Remarks by

Thomas J. Curry

Comptroller of the Currency

Before the

10th Annual Community Bankers Symposium

Chicago

November 7, 2014

Good morning, it's a pleasure to be here today and to have this opportunity to speak to so many who have an interest in the viability of community banking in the United States. The issue of community bank viability is one that I have addressed many times since becoming Comptroller, and my focus has been on viability, not in the sense of just getting by, but on vitality. The reason for that is simple: I happen to believe that a robust system of community banks and thrifts is essential to our nation's economic health.

We at the OCC try do our share to maintain the strength of community national banks and federal savings associations, and we do it in many ways. I won't attempt to catalog all of the things that we do for smaller institutions – I've discussed them many times in the past, and I suspect that almost everyone in this room has heard at least one of those talks – but I would like to mention one general principle before moving on to the subject of today's remarks.

We believe that every bank or thrift is unique, and that it's impossible to take a cookie-cutter approach to community bank supervision. Our Assistant Deputy

Comptrollers and portfolio managers tailor their supervision of each community bank or thrift to its own specific needs, its own business plan, and the unique characteristics of its own market. As a result, our expectations and standards for risk management practices consider the complexity and scope of a bank's operations. In this regard, it goes without saying that large and midsize banks are different from community institutions. Because of the outsized effect that large banks can have upon the economy and financial system, we demand more from them. That's why, for example, our heightened standards guidelines apply only to large and some midsize institutions, and not to community banks.

The differences between these two groups of banks and thrifts are also evident in the area of cybersecurity, and I'd like to spend the rest of my time today on that subject. This is a topic that's been very much in the headlines lately. We've seen a number of attacks on banks and large retailers that have caused problems not just for those companies, but for their customers as well. In the case of the retailers, the card numbers and other information from millions of customers was stolen, and that has caused no end of worry for the affected consumers. In an age of identity theft and cyber crime, people fear their financial security could be jeopardized in one of these breaches.

Community banks and thrifts also suffer from these data thefts, even if they were not involved in any way. Financial institutions are often on the hook to compensate customers for fraudulent charges, and replace credit and debit cards and monitor account activity for fraud at significant cost. That's not easy for any bank, but it's a burden that falls especially heavily upon community institutions. At a cost of $5 or more per card and covering the related fraud charges, the costs can run up very quickly.

These recent incidents highlight the need for improved cybersecurity. But they also demonstrate why we need to level the playing field between financial institutions and merchants. The same expectations for security of customer information and customer notification when breaches occur should apply to all institutions. And when breaches occur in merchant systems, it seems only fair to me that they should be responsible for some of the expenses that result.

While we sometimes think of cybercrime as a threat aimed primarily at large banks, much of my focus in this area has been on community institutions. That's not to say that we don't pay close attention to what goes on at our large banks in the area of cybersecurity, because clearly these institutions are attractive targets for hackers. However, they have sophisticated and well-funded programs in place to address threats, and we devote full-time onsite supervisory resources to monitoring their efforts.

Smaller financial institutions don't have the same kind of resources, so they need to take advantage of other options available to them. These options include support from public-private partnerships, such as the Financial Services Information Sharing and Analysis Center or FS-ISAC, as well as the support available from the OCC and other regulators. In that regard, I believe the Federal Financial Institutions Examination Council, or FFIEC, which brings together all of the supervisory agencies, has an important role to play in helping community institutions develop the processes to manage cyber-threats.

As chairman of the FFIEC, I called for – and the Council members concurred in – the creation of the Cybersecurity and Critical Infrastructure Working Group. The working group has been quite active, and was responsible for alerts on the "Heartbleed"

and “Shellshock” vulnerabilities, and statements addressing cyber-attacks on automated teller machines, among other issuances. The FFIEC also sponsored a webinar for community bankers on cyber issues that was very well attended.

One important initiative launched this summer by the FFIEC’s member agencies was the Cybersecurity Assessment, involving the pilot of a new cybersecurity examination workprogram at more than 500 community institutions. The results were instructive. They will help member agencies make informed decisions about ways to enhance the effectiveness of cybersecurity-related supervisory programs, guidance and examiner training. The findings from the assessment will also help supervisors and bankers alike identify actions that can strengthen the industry’s overall level of preparedness and its ability to address the growing level and ever-evolving nature of threats to systems and data.

As you may know, the FFIEC released two documents earlier this week: a report containing general observations from the Cybersecurity Assessment, plus a statement encouraging financial institutions to join FS-ISAC. With threats evolving so rapidly, we expect management at every institution we supervise to monitor and maintain sufficient awareness of cybersecurity threats and vulnerabilities. The FS-ISAC is an important resource for institutions to identify, respond to, and mitigate cyber-threats and incidents. Both documents are important, and I would encourage you to give them some attention.

The General Observations report highlights some of the key findings from the pilot, and also provides questions we think directors and senior management at community banks and thrifts should be asking. For example, it encourages management to incorporate cyber-incident scenarios into business continuity and disaster recovery

planning. The report stresses that management should consider how it will respond to a cyber-attack, not just internally, but with customers, third parties, regulators and law enforcement.

In addition, the report notes that it's extremely important for management to understand the institution's inherent risk to cyber-threats and vulnerabilities when assessing its state of readiness. In that regard, management should be asking questions about the types of data connections the bank or thrift has with other institutions and third parties, and whether all of those connections are properly managed. This falls under the category of what our cybersecurity-gurus refer to as "external dependency management." We want the institutions we supervise to understand the increasing complexity and interconnectedness of the financial system, as well as the importance of maintaining strong controls and carefully monitoring the ways in which they connect to third parties.

Complexity and interdependency create opportunities for hackers to gain access to the systems of financial institutions and the third-party vendors that provide services to the industry. Not only do financial institutions need to have good controls over their own systems, they need to monitor carefully the ways in which they connect to vendors, how these contractors manage their systems, and how these vendors connect to still other third parties. Financial institutions also need to be aware of the various ways in which even their own employees may inadvertently create opportunities to compromise systems, by introducing personal (and possibly corrupted) devices into bank networks. In a highly interconnected environment, it can be very difficult to identify and address all of the potential vulnerabilities a bank might face.

In addition to being interconnected, the networks that serve the financial industry are global, which has additional implications for cybersecurity. Today, the global nature of the Internet means hackers can target bank systems from almost anywhere. That includes countries with regimes that, at a minimum, act as criminal havens by turning a blind eye toward illicit activities, and at their worst, sponsor attacks. As a result, financial institutions today face threats not only from insiders and individuals acting alone, but also from global networks of well-organized nation-states, criminals, and so-called "hacktivists."

An additional area of concern is third-party relationships. Third-party service providers are important to all financial institutions, but they can be especially important for community banks. While they have important benefits and are in many ways an essential part of business, it can be easy for financial institutions to become overly dependent upon third parties and overly-trusting. But just because these contractors have long client lists and hard-to-duplicate expertise doesn't mean they are infallible.

Third-party relationships have been a significant area of concern for years, and not just in the area of cybersecurity. We've taken serious enforcement actions against some of our large institutions for problems brought on by poorly-managed third-party relationships, from debt collection companies to telemarketers. And last year, we issued an enforcement action against one technology service provider that had been unable to promptly restore service after Superstorm Sandy.

One concern that all of us have to be sensitive to in this regard is the access third parties have to large amounts of sensitive bank or customer data. For an industry in which reputation means everything, a single data breach involving confidential customer

information can be extremely costly. Just think about the reaction to the breaches at Target. Banks are particularly vulnerable to events that erode trust, and once an institution's reputation is damaged, it can take years to repair. In the eyes of the customer, it doesn't really matter whether the breach was occasioned by problems within the bank or thrift itself or by a flaw in a third-party's security.

I'm not trying to discourage the use of third-party vendors. They provide important services to both large and small banks, and community banks in particular often use outside contractors to leverage expertise and resources that they can't support internally. But we do expect the banks and thrifts we supervise to recognize that third-party relationships can pose significant risks, and any institution that supplements its own resources with outside providers needs to have risk management practices in place that are commensurate with that risk.

All of these risks <u>are</u> manageable, but they must be well understood and they <u>must</u> be managed. Given the level of interconnectedness and dependency of third parties, a financial institution needs to understand not just its own cybersecurity precautions, but the precautions its vendors take to protect themselves from <u>their</u> third-party relationships.

The OCC and the other regulators are playing a role in watching over technology service providers. While we won't go into every provider, we will examine service providers that support a large number of banks and that could, therefore, pose a systemic risk to the financial sector. However, I want to caution everyone that even if we do supervise a service provider, that does not alleviate a bank or thrift of its responsibility to understand and manage risks involved in their third-party relationships. Our supervision

does not take the place of due diligence or ongoing monitoring commensurate with the level of risk and complexity of the arrangement.

Clearly, our expectations as supervisors are high in the area of cybersecurity. But the stakes are high as well. The industry's reputation is at stake, as is the trust that consumers place in their financial institution. Financial institutions of all types and sizes have a lot of work ahead of them. For our part, we at the OCC will do everything we can to support community banks in this effort.