For Release Upon Delivery

10:00 a.m., December 10, 2014

TESTIMONY OF

VALERIE ABEND

SENIOR CRITICAL INFRASTRUCTURE OFFICER

OFFICE OF THE COMPTROLLER OF THE CURRENCY

Before the

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

UNITED STATES SENATE

December 10, 2014

Statement Required by 12 U.S.C. § 250:
The views expressed herein are those of the Office of the Comptroller of the Currency and do not necessarily represent the views of the President.

Chairman Johnson, Ranking Member Crapo, and members of the Committee, thank you for the opportunity to appear before you today to discuss the important issue of cybersecurity, including our efforts to address cyber threats and vulnerabilities and coordinate information sharing for the benefit of the banking industry, regulatory community, and the financial system overall. There are few issues more important to the OCC and to our country's economic and national security than the risks posed by cyber attacks.

My name is Valerie Abend, and I serve as the OCC's Senior Critical Infrastructure Officer. In collaboration with the agency's supervisory divisions, I lead the agency's cybersecurity and resilience efforts for the national banks and federal savings institutions (referred to collectively as banks) that we supervise. I also currently chair the Federal Financial Institutions Examination Council's (FFIEC) Cybersecurity and Critical Infrastructure Working Group (CCIWG). I have more than 20 years of private and public sector experience in the cybersecurity and critical infrastructure fields. My testimony today will discuss the cybersecurity initiatives the OCC and the FFIEC have taken, the avenues in place to share cybersecurity information, and recommendations where legislation may be helpful to enhance information sharing among financial institutions.

I. Background

We live in a world of rapidly changing technology that impacts financial institutions both in terms of the products and services they offer and the risks that they face. We are long past the time when retail payments occur through face-to-face cash transactions or with paper checks. Instead, consumers increasingly use their cellphones to deposit checks, pay bills, and make purchases at the mall. For most consumers, electronic-based payment mechanisms and electronic banking are a routine part of life, and they may not give much thought to what goes on

behind the scenes to provide the speed, convenience, and security in our payment and settlement systems today. What they may not know is the vast amount of information technology that institutions necessarily rely upon to make this convenience possible. To continue to improve efficiency and offer new products and services, institutions are rapidly adopting new information technology. From connecting personal devices such as tablets and phones to their networks and launching new mobile banking applications, to using cloud computing, banks are adopting new technologies and establishing new connections. Collectively, this dependence on technology and the data that financial institutions create along with the funds they maintain and transmit every day make financial institutions attractive targets for hackers. Unfortunately, new vulnerabilities in both hardware and software are identified daily, making it difficult to protect systems from cyber attacks.

Furthermore, networks that serve the financial industry are global, which means hackers can target banks and other systems from almost anywhere in the world. Financial institutions today face threats from insiders and individuals acting alone, and from international networks of well-organized nation-states, criminals, and so-called "hacktivists" who use cyber attacks to raise awareness and support for their political or social causes.

As the risks evolve, financial institutions must continue to prepare for cyber attacks and how they will identify, mitigate, and respond to them – and regulators must take steps to ensure that they do so.

II. OCC Supervisory Framework and Initiatives

The OCC's supervisory framework is built around four key elements. The first is the OCC's ongoing monitoring and information sharing with other regulators, government agencies, and banks with respect to emerging threats and changes to the risk landscape. The second is the

OCC's development and continual refinement of standards and guidance that set forth supervisory expectations as to how banks and third-party service providers can best safeguard bank and bank customer information. The third key component is the agency's communication of these supervisory expectations to examiners and bank management through training and other forms of communication. The final component of the framework is the implementation of policy through on-site examination of banks and critical third-party service providers to assess their compliance with our supervisory expectations to ensure that they are appropriately managing risks, and when necessary, directing them to take corrective action. Each of these elements is described below.

1) Ongoing Monitoring, Assessment, and Information Sharing

Ongoing monitoring and timely information sharing across the financial sector regarding cybersecurity issues including threats, vulnerabilities and risk mitigation tactics, is a crucial component of our efforts. The OCC conveys risk management practices to banks, including strategies to identify, prevent, mitigate and respond to attacks. During and following a cyber attack, the OCC plays an important role in evaluating the impacts from the attack to determine if they pose a material risk to bank systems and bank customer information. At the same time, the OCC evaluates whether the institutions involved are taking appropriate and timely corrective action.

We encourage banks and service providers to participate with regulators in forums to learn about specific cyber threats in a timely manner. For example, the OCC is a member of both the Financial and Banking Information Infrastructure Committee (FBIIC) and the Financial Services Information Sharing and Analysis Center (FS-ISAC), which are among the financial

sector's public-private partnerships that provide information regarding cyber threats and various means to improve the security and resilience of the financial sector.

OCC examiners also maintain ongoing communication with the banks they supervise. This includes information related to pervasive vulnerabilities and incidents that may cause significant disruption to systems, facilities, or business processes at the bank, its operating subsidiary or affiliate, or at a third-party service provider. Examiners monitor the bank's response to incidents and to reports on threats and vulnerabilities and assess the level of impact and risk to customers, business operations, as well as any system-wide or downstream effects.

The OCC uses a number of mechanisms, based on the nature of the threat or vulnerability and the immediacy of potential impact, to communicate information that may pose a material risk to the banks we supervise. This includes providing examiners with instructions and messages to use in contacting bank management on specific wide-scale vulnerabilities and threats, the risks these may pose to the bank, and actions the bank should take to prevent, detect, and respond to a threat or vulnerability.

2) Supervisory Standards and Guidance

The banking sector is highly regulated and has been subject to stringent information security requirements for decades. The OCC has the authority to require the banks we regulate and their service providers to protect their own systems and bank customer data and to require banks to take steps to identify, prevent, and mitigate identity theft.

For example, following the 1999 enactment of the Gramm-Leach-Bliley Act, the OCC, in conjunction with the Federal Deposit Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System (FRB), and the National Credit Union Administration (NCUA), published enforceable information security guidelines that set forth standards for administrative,

technical, and physical safeguards that financial institutions must have to ensure the security and confidentiality of customer information. These interagency guidelines require banks to develop and implement formal information security programs that are tailored to a bank's assessment of the risks it faces, including internal and external threats to customer information and any method used to access, collect, store, use, transmit, protect, or dispose of the information. Given the evolving threat and technology environment, the guidelines require a bank's information security program to be dynamic – to continually adapt to address new threats, changes in technology, and new business arrangements. Since banks often depend upon service providers to conduct critical banking activities, the guidelines also address how banks must manage the risks associated with their service providers.

In addition, pursuant to section 114 of the FACT Act, the OCC, FRB, FDIC, NCUA, and the Federal Trade Commission, issued regulations in 2007 titled "Identity Theft Red Flags and Address Discrepancies." These rules require each financial institution and creditor to develop and implement a formal identity theft prevention program that includes policies and procedures for detecting, preventing, and mitigating identity theft in connection with account openings and existing accounts. A bank's program must include policies and procedures to identify, detect and respond to relevant indicators of identity theft, and must be updated periodically to reflect changes in risks to customers and to the institution from identity theft.

Over the years, the OCC on its own, and through the FFIEC, also has published guidance and handbooks that make clear our expectations about acceptable risk management processes and procedures for safeguarding information and managing information technology (IT) risks. This guidance addresses broad subjects such as information security, business continuity planning, and outsourcing technology services. It also focusses on specific areas of risks, such as

authentication of users in an Internet banking environment and effective software patch management. As noted below, this guidance is reviewed continually and updated to take into account evolving risks.

3) Examiner Training and Communicating Expectations

All entry-level OCC examiners receive training on information technology risk management within their first three years of employment. In addition, the OCC has examiners who specialize in IT. These examiners have specialized skills and experience to focus on information security and other technology risks inherent in bank operations. To help these specialists maintain their skills and knowledge, the OCC has an advanced IT training program. This is further augmented through webinars, in-person meetings, and formal and informal networking groups. When the OCC issues new guidance or updates existing guidance, we incorporate it into our training and develop communications so that our examiners can effectively implement these changes through the examination process.

Additionally, the OCC has taken steps to raise awareness of banks about the risks posed by cyber threats and vulnerabilities and to inform them of changes to supervisory expectations. This includes highlighting cybersecurity as an important operational risk that banks must pay close attention to through our public Semi-Annual Risk Perspective reports, releasing bulletins to the industry on topics such as distributed denial of service attacks, and hosting webinars, outreach meetings and roundtable discussions.

4) Onsite Examinations

As part of their ongoing supervision, OCC examiners assess the adequacy of the controls that protect customer information, and bank systems and information. The OCC and the other federal banking regulators also conduct joint examinations of major technology service providers that provide critical services to the banking sector.

Due to the complexity of the largest national banks, the OCC has resident IT examiners onsite who perform ongoing supervision of the banks' IT policies, procedures, and practices. OCC examiners also perform onsite IT examinations at smaller banks every twelve to eighteen months as part of their regular exam. Examiners also follow up on identified concerns or emerging cyber risks during quarterly communications with the banks they supervise, or on a more frequent basis depending on the nature of the concern or risk. The OCC uses information from bank examinations to inform our policies, training, and exam procedures. For example, through our exams, the OCC identified increasing risks and the need for additional guidance for banks on how to manage the complex risks posed by critical third-party relationships. As a result, in 2013, the OCC updated its Third-Party Relationship Risk Management Guidance, which incorporates important expectations for banks to evaluate their third parties' information security, incident response, and management of information systems, as well as the servicers' ability to assess, monitor, and mitigate risks posed by its subcontractors.

III. FFIEC Initiatives

The Comptroller currently chairs the FFIEC, an interagency body comprised of the principals of the five federal banking regulatory agencies – the OCC, the FRB, the FDIC, the NCUA, and the Consumer Financial Protection Bureau (CFPB) – and the FFIEC's State Liaison Committee. The FFIEC is empowered to prescribe uniform principles, standards, and report forms to promote uniformity in the supervision of financial institutions. One of the Council's top priorities is to strengthen institutions' resilience to cyber attacks. Last year, the Comptroller called for – and the Council members concurred in – the creation of the CCIWG to enhance communication among the FFIEC members and to build on existing efforts to strengthen the activities of other interagency and private sector groups with respect to cybersecurity.

The CCIWG serves as a liaison between the members of the FFIEC and the intelligence community, law enforcement, and the Department of Homeland Security (DHS) on issues related to cybersecurity and the protection of critical infrastructure. The working group is empowered to help the FFIEC members collaborate in establishing cyber-related examination policy, developing training programs, coordinating responses to cybersecurity incidents, and managing information-sharing efforts.

The working group has been quite active since its inception. Through its coordination and information sharing with intelligence, law enforcement, DHS, and the Department of the Treasury, the group has drafted several statements to institutions advising firms about the threats posed by ATM cashout schemes, distributed denial of service attacks, and widespread vulnerabilities such as Heartbleed and Shellshock.

One major initiative that the working group launched this summer was the Cybersecurity Assessment, which involved the pilot of a new cybersecurity examination work program at more than 500 diverse community institutions supervised by the OCC, FRB, FDIC, NCUA, and state regulatory agencies. The Cybersecurity Assessment evaluated the complexity of each institution's operating environment, focusing on such factors as the types of connections employed, products and services offered, and technologies used. It also assessed each institution's overall cybersecurity preparedness, with a focus on the following key areas: Risk Management and Oversight, Threat Intelligence and Collaboration, Cybersecurity Controls, External Dependency Management, and Cyber Incident Management and Resilience. The results of the assessment are instructive and will help FFIEC members make informed decisions about how they identify and prioritize actions to enhance the effectiveness of cybersecurity-related supervisory programs, guidance, and examiner training.

Preliminary findings that members agreed would be beneficial to share with institutions were released as *General Observations* and are available on the FFIEC's website.[1] This document highlights some high-level observations and provides questions that boards of directors and chief executive officers (CEOs) of financial institutions should consider when assessing their cybersecurity preparedness. For example, the document encourages institutions to routinely discuss cybersecurity issues in board and senior management meetings to help the financial institution set the tone from the top and build a strong security culture. It also encourages institutions to clearly define roles and responsibilities and assign accountability to identify, assess, and manage cybersecurity risks across the financial institution. While the institutions' leadership is responsible for cybersecurity risk management, employees are typically the first line of defense. As such, the FFIEC also encourages institutions to keep their training programs current and provide them more frequently.

Additionally, the document emphasizes that management should monitor and maintain sufficient awareness of cybersecurity threats and vulnerabilities to help ensure that financial institutions can evaluate and respond to emerging risks. To help build this capability, the FFIEC on behalf of its members issued the statement recommending that institutions of all sizes participate in the FS-ISAC to better understand the risks posed to their institution and to support their risk management program.

Institutions in the pilot assessment implement controls to impede unauthorized access to their systems and have tools in place to detect previously identified attacks. The *General Observations* document stresses that institutions should review and adjust controls when making changes to their IT environment, routinely scan networks for vulnerabilities and anomalous

[1] The FFIEC Cybersecurity Assessment, General Observations document can be accessed at http://www.ffiec.gov/press/PDF/FFIEC_Cybersecurity_Assessment_Observations.pdf

activity, test systems for potential exposure to cyber attacks, and remediate issues when identified. Similarly, the document highlights the importance of identifying the connections an institution has with third-party service providers and ensuring formal controls are in place to secure the ways these providers transmit, access, and store data.

Finally, while we found that institutions have procedures for notifying customers, regulators, and law enforcement when incidents affect sensitive customer information, the document emphasizes that institutions should strengthen their ability to address breaches that may occur by establishing and routinely testing incident response plans throughout the institution. This would include incorporating cyber-attack scenarios into business continuity plans and programs.

In addition to the Cybersecurity Assessment, the CCIWG has made strides in increasing financial institutions and examiners' awareness of cyber threats and vulnerabilities and the actions that management can take to mitigate these risks. During the past year, the working group led a webinar, "Executive Leadership of Cybersecurity" for which over 5,000 community institution CEOs registered, and conducted web-based trainings for over a thousand examiners on cybersecurity issues. Last month, concurrent with the release of the *General Observations* document, the FFIEC, on behalf of its members, released the *Cybersecurity Threat and Vulnerability Monitoring and Sharing Statement*.[2] The statement reiterated members' expectations that management monitor and maintain sufficient awareness of cybersecurity threat and vulnerability information in order to evaluate risk and respond accordingly. In addition, it reinforced the need for all institutions and their critical technology service providers to have appropriate methods for monitoring, sharing, and responding to threat and vulnerability

[2] The FFIEC Cybersecurity Threat and Vulnerability Monitoring and Sharing Statement can be accessed at http://www.ffiec.gov/press/PDF/FFIEC_Cybersecurity_Statement.pdf

information. In addition to recommending institutions to join FS-ISAC, the statement also listed additional government resources that are able to assist financial institutions with identifying and responding to cyber attacks.

IV. Cross Sector Cybersecurity Dependencies and Information Sharing

As noted earlier, ensuring appropriate information sharing is an essential component of the OCC's cybersecurity efforts. The OCC uses information sharing forums, relationships with government agencies, and the supervision process to acquire information on potential and confirmed cyber threats and attacks.

As a member of the FS-ISAC and through our work with the Treasury Department, we receive significant alerts that provide information related to cyber threats, attacks, and vulnerabilities. We also recognize the importance of maintaining relationships with the law enforcement and intelligence communities to share information and keep lines of communication open. The OCC is an active member of the FBIIC, created to improve coordination and communications among a broad array of financial regulators, and chaired by the Treasury Department. These efforts include monthly staff-level meetings and periodic meetings with agency principals. In addition, we attend classified briefings for FBIIC and support the collaborative initiatives of this sector-wide partnership.

The Financial Stability Oversight Council (FSOC) also provides a mechanism to promote collaborative efforts on a range of issues, including cybersecurity issues, and has set forth specific recommendations to advance cybersecurity efforts. The creation of the CCIWG, and some of its activities are directly responsive to the FSOC's recommendations. In its 2014 annual report, FSOC recommended that the Treasury Department continue to work with regulators, other appropriate government agencies, and private sector financial entities to develop the ability

to leverage insights from across the government and other sources to inform oversight of the financial sector and to assist institutions, market utilities, and service providers that may be targeted by cyber attacks. The FFIEC's aforementioned issuances are prime examples of responses to these recommendations. The FSOC also recommended that financial regulators continue their efforts to assess cyber-related vulnerabilities facing their regulated entities, identify gaps in oversight that may need to be addressed, and inform and raise awareness of cyber threats and attacks. As discussed earlier, the FFIEC's Cybersecurity Assessment responds to these recommendations.

The OCC and other banking agencies have a robust process for issuing standards and guidance and supervising the financial sector through our examinations. However, the resiliency of the financial sector is also dependent on other critical sectors, including the telecommunications and energy sectors, which do not operate under a comprehensive supervisory regime like financial institutions. The OCC strongly supports efforts to ensure other sectors have commensurate standards and improved transparency as it relates to the cybersecurity preparedness for these other sectors. In addition, the financial services industry and retailers have interdependencies. We have seen a number of attacks on large retailers in which credit card and other information from millions of consumers was compromised. In response, financial institutions compensate customers for fraudulent charges and replace credit and debit cards, and monitor account activity for fraud at significant cost. This is not easy for any bank, but the burden falls especially heavily upon community institutions. At a cost of $5 or more per card plus fraud related charges, the costs can escalate quickly. We would support efforts to even the playing field between banks and merchants to ensure that both contribute to efforts to make affected consumers whole.

The Treasury Department, as our Sector Specific Agency, has been leading efforts to work more closely with the government agencies responsible for overseeing these other sectors. The OCC supports these efforts and hopes they lead to more in-depth interactions between the financial sector and other sectors with which it closely interacts. For our part, the OCC is a member of a newly formed Cybersecurity Forum for Independent and Executive Branch Agencies. The Forum's objectives are to enhance communication, identify lessons learned, and develop a common understanding of cybersecurity activities through the sharing of best practices and exploring approaches to enhance cybersecurity protections.

V. Recommendations for Congressional Consideration

As we work to safeguard our financial system, we note some areas where Congressional action is necessary to provide parity among the parties impacted in cyber breaches that adversely affect consumers and to facilitate additional information sharing within the banking industry.

1) Parity for Retailers

The recent breaches at large retailers highlight the need for improved cybersecurity for merchants. Enhanced cybersecurity should apply to all industries where customer information is at risk. There should be consistent protections across all industries for securing financial transactions, customer information, and systems. Further, these protections should include appropriate responses to breaches when they do occur. As mentioned previously, when breaches occur in merchant systems, merchants should contribute to efforts to make affected consumers whole.

2) Industry Information Sharing

The OCC believes the existing statutory framework could be improved to encourage information sharing about cyber attacks among institutions. We believe that amending the USA

PATRIOT Act by creating a safe harbor to facilitate and promote the timely sharing of information among financial institutions concerning cybersecurity threats, cyber attacks, and data breaches would create incentives for enhanced information sharing, which would result in increased awareness of potential threats within the banking industry.

3) Other Legislative Proposals

The OCC has reviewed a number of legislative proposals that are pending in Congress to promote and facilitate information sharing concerning cyber threats and attacks among government agencies. The OCC generally supports such legislative initiatives. However, in the case of cyber threat information involving banks, the bills we have reviewed do not require or encourage the DHS, the Department of Justice, or other government agencies to share this information with the appropriate federal banking agency. The federal banking agencies need cyber threat information involving banks to ensure the safety and soundness of both individual banks and the broader financial system. Accordingly, we believe that legislative proposals designed to improve and promote cyber threat information sharing among government agencies should require other government agencies to share information related to banks with the federal banking agencies.

In addition, most legislative proposals designed to promote and facilitate cyber threat information sharing provide that the information shared may not be used for regulatory purposes. This provision could impede our ability to issue cybersecurity guidance or regulations, or to take action to correct deficiencies in cybersecurity risk management.

VI. Conclusion

We have high expectations for our supervised entities in the area of cybersecurity. Financial institutions of all types and sizes must remain vigilant to protect against and mitigate

cyber breaches, and we at the OCC will continue to support banks in this effort. To ensure we stay on top of the evolving threats to the financial services industry, the OCC is committed to refining our supervisory processes on an ongoing basis and to participating in public-private partnerships to help keep abreast of and respond to emerging threats.

The Comptroller has emphasized the importance of communication, collaboration, and cooperation in all aspects of our mission. Nowhere is such communication and collaboration more important than in the realm of cybersecurity, where the threat transcends agency jurisdictions and industry boundaries. Combatting cyber threats and protecting our economic security requires the government and industry to work together for the good of consumers, the industry, and the entire financial services sector.