ 6801-6810 (disclosure of personal financial information), 15 U.S.C. §§ 6821-6827 (fraudulent access) repealed the Glass-Steagall Act of 1932, and is part of broader legislation which removes barriers to banks engaging in a wider scope of financial services. GLBA applies to financial institutions' use and disclosure of nonpublic financial information about consumers. Section 501(b) requires administrative, technical, and physical safeguards to protect covered nonpublic personal information. Federal banking agencies have published Interagency Guidelines Establishing Standards for Information Security for financial institutions subject to their jurisdiction. 66 Fed. Reg. 8616 (February 1, 2001) and 69 Fed. Reg. 77610 (December 28, 2004). The Guidelines are published by each agency in the Code of Federal Regulations, including:

- Federal Deposit Insurance Corporation, 12 C.F.R., Part 364, App. B;
- Office of the Comptroller of the Currency, 12 C.F.R., Part 30, App. B;
- Board of Governors of the Federal Reserve System, 12 C.F.R., Part 208, App. D-2 and Part 225, App. F;
- Office of Thrift Supervision,12 C.F.R., Part 570, App. B; and
- National Credit Union Administration, 12 C.F.R., Part 748

The Federal Trade Commission has issued a final rule, Standards for Safeguarding Customer Information, 16 C.F.R. Part 314, and the Securities and Exchange Commission promulgated Regulation S-P: Privacy of Consumer Financial Information, 17 C.F.R. Part 248 for financial institutions within their respective jurisdictions.

GLBA requires financial institutions to disclose privacy notices to all customers, and provide a means for customers to opt out of the sharing of information with third parties. However, it is § 6801, "Protection of Non-Public Personal Information" that contains the most sweeping provisions, by requiring each regulatory agency to:"Establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards to:

1) insure the security and confidentiality of customer records and information;
2) protect against any anticipated threats or hazards to the security or integrity of such records; and
3) protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."

These requirements mean that all financial institutions must develop, document and operationalize a comprehensive information security program. The administrative, technical and physical safeguards are sweeping and expansively interpreted by federal and state regulators to include everything from the physical security of buildings, data security at service providers, to the types of authentication used during online banking sessions. Each bank must report annually to the Board of Directors on the status of the information security program.

The Guidelines require a risk assessment designed to: "identify reasonably foreseeable internal and external threats" to customer information, assess the likelihood and potential damage of these threats, and to assess the effectiveness of a wide variety of information security controls. GLBA is significant because of the extensive requirements and regulatory oversight imposed upon the financial industry and carried out by federal and state regulators.

The Interagency Guidelines Establishing Information Security Standards includes a provision to implement a notification program to notify customers, regulators and law enforcement officials of data breaches. The regulations promulgated to implement the response program have been codified as Supplement A to Appendix B of 12 C.F.R. Pt. 30. "[E]very financial institution should . . . develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems" regardless of whether the breach occurs in the financial institution's own computer systems or those hosted by third party service providers.

B. Bank Secrecy Act

In 1970, Congress passed the Bank Secrecy Act (BSA). BSA requires U.S. financial institutions to assist U.S. government agencies to detect and prevent money laundering. The act specifically requires financial institutions to keep records of cash purchases of negotiable instruments, file reports of cash transactions exceeding daily aggregate amounts of $10,000, and to report suspicious activity that might signify money laundering, tax evasion, or other criminal activities. Several anti-money laundering acts, including provisions in title III of the USA PATRIOT Act, have been enacted up to the present to amend the BSA. (See 31 USC 5311-5330 and 31 CFR Chapter X (formerly 31 CFR Part 103). The documents filed by financial institutions under BSA are used by law enforcement agencies, both domestic and international to identify, detect and deter money laundering whether it is in furtherance of a criminal enterprise, terrorism, tax evasion or other unlawful activity.

C. USA PATRIOT Act

The USA PATRIOT Act (Patriot Act), enacted by President George W. Bush in 2001, reduced restrictions on law enforcement agencies' ability to search telephone, e-mail communications, medical, financial, and other records; eased restrictions on foreign intelligence gathering within the United States; expanded the Secretary of the Treasury's authority to regulate financial transactions. Section 314(b) of the USA PATRIOT Act permits

financial institutions, upon providing notice to the US Department of the Treasury, to share information with one another in order to identify and report to the federal government activities that may involve money laundering or terrorist activity. More specifically, the BSA authorizes the Treasury to require financial institutions to maintain records of personal financial transactions that "have a high degree of usefulness in criminal, tax and regulatory investigations and proceedings" and to report "suspicious transaction relevant to a possible violation of law or regulation." Again, because The Patriot Act deals with governmental, rather than private, intrusion into customer privacy, it is outside the scope of this discussion.

D. Identify Theft Red Flags Rule

The Identify Theft Red Flags Rule (Red Flags Rule) requires financial institutions to implement a written Identity Theft Prevention Program that is designed to detect the warning signs of identity theft in their daily operations. By identifying red flags in advance, financial institutions will be better able to identify suspicious patterns that may arise, and take steps to prevent a red flag from escalating into identity theft.

A financial institutions' Identify Theft Red Flags Program should enable the organization to:

1) identify relevant patterns, practices, and specific forms of activity — the "red flags" — that signal possible identity theft;
2) incorporate business practices to detect red flags;
3) detail appropriate response to any red flags you detect to prevent and mitigate identity theft; and
4) be updated periodically to reflect changes in risks from identity theft.

Shortly thereafter, regulatory agencies began issuing examination procedures to assist financial institutions in implementing the Identity Theft Red Flags, Address Discrepancies, and Change of Address Regulations, reflecting the requirements of Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003.

E. Sarbanes Oxley Act of 2002

The Sarbanes-Oxley Act of 2002 (SOX) was enacted to restore confidence in the integrity of the financial reporting process at publicly traded companies, influenced by high profile accounting scandals at firms such as Enron and WorldCom. However, each publically-traded financial institution that is affected by the Sarbanes-Oxley Act has some level of reliance on automated information systems to process, store and transact the data that is the basis of financial reports, and SOX requires financial institutions to consider the IT security controls that are in place to promote the confidentiality, integrity, and accuracy of this data. SOX states that specific attention should be given to the controls that act to secure the corporate network, prevent unauthorized access to systems and data, and ensure data integrity and availability in the case of a disaster or other disruption of service. Also, each system that interfaces with critical financial reporting data should have validation controls such as edit and limit checks built-in to further minimize the likelihood of data inaccuracy.

F. Payment Card Industry Standard

The Payment Card Industry Security Standards Council is an industry group formed to manage and maintain the Data Security Standard (DSS), which was created by the Council to ensure the security of payment card information. Sensitive data is involved in card transactions, including account number, cardholder name, expiration date, and PIN. The intent of the PCI DSS is to ensure that card transactions occurring across multiple private and public networks are subject to end-to-end transaction security. The payment card industry consists of Card Issuers, Card Holders, Merchants, Acquirers, and Card Associations. From the collection of card information at a point of sale, transmission through the merchant's systems to the acquiring bank's systems, then on to the card issuer, the PCI DSS requirements attempt to ensure sufficient security safeguards are in place on the card data from beginning to the end of a card transaction. Enforcement of the security requirements is done by the card associations and through a certification process of each association member. The certification process is carried out by Qualified Security Assessors (QSA), who audit systems and networks to ensure the mandatory controls are in place. Certification does not guarantee that an organization will not suffer a data breach, as several PCI-certified organizations have suffered data breach incidents.

G. Regulatory Guidance

The Federal Financial Institutions Examination Council (FFIEC) is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the federal financial regulatory agencies." As such, the FFIEC publishes the "Information Technology Examination Handbook", which is used by banking regulators in executing examinations of information technology and systems of financial institutions. The Handbook includes ten (10) booklets, one of which is the "Information Security Booklet, which provides a baseline against which a financial institution subject to GLBA can be evaluated. The "Information Security Booklet" attempts to provide a high level, comprehensive overview of the major types of information security controls one would necessarily expect to be operating effectively within a financial institution. The types of controls are not limited in applicability to just financial institutions, and are derived from the same principles underpinning all major information security frameworks.

Further, each regulatory agency produces further guidance for their financial institutions. For example, FDIC FIL-103-2005 Authentication in an Internet Banking Environment established single factor authentication (such as a userid and password) as necessary but insufficient in logging users onto electronic banking systems, requiring the use of an additional factor to establish identity. This FIL involved industry investing in multi-factor authentication solutions, vendors leveraging these solutions in their systems, and financial institutions operationalizing them. A second example is Corporate Credit Union Guidance Letter 2010-01 dated July 8, 2010 entitled "Confidentiality and Protection of Sensitive

Data". The OCC occasionally issues security bulletins, while FRB issues Supervision and Regulation Letters (an example includes the April 4, 2011 release of SR11-7 entitled "Guidance on Model Risk Management"). The FDIC also authored the Information Technology Officer's Questionnaire, whereby an officer of the financial institution must document, attest and sign to 71 questions in five information security categories: risk assessment, operations security and risk management, audit/independent review program, disaster recovery and business continuity management, and vendor management and service provider oversight. This questionnaire is periodically updated and released as the security/technology landscape changes.

H. Third Party Self Regulation

Small and medium-sized financial institutions depend heavily on hardware and software vendors for nearly all banking products. In addition, many of these vendors become service providers offering to host and manage their products for the SMFI. The service provider industry has experienced several significant data breaches affecting the financial services industry in the past several years, including ChoicePoint (163,000 data records), TJX (100 million data records), Heartland Payment Systems (130 million data records), etc. When companies choose to outsource data processing to a third party, they typically perform information security due diligence on the third party to understand how the data will be protected. A very common standard for third party assurance has been the SAS 70; however, the SSAE16 standard is replacing the SAS70 and moving more to an attestation model (similar to independent financial audits). BITS, a non-profit organization, has also attempted to standardize the assessment of third-party service providers by developing the "BITS Framework for Managing Technology Risk for Service Provider Relationships", which includes two tools to help service providers in control selection and implementation. The first tool is called Standardized Information Gathering Questionnaire (SIG), which is a template based on the ISO 27002 standard, and specifies the expected information security controls that should be in place at the service provider organization. The second tool is the Agreed Upon Procedures (AUP), which serve as testing procedures meant to validate the effectiveness of the controls specified in the SIG.

In summary, SMFIs operate in an increasingly complex regulatory environment, with community banks regulated aggressively and credit unions a little less. This regulation is necessary, but causes significant financial, resource, and other issues in SMFIs who must leverage technology to compete. Increasing regulation is likely as additional technologies are deployed and the cybersecurity stakes grow, but all increased regulation must be tempered with a SMFI's ability to stay in business and meet the needs of their customers. The majority of SMFIs are in rural locations and may be the only local funding source for a community.

SECTION II. Data Security and Privacy Issues in the Financial Sector

Over 500 million data records have been breached since the ChoicePoint breach of 2005:

534,232,379 RECORDS BREACHED
from 2,539 DATA BREACHES made public since 2005
Source: PrivacyRights.Org

How many of these data records and breaches involved the financial sector?

247,808,947 RECORDS BREACHED
from 386 DATA BREACHES made public since 2005
Source: PrivacyRights.Org

U.S. SMFIs and SMEs are important as millions of consumers depend upon community banks, credit unions, accounting firms, tax-preparation firms, investment offices, insurance agencies, and the like. When issues in the financial system exist, confidence erodes and consumers are left paralyzed wondering what to do. Similarly, as Deborah Platt Majoras Chairman of the Federal Trade Commission stated at High-Tech World, 2005, "when data breaches or an infrastructure attack occurs, customer confidence is eroded and spending is held close to the vest." The margin for error in SMEs is relatively small, and one such data breach can shut the doors on viable businesses.

Further, if terrorists would target these vulnerable SMFIs or SMEs, they would find a soft underbelly of relatively under-protected targets. A plethora of nefarious activities are then possible, including stealing and selling customer data, extorting ransoms, "owning" the computer, making these systems unavailable, etc. Stated directly, these activities could be enough to put a SME or SMFI out of business. The reality is that while it is nearly impossible to challenge the importance of SMEs and SMFIs in the U.S., it is equally difficult to convince security experts that either are prepared to protect their critical systems, important customer information and do their part to battle against the war on terror.

The federal government identified banking and finance as a critical infrastructure that requires protection, yet most of the attention is paid to the large financial institutions. SMFIs and SMEs store and transmit much non-public data, with limited resources to fend off a well-equipped, well-funded enemy. A recent survey of bank executives called out this very fact. When asked what their top technology concern was over the next two years, risk management and compliance topped the list. A black market drives insiders and hackers to steal information because of its value. An article in InformationWeek highlighted the problem: "More electronic records were exposed in 2009 than in the previous four years combined and most of those breaches - - nine out of 10 - - could be easily avoided with basic preventative controls consistently applied." SMFIs and SMEs have a wealth of non-public, sensitive data that cyber thieves are targeting with increasing regularity.

Cyber security is a broad and pervasive issue leading to at least two national issues: critical information protection and identify theft. Critical information protection is guarding our electronic infrastructures as an issue of national security. Incidents are classified, but it is well established that China and others are interested in technology disruptions that affect the United States' ability to conduct commerce. President Obama is on record stating that the United States is not prepared for CIP and despite national budget pressures is creating a division within the national government (Cyber Command) to begin focusing on this new national issue.

Identity theft is the fastest growing crime in America and the risks of not protecting such information can be catastrophic to SMEs in communities. When identities of good U.S. citizens are stolen by cyber criminals, the good citizen can be humiliated, lack good credit, and spend significant time and money in an attempt to partially restore their good name. Information risk management is the first step in resolving the broad and pervasive issues of CIP and Identity Theft. Public Law 111-24 was signed by the President establishing a Small Business Information Security Task Force to look into the issue. The Ponemon Institute, an independent research firm which conducts research on privacy, data protection, and information security policy, calculates in 2010 businesses paid an average of $202 per compromised record (Ponemon Institute). This equates to $101,000 for a SME with 500 customer records. SMEs who cannot securely manage customer data from identity theft face either closure or acquisition by larger metropolitan-based organizations that have in-house IT security.

Cybercrime is having enormous real consequences, which holds the potential to cripple businesses and services," says Steven Chabinsky, deputy assistant director of the FBI's Cyber Division. He continues, "Cyber security is not a nice thing to have for American businesses, it is critical to their survival." Cyber criminals began by hacking phone systems and government networks, and expanded their operations to penetrate large organizations over the past ten years. Today, cyber criminals are expanding again, this time to target and thieve small and medium-sized businesses. This issue is magnified in America where there is very limited information security expertise, offering unprotected businesses as easy targets for organized cyber criminals with financial motivation.

Electronic Crimes in Commercial Banking with Small and Medium-Sized Financial Institutions

Organized cyber-gangs are increasingly preying on small and medium-sized companies in the U.S., setting off a multimillion-dollar online crime wave and grave concerns that critical infrastructure government and business depends upon each day may become compromised. It appears there are three contributing reasons they are growing so fast: (1) Low threat of arrest in these "safe havens", (2) High payout for the crime, and (3) Victim sharing data on these attacks has been minimal. The attacks are amazingly simple and the amount of money taken, information stolen, or infrastructure compromised is concerning. SMEs do not know how to protect themselves. In some cases where credit card theft has occurred, they have had to shut down because they lost the ability to process

credit cards. Small businesses are being affected greatly by poor security practices. It is not a risk issue, but rather an issue of survival.

Cyber criminals view SMEs as easy targets without the resources or knowledge to fend them off or prosecute them if caught. Consequently, cyber criminals are turning their attention to perceived easy targets in America. Identity thieves can cost SMFIs and SMEs their basic ability to stay in business (i.e., financial losses, bad publicity of a data breach, significant costs of recovering from a data breach, inability to process credit cards, etc.). Even if there were no measurable damages to customers, the notification costs alone can put the SME out of business. One-third of companies said that a significant security breach could put their company out of business. Information Week reports data breaches cost an average of $202 per record breached, with $139 of this cost attributable to lost businesses as a result of the breach. Many SMEs are having a difficult time in this recession, and even the smallest of distractions can be devastating. SMFIs, too, are struggling with increased assessment fees, limited deposits, limited fee-based products, and overwhelming compliance expenses, which is spurring closures and consolidation in the industry.

While SMFIs have struggled to keep pace with hackers, the SMEs have clearly fallen short. In a study I completed of SMEs, 7 out of 10 SMEs lack at least one basic security control, such as a firewall, antivirus software, strong passwords, or basic security awareness for staff. Many SMEs simply lack the basic security most of us expect on our home PCs. As evidence, I provide a statistic. I am founder of Secure Banking Solutions, LLC, a security/privacy firm focused on information security and compliance for SMFIs. As such, SBS is regularly hired to conduct penetration tests on SMFIs where SBS security personnel run (after authorization) hacking tools to see if they can break into the bank's network and systems. SBS is effective in 27% of SMFIs (meaning that SBS personnel were able to gain access to information and systems they were not authorized for). To contrast, SBS is effective in 98% of SME penetration tests. The question is "why?" and the answer is simple: SMFIs are regulated to a certain level of security that is far superior to a SME. Most anyone can download hacking tools from the Internet, point them at a SME, and gain unauthorized access, zombie the machine, steal data, or disrupt the environment.

Traditionally, most SMEs have viewed security as a problem faced solely by large organizations, government agencies, or online intensive operations as large organizations possess large, prolific information targets and are generally more regulated than SMEs. However, cyber criminals are finding easy targets in SMEs that have limited security. The financial gain for cyber thieves targeting SMEs is obviously less than that of large organizations, but they can be hacked in significantly less time with little to no effort. Tools to conduct these attacks on SMEs are freely downloadable from the Internet.

Howard Schmidt, the White House Cyber Security Coordinator, recently stated:

> "Around 85% of cyber attacks are now targeting small businesses."
>
> - SOURCE: Howard Schmidt, White House

SMEs are targeted as they are easy prey and do not have the expertise to ward off attacks. Generally, SMEs with less than $10 million in revenue will be a big market over the last 18 months. Most small businesses (86%) do not have staff dedicated to IT security and only 28% have an Internet security policy, on which only 35% train employees.

The FBI recently issued an alert to all SMFIs and SMEs of this issue. These attacks are working because of a lack of security controls at the SME whereby fraudulent transactions are directly taken out of commercial customer's bank accounts.

> *The Ponemon Institute reported in 2010 that 58% of small businesses had a security loss due to online banking fraud, and nearly one third of these small businesses experienced a loss of more than $5,000.*

At a basic level, the attacker compromises the SME network due to a lack of basic security controls, and proceeds to install malware to steal login credentials. After receiving the login credentials (User ID and password), the hacker simply logs onto the SMFI network, escalates privileges as necessary, and steals data or money. Figure 1 outlines a typical corporate account take-over attack.

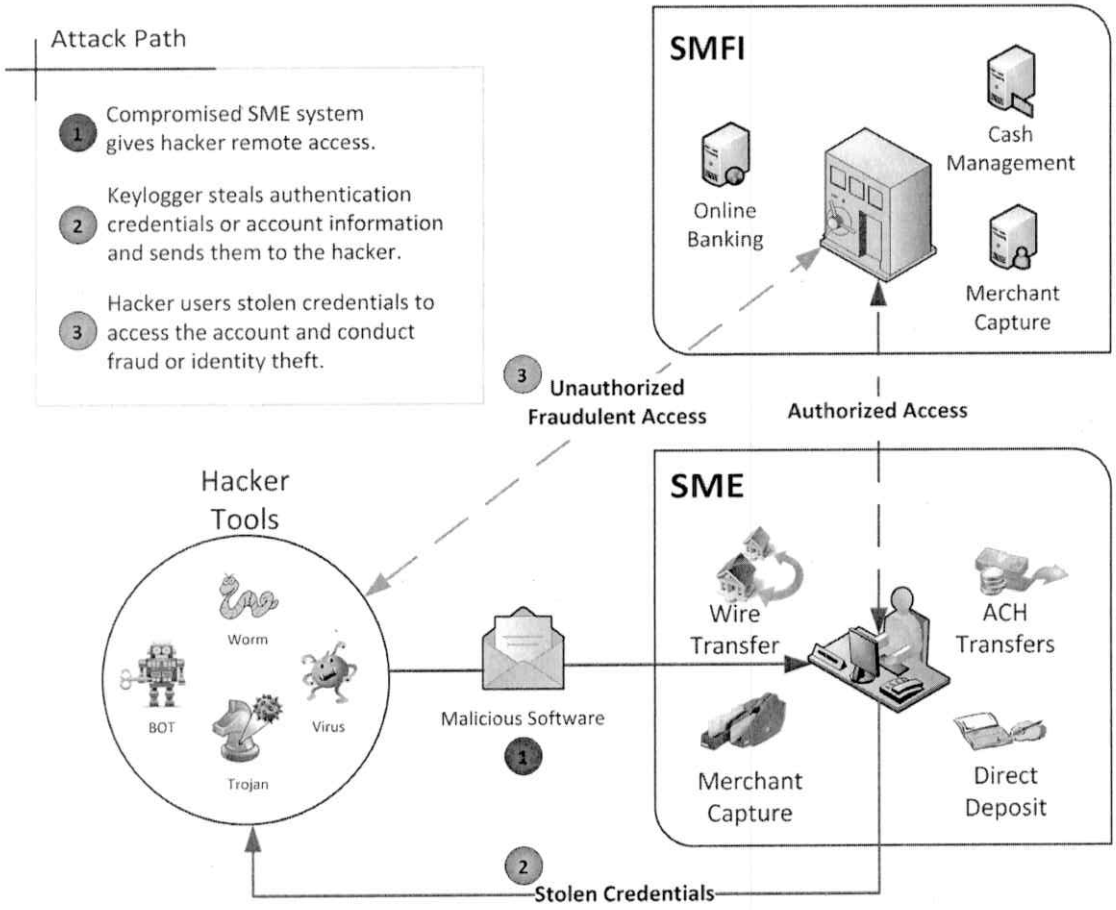

Figure 1 – Anatomy of a Corporate Account Takeover Attack

SMFIs today lack an ability to understand which businesses represent risk to these new-wave attacks. SMEs are the target of these attacks and must understand how to prevent them from occurring.

The current generation of banking products work because of technology, including remote deposit capture, Internet banking, mobile banking, item imaging, and on-line account origination. However, USA Today quoted Amrit Williams, a chief technology officer, "Any organization that cannot survive a sudden five- or six-figure loss should consider shunning Internet banking altogether." Banking security analyst at Gartner, Avivah Litan, tells acquaintances that run small businesses to switch from commercial online accounts to an individual consumer account to take advantage of consumer-protection laws under Regulation E, because 57% of the time SMEs are stuck paying some or 100% of the bill. Regulation E protection does not exist for corporate accounts; consequently, SMEs have no legal protection if commercial account fraud occurs. Unlike individual accounts that protect individual consumers to a maximum exposure of $50 if fraud occurs, corporate accounts have no such protection. The SME can sue or go to the media, but these approaches likely do not get the money back and drains even more resources from SME which are typically resource challenged.

New fees levied by financial institutions on paper-based banking products are likely to push more small businesses into banking online, whether or not they are aware of and prepared for the types of sophisticated cyber-attacks that have cost organizations tens of millions of dollars in recent months. Gartner analysts say banks should not be pushing more businesses into online banking without adequately informing them of the risks. The reality is that the perfect small-business storm is occurring: heaving attacks are already beginning and significantly more technology will be deployed by SMFIs over the next five years, creating a fertile cyber ground for terrorists to create problems.

The 2011 Business Banking Trust Study provides insights from the SME perspective on the pervasiveness of fraud, the state of security at banks and businesses, and the impact fraud has on businesses' relationships with their banks. The 2011 study found:

1) 56% of businesses reported experiencing payments fraud or attempted payments fraud in the last 12 months;

2) in 78% of fraud cases, banks failed to catch fraud involving the illegal transfer of funds or other nefarious practices such as information identity theft; and

3) 38% of respondents said they access their company's banking accounts from mobile devices including smart phones and tablet PCs like the iPad, compared to only 23% in 2010.

The survey data reveals that despite a year of increased public attention to the impact that corporate account takeover has had on businesses and banks, the industry has barely moved the needle in addressing the problem.
The National Cyber Security Alliance has conducted a new 2011 National Small Business

Security Study with Visa Inc. to analyze small business' cyber security practices and attitudes. Results include:

- Only 43% of small and medium-sized businesses have a plan in place to respond to the loss of customer data, such as credit or debit card information or personal identifying data.
- 47% of employees at SMEs report receiving no security training.
- 53% of all small business owners believe the high cost in time and money to fully secure their business is not justified by the threat.
- 57% are NOT confident that their business is protected against cyber thieves.

In summary, there is little doubt that the financial services sector is under attack for identity theft and infrastructure corruption motives. There is also little double that the small and medium-sized businesses and financial institutions are coming in the cross-hairs of cyber criminals. The number and significance of data breaches and attacks is significant, and only a comprehensive approach that looks at all infrastructure holistically (from government, academia, and industry) can ward off these terrorists.

SECTION III. Analysis of Administration's Cybersecurity Bill on the Financial Industry, with Particular Attention to Small and Medium-Sized Financial Institutions

This section will summarize the state of cybersecurity protection and compliance in both SMFIs and SMEs and discuss the Administration's Cybersecurity Bill and its impact on SMFIs.

1. Technology, Cybersecurity, and Compliance Challenges are Outpacing the Capabilities of SMFIs and SMEs.

Technology is advancing faster than SMFIs' ability to respond with appropriate mitigating security controls. For example, the use of cell phone cameras to take a picture of a check as the basis for making an electronic deposit into an account, or P2P, B2B or B2P transactions by cell phone create security exposures for which there are inadequate controls to prevent fraud. Fortunately, most SMFIs are not first adopters of new technology, but rather prefer to wait until the systems become more seasoned before embracing newer technologies. Moreover, the timeline between introduction, implementation and adoption of new technology by consumers continues to shrink. Just ten years ago, data processing was the buzz where computers were essentially back-off equipment designed to promote efficiency in the financial institution. Today, technology is front-line differentiators for banks, with customers demanding to use mobile technologies and social media to conduct banking commerce. The risk profile ten years ago included someone breaking into the bank's computer to get customer records, while the risk profile today is someone breaking into cell phones, laptops, mobile devices, social media sites, merchants who deposit checks via imaging systems, service providers who host critical banking applications, websites which

validate flood plains or credit bureau information, etc. This list goes on and on regarding the technologies typical in a SMFI. The next generation of technologies will exponentially increase the risk profile because information and infrastructure will be further distributed, and not partitioned off by the walls of the bank. With the increase in outsourcing and the mounting risks of offshoring, requiring data centers to be located in the U.S. seems consistent with the goal of increasing our cybersecurity posture. Banks leverage Brinks trucks to secure the delivery of cash to their bank. The financial industry needs to devise "cyber Brinks trucks" to perform the same role in cyberspace.

The attack target at SMFIs is typically individual accounts and small and medium-sized business accounts (i.e., corporate accounts). For the most part, cyber crooks have used malicious software to infect those computers because the controls at small and medium-sized businesses (SMEs) are nonexistent or rudimentary at best – certainly not nearly as in-depth as even the smallest financial institutions. The PCI standards are clearly inadequate, and for the most part based on voluntary compliance and self-audit. Today, the best mitigation strategy seems to be to educate individuals and SMEs to the risks and controls that are essential to minimize the potential for major cyber loss or disruption. Moreover, we do not think it is appropriate or reasonable to shift the burden of loss from the person or organization that had inadequate controls in place to detect and deter cyber hacking attacks, to the financial institutions that process the withdrawals by the crooks, generally through ACH debits. The recent Experimental Metal Incorporated (EMI) vs. Comerica Bank decision is concerning to the small and medium-sized financial sector as it appears to increase SMFI responsibilities to information risk management of corporate accounts (even if the security attack occurred at the SME). Automated systems are necessary that help individuals and SMEs identify risks, controls and mitigation strategies. It would appear that SMFIs, which already conduct a bank I.T. risk assessment and a third party vendor assessment, will need to put in place a corporate account risk management program very shortly.

The mounting compliance drivers are beginning to take their toll on SMFIs around the country.

> *"The compliance burden continues to rise. We cannot discount the impact of using limited resources to combat cybersecurity risks when so much time, energy, and money are being spent today on operational compliance issues, training, and staff time."*
>
> Source: Daryll Lund, President and CEO, Community Bankers of Wisconsin

2. *SMFIs and SMEs Lack Sufficient Cybersecurity Resources.*

As we have discussed, cyber crime is now big business. There is every reason to believe that cyber crooks will continue to find ways to defeat controls and attempt to hack small and medium-sized businesses and high net worth individuals. To date, one of the most effective deterrents has been in educating customers, "know your customer" and placing per transaction and aggregate daily limits on ACH and wire transfers. Smaller financial

institutions are generally in a better position than large institutions to know their customers, enforcing lower transaction and aggregate limits, and placing more restrictive controls involving ACH and wire transfer controls. However, smaller financial institutions cannot afford to put in place the highly sophisticated equipment that the large financial institutions use to monitor data/cyber security exposures. Smaller financial institutions generally do not have the resources to continually put in place the most advanced security controls. However, the solution for the smaller financial institutions is to form strategic partnerships with organizations that have expertise and infrastructure to combat the latest cyber threats. This of course requires a system for procedural controls and continuous monitoring of vendors, more effective risk management tools honed to the unique needs of small and medium-sized financial institutions, and normative data to help decision-makers understand trends, anomalies and the like to support cost-effective information security spending.

In addition, SMFIs and SMEs typically lack information security staff. At a SMFI, a loan officer, head teller, VP of Operations, or I.T. staff are the usual candidates named Information Security Officer. We have yet to meet a SMFI Information Security Officer with a formal education in information protection. Bachelor, Masters, and Doctoral programs are available in Computer and Network Security, Information Security, Information Assurance, Homeland Security, and other derivatives of cybersecurity; yet, because demand simply outpaces supply, the SMFIs are left without qualified resources. Further, the Information Security Officer that is named typically wears four or five "hats" at the SMFI. Understanding emerging security threats, threat actors, vulnerabilities, and the like takes time and expertise, and cannot simply be assigned likely to existing staff.

Further, we applaud the President for inclusion of CNCI Initiative #8: Expand Cyber Education in his comprehensive strategy. While technology is vital to preventing, detecting and responding to security attacks, equally important are the people who determine security strategy, devise and operationalize security programs, and skillfully deploy the technologies that wall-off our critical infrastructures and information. We commend the federal government for starting the NSA/DHS Center of Academic Excellence in Information Assurance Education and Research Programs. The NSA/DHS partnership was formed in 2004 in response to the *President's National Strategy to Secure Cyberspace* of 2003. The CAE-R program was added in 2007 to encourage universities and students to pursue research, development and innovation in Information Assurance (cyber security). The program originally created by this partnership has continued to grow and become even more relevant and critical to U.S. national security today. 106 universities across the United States, located in 37 states, the District of Columbia and the Commonwealth of Puerto Rico, are now designated by NSA/DHS as National Centers of Academic Excellence in Information Education and/or Research. Qualified IA professionals from the National Security Agency, the Department of Homeland Security, and the Committee on National Security Systems review and assess applications. Universities designated as National Centers of Academic Excellence in Information Assurance are eligible to apply for scholarships and grants through both the Federal and Department of Defense Information Assurance Scholarship Programs. Graduates from Information Assurance programs at CAE institutions become the professional cyber security experts protecting national security

information systems, commercial networks and critical information infrastructure. These professionals are helping to meet the increasingly urgent needs of the U.S. government, industry, academia and research. Designation as a CAE/IAE or CAE-R is awarded for five academic years, after which the college or university must successfully reapply in order to retain the designation.

CAE2Y - National Centers of Academic Excellence in Information Assurance 2-Year Education
CAE/IAE- National Centers of Academic Excellence in Information Assurance Education
CAE-R - National Centers of Academic Excellence in Information Assurance Research

The CAE program is a huge success and the credit goes to the thought leaders in the federal government that anticipated the cybersecurity issue and the resource shortage it would create. We advise the President to consider expanding this program with funding so that more educational, research, and outreach capacity is created to serve the needs of government and industry (companies small and large). We advise the expansion of the scholarship for service program (SFS) at NSA, DoD, and NSF, including expanding the number of scholarships and the places scholarship students can pay back their scholarship. For example, can we make it possible for a SFS student to complete his/her service at a critical infrastructure owned and operated by the private sector? NSA and DHS alike deserve a lot of credit for operationalizing this successful program, and we suggest Administration considers leveraging this investment as a starting point for CNCI Initiative #8: Expand Cyber Education, rather than creating a new mousetrap and starting over.

More effective training and educational programs must be made available to SMFI and SME industry personnel. One such example is the program in Bank Technology Management that Kirby Davidson at the Graduate School of Banking at the University of Wisconsin has developed. This program launched in April, 2011 and was capped at 50 students (which filled in two weeks). The program is a blend of technology and security honed specifically to the community banking audience. The program includes 12 hours of "ethical hacking", where students download and execute common hacking tools so they understand what tools the adversary has in the arsenal.

> "As the technologies used to support banking become more important, and as banking products demand more sophisticated technology solutions, it's vital that IT professionals and information security officers understand how to effectively choose, deploy and lead the use of current and emerging technologies to meet business goals and regulatory requirements. It's also critical that IT professionals understand key steps that they can initiate at their bank to proactively protect vital customer information from cyber and network attacks. All of this, and more, is included in the new Bank Technology Management School offered through the Graduate School of Banking at the University of Wisconsin-Madison. The school uses a mix of lectures, small group discussions and interactive computer simulation labs that allow students to work with learned concepts in real-world situations."
>
> - *Kirby Davidson, President & CEO, Graduate School of Banking, Madison, WI*

Small and medium-sized financial institutions lack qualified security experts to protect their interests. SMFIs simply cannot afford or do not have access to security specialists. Many certified and qualified security officers command six-figure salaries, inconsistent with the resources available at SMFIs. Most of these certified, qualified individuals live in urban areas, again inconsistent with the demands of SMFIs. Universities, community colleges and trade schools can do even more to create programs that produce security experts who can work into the SMFI environment. As the federal government continues hiring of cyber experts, this will likely put even more pressure on the supply of such experts needed in SMFIs.

3. *Digital Infrastructure is Infrastructure*

When an ice storm occurs in North Dakota, icing up power lines and taking out power, the region is paralyzed until power is restored. It can sometimes take weeks and months to complete this task, depending upon the tenacity of Mother Nature. What would happen to these financial institutions, our economy, and our consumer confidence level if malicious nation-states disrupted our power instead of an ice storm? How long would it take for power to be restored on infrastructure dating back centuries?

Power, water, transportation, and the Internet (just to name a few) are all required to conduct banking commerce. While SMFIs are required to devise business continuity, incident response, and pandemic preparedness plans, no SMFI could operate if essential infrastructure we all depend up (such as the power grid) was compromised. The job is much larger than any one SMFI. The CNCI's major goals to establish a front line of defense against today's immediate threats and to defend again a full spectrum of (future) threats is so massive that only the Federal government could take this on. However, to the degree major and minor changes are needed at SMFIs or SMEs, we urge the Administration to consider this infrastructure and fund it. There needs to be a mindset shift away from industry paying for everything in this infrastructure (because they created it and are the users of it) to some shared cost model. If this infrastructure is truly a matter of national security then the Federal government has a funding responsibility. Just as tanks, planes, and weapons are funded to protect our interests, we urge the Administration to consider their financial responsibilities as it relates to this vital electronic infrastructure. President Obama said it best:

> *We count on computer networks to deliver our oil and gas, our power and our water. We rely on them for public transportation and air traffic control... But just as we failed in the past to invest in our physical infrastructure – our roads, our bridges and rails – we've failed to invest in the security of our digital infrastructure... This status quo is no longer acceptable – not when there's so much at stake. We can and we must do better.*
>
> *Source: President Obama, May 29, 2009*

Conclusion

Electronic banking is the future, and if SMFIs cannot understand and resource their technology and security requirements then they will likely be left behind. We agree with the White House's conclusion in their recent cyber security legislative proposal that, at least with respect to cyber terrorists, the vulnerability of the electricity grid poses one of the most severe exposures to our country's critical infrastructure. The fact that a computer programmer in another country could cause the partial or complete disruption of this nation's grid is, to say the least, extremely disturbing, but is beyond the scope and expertise of SMFIs to respond. However, small and medium-sized financial institutions need representation at the table, and we encourage the President to consider including this voice as small and medium-sized financial institutions and businesses are the majority, not the minority, of American businesses.

Thank you for the opportunity to participate in this important and timely hearing. The National Center for the Protection of the Financial Infrastructure and Dakota State University look forward to working with all stakeholders to operationalize the President's vision of a safe electronic infrastructure for all businesses to use. We applaud the President in making cybersecurity an Administration priority, and concur with the President's comments that the "cyber threat is one of the most serious economic and national security challenges we face as a nation." To make an impact, policy must change, resource allocation must change, and a more comprehensive approach must be deployed.

We want to thank you again for this opportunity to appear before you.