Remarks by

Thomas J. Curry
Comptroller of the Currency

Before the

Exchequer Club
Washington, DC

September 18, 2013

Thank you, it's a pleasure to be here with you today. The Exchequer Club has always been an important forum for the exchange of ideas on financial issues, particularly in the area of bank regulation and legislation, and I will do my best today to make a contribution to that tradition.

Since taking office as Comptroller of the Currency, a lot of my time has been spent addressing issues stemming from the financial crisis. That's as it should be. Ensuring that our banks have sufficient capital to absorb losses in times of stress, curbing excesses in the securitization market, and restricting bank investment in hedge funds and private equity companies are all important steps that will protect not just banks and thrifts in times of future turbulence, but the financial system as a whole.

However, as important as it is to look back and deal with issues arising from the financial crisis, it is equally urgent that we look ahead and stay on top of emerging threats – some of which have the potential to be as destructive of the financial system as the excesses of the mortgage and securitization markets. The particular issue I have in mind, and the one I want to spend the rest of my time on today, involves the operational risk posed by cyberattacks.

Since the first "website" went live in 1991, the Internet has become home to 2.5 billion users worldwide, and it has changed the way we shop, socialize, and bank. Along with these very positive changes have come some significant concerns over the potential for systemic risk posed by cyberattacks. I can tell you that we at the OCC, and my counterparts at the other regulatory agencies as well, are taking cyber threats in all of their forms very seriously.

The denial of service attacks that began in 2012 and continue today drew the attention of our largest financial institutions. While they have been only minimally disruptive so far, we know that these types of attacks are just one of the many cyber threats that our financial system faces. The growing sophistication and frequency of cyberattacks is a cause for concern, not only because of the potential for disruption, but also because of the potential for destruction of the systems and information that support our banks. These risks, if unchecked, could threaten the reputation of our financial institutions as well as public confidence in the system.

The financial services industry isn't alone in facing the threat of cyberattacks. Almost every business sector, from newspapers to power utilities, faces similar threats. But the financial services industry is one of the more attractive targets for cyberattacks, and, unfortunately, the threat is growing, for several reasons.

First, hackers have easy access to the necessary tools and infrastructure. The global nature of the Internet means they can conduct their activity from almost anywhere, including in countries with regimes that, at worst, sponsor attacks and, at a minimum, act as criminal havens by turning a blind eye toward criminal behavior. To make matters worse, the cost of tools has dropped precipitously. In fact, in some cases, they can be obtained for free, along with how-to videos. As a result, financial institutions today face cyber threats from global networks of well-

organized nation-states, criminals, "hacktivists," and insiders that operate outside of the walls of our judicial system.

From a vulnerability perspective, we are at increased risk due to our banking system's significant reliance on technology and telecommunications, and the interconnections between these systems. Banks not only operate their own networks, they also rely on third parties to support their systems and business activities. Some of these third parties have connections to other institutions and servicers. Each new relationship and connection provides potential access points to all of the connected networks and introduces different weaknesses into the system. Ultimately, these interconnected networks are vulnerable to attacks that may affect multiple organizations at one time. Moreover, the ubiquitous nature of the Internet means that a large part of the systems used by banks and third parties ultimately rely on telecommunications and technology that is outside of their control.

This reality is even more daunting as we look into the future. The financial services industry has always been a leader when it comes to advances in technology. Banks and thrifts today are leveraging cloud computing, social media, mobile banking, and new payment solutions, and it's impossible to guess what opportunities technology will bring ten years from now. These technologies all bring benefits to the average consumer of financial services. However, as we expand our use of technology, we could be expanding our exposure to these attacks. Each new product can introduce a new set of weaknesses into the system, and our early adoption of new applications and technology could outpace our ability to identify and mitigate the vulnerabilities during the product design phase, thereby providing new exploit opportunities for cyberattackers.

All of these trends pose special challenges at a difficult time for the industry. While the cost of attacking bank systems is going down, the resources needed to identify, monitor, and mitigate against vulnerabilities and potential attacks are increasing. It's not easy to demonstrate a return on investment for implementing strong security that prevents systemic cyberattacks. How does an institution know whether its defenses are sufficient? Or what costs might have been incurred from an attack had it not been successfully thwarted? The fact is that cyberattackers need only limited resources to trigger significant costs for these institutions.

For all that, I think the nation's banking system is prepared to take on these challenges. Financial institutions are improving their security daily, and the OCC and the other bank regulatory agencies are working hard to support them. But clearly, staying ahead of these threats is a job that will require all of our skill and, more importantly, will require all of us to work together.

And we are. In my capacity as chairman of the Federal Financial Institutions Examination Council, which brings together all of the bank regulatory agencies, I called for the creation of a working group on cybersecurity issues to be housed under the FFIEC's task force on supervision. The Cybersecurity and Critical Infrastructure Working Group was launched in June, and its members are already meeting with intelligence, law enforcement, and homeland security officials. They are going to be considering how best to implement appropriate aspects of the President's Executive Order on Cybersecurity, as well as how to address the recommendations of the Financial Stability Oversight Council.

As we develop the working group's priorities, there are a number of areas that I hope the group will engage in. One is examination policy. We need to identify and address gaps in the landscape of federal and state bank examination policies related to cybersecurity and critical

infrastructure resilience. It is important that our examiners continue to have clear and meaningful policy guidance to address today's threats – and tomorrow's.

Information sharing is another critical objective. Not only do we need to augment relationships between regulators and the law enforcement and intelligence communities**,** we need to share information between the banking regulators about threats we are seeing as well as best practices to address them. Likewise, we need to continue to improve the awareness across financial institutions, particularly community institutions, about the evolving nature of the cyber landscape and encourage their engagement in public-private partnerships.

We also need to enhance incident communication and coordination among FFIEC members to help ensure we respond effectively to domestic and international incidents capable of impacting the critical infrastructure security and resilience of financial institutions and technology service providers.

Clearly, much of the responsibility for assessing cyber threats is housed in other agencies, from the Department of Homeland Security to the FBI to the National Security Agency. They are on the front lines, and they are the ones that are doing the most within government to identify, evaluate, and respond to threats in this area. However, we – the OCC, the FFIEC, and the other regulatory agencies individually – are working closely with them to strengthen the coordination and overall effectiveness of government's approach to cybersecurity of critical infrastructure.

And the OCC also has a number of projects and initiatives underway to ensure that we and the institutions we supervise are on top of this important area of concern. At our largest banks, we have teams of examiners dedicated to IT security issues, and the banks themselves

may have several hundred employees who either focus exclusively on cybersecurity or play some role in defending against cyberattacks.

But we are focusing in particular on community banks and thrifts. As our largest institutions improve their defenses, it is very likely that hackers will turn their attention to community banks. These smaller institutions can provide a point of access into the system, and they may have less sophisticated defenses than large banks. For the most part, they depend upon third-party providers for their IT services, including security. That's understandable, but they still have to be able to assure themselves that these service providers have adequate controls and solid processes in place to protect them and their customers. This can be particularly problematic for community banks and thrifts that may not have the resources or specialized expertise needed to identify and mitigate these vulnerabilities.

So, we're devoting more resources to cybersecurity – at all of our institutions, but especially at community banks and thrifts. Within the last year, we appointed a Senior Critical Infrastructure Officer who works with officials across government and the private sector to address systemic concerns posed by cyber threats, and provides support to examiners in the field. Valerie Abend, who was named to that position, also chairs the new FFIEC working group, which I hope will be another point of support for community banks.

Because information sharing is so important, we helped coordinate a series of classified briefings for banks, third-party service providers, and examiners. These briefings are an effective way to provide the industry with information needed to anticipate and prepare for attacks. We are conducting a number of other outreach events, including a teleconference for community banks and thrifts that attracted about 750 institutions.

We also issued an alert on Distributed Denial of Service attacks, and we are reviewing our policies and updating examination handbooks, procedures, and training to ensure that as cyber threats evolve, all banks and thrifts are prepared to effectively identify the risks and strengthen their risk management and control systems.

In line with the President's Executive Order on Cybersecurity, we will also be looking, as an agency, but especially in concert with our colleagues at the other regulatory agencies, at whether our supervisory authority is up to the challenges of the cyber age. We need to be sure we are taking full advantage of the authority we already have over both financial institutions and service providers. In particular, we need to engage in the kind of open and effective communication that ensures that information is shared, problems are discussed, and solutions are implemented.

But if we determine that legislation is needed to fill gaps in our authority, I can assure you that we will move promptly to raise our concerns to Congress. My hope is that the FFIEC working group will provide a forum for these kinds of discussions.

Meanwhile, we have much work to do as regulators to make sure the banks and thrifts we supervise are doing everything necessary to protect themselves. It's important to remember that cybersecurity is a safety and soundness issue, and more specifically, an example of operational risk. In my time as Comptroller, I've spent a lot of my time talking about op-risk. It's the failure of people, processes, and systems. Unchecked, these failures have the potential to do enormous harm to an institution, whether the issue is Bank Secrecy Act compliance or information security.

So, in our outreach to banks and thrifts and through our supervisory process, we are stressing some lessons learned and some fundamental processes that need to be in place to ensure that banks are secure and resilient.

First, it's important that financial institutions, at the board and senior management level, are aware and engaged, and that they understand the risks posed by these threats and the security measures needed to address them. It's crucial that they set the right tone at the top, that they create a culture of risk management and emphasize the importance of identifying and escalating risks internally, and communicate enterprise-wide about these risks. Whether offering a new product or making a strategic business decision, most bank activities have the potential to introduce vulnerabilities into the system, and it's vital that senior management appropriately evaluate risks and develop prudent implementation and contingency plans.

Senior level engagement shouldn't stop at the bank walls. To deal with cybersecurity effectively, institutions both large and small need to communicate with each other, as well as with relevant government agencies. The financial services community has a robust public-private sector partnership, which can be leveraged even more for the benefit of the system. For example, the Financial Services Information Sharing and Analysis Center or FS-ISAC, which is an information sharing non-profit organization run by financial institutions, includes the OCC and other public-sector agencies as members. Additionally, the Financial Services Sector Coordinating Council, which was formed by the private sector after the 9-11 attacks, brings together private sector firms and trade associations across banking, financial markets, and insurance. These organizations meet regularly with the regulators to discuss emerging issues and best practices and to work cooperatively on ways to deal with critical infrastructure issues facing the financial sector.

Effective information sharing in the industry will help to increase awareness within individual institutions and across the industry. It will enable the sharing of best practices,

techniques and strategies, and collective response to wide-scale events. It will also help banks focus resources on the most significant areas of concern.

The OCC stands ready to help the institutions we supervise in any way we can. We will participate actively in our public-private partnerships, and we will work to raise awareness among the banks we supervise through teleconferences and other outreach events. We will disseminate guidance, working papers and other information, and will leverage expertise provided by our information technology, operational risk, and governance specialists during examinations.

But this is not a problem that can be addressed by one agency alone or by any one institution acting on its own. It is a threat that we can deal with only if we work together in a collegial and collaborative way for the good of our country.

Thank you. I think we have some extra time, and I'd be happy to use it to respond to some of your questions.