Remarks by

Thomas J. Curry
Comptroller of the Currency

For the
Independent Community Bankers of America
Annual Convention

March 4, 2014

Good morning. It's a pleasure to be with you, even if it is through a virtual presence. The ICBA annual convention is one of the industry's most important gatherings, and I would have greatly enjoyed the opportunity to spend some real time there with you, to hear directly about your concerns and, honestly, just to have the opportunity to talk with community bankers. But with all that is going on here in Washington, it just wasn't possible to make the trip, and so, with apologies, I'm going to take advantage of technology to offer a few thoughts on the state of community banking today.

I'll start by repeating something I said to you last year. Community banks are important. They're important to the families that rely upon them as a safe place for their savings and as a source for the credit they need to improve their lives. They're important to small businesses and farm operators that want to deal with a local financial institution that knows their market and their business and is willing to work with them through good times and bad. They're important to communities everywhere that depend upon local bankers to handle municipal finance needs, serve on hospital boards, and participate in the civic life of their town.

You, the men and women who run our nation's community banks, are important to the people you serve, and so you're important to the OCC. That's why we put so large a share of our resources into community bank supervision.

As you probably know, we supervise community banks not from Washington, but from more than 60 offices located throughout the country. You make decisions locally, and so do we. We not only empower our examiners to make most supervisory decisions at the local level, we expect them to make those decisions without consulting Washington.

That doesn't mean that we don't support them – and you – with all of the resources available to a national organization. Quite the contrary, that's very much a part of what we offer as a supervisory agency. We sponsor workshops for community bank directors and make a number of important services available to the institutions we supervise through BankNet, our dedicated Web site just for national banks and federal savings associations. We provide issue briefs from our economists and accountants, and our banks and our examiners have access to licensing specialists, legal counsel, and liquidity experts, to name just a few of the resources we make available. If you're a national bank or a federal savings association, I hope you are taking advantage of those products and services.

While we try to offer value as a regulator, we also know that every new law, and every rule, regulation, or piece of supervisory guidance that comes out of the banking agencies has the potential to impose a burden on smaller institutions, so we've also tried to eliminate as much of the noise as possible. For example, when we issued the domestic capital rule last year, we also put out a two-page OCC guide to the rule that gave you the essential information you need in a straight-forward summary. In addition, each new regulation or piece of supervisory guidance

includes a box on the cover that tells you quickly whether the issuance applies to community banks. If it is directed only to large institutions, you'll see that at a glance.

Most importantly, though, we listen to you. We're supervisors, and so we won't always agree with you, but I can tell you that we will always hear you out, and we will take your concerns and your views into careful consideration in everything we do.

In completing action on the domestic capital rule, for example, we took a close look at several of the issues you raised, including the treatment of Trust Preferred Securities, AOCI, and residential mortgages, and made changes with an eye toward minimizing burden on community banks.

More recently, we engaged with you on the treatment of TruPS CDOs under the Volcker Rule. As it happened, our final rule, which was the product of long interagency discussion and consideration of thousands of comment letters, would have effectively required community banks to divest these CDOs. That was a mistake, and I want to say that Cam Fine and the ICBA played a particularly important and constructive role as we weighed how best to deal with it. Cam gave us the benefit of the ICBA's views – sometimes in rather colorful language – and we listened, and acted.

I won't be quite as colorful as Cam in my comments this morning, but hopefully I'll still be able to hold your attention. What I want to talk about is one of the key factors that I think got so many of you through the challenge of the financial crisis and will get you through the challenges of the future.

The financial crisis that began in 2008 was the most intense shock to the banking and financial system since the Great Depression, and the recession that followed was as deep and long as any downturn that we've experienced since the 1930s. Indeed, it is still with us, and

banks in many parts of country are only just now returning to their pre-crisis levels. Several hundred community banks failed during the recession, and that's a tragedy for everyone involved – owners, employees, customers, communities, and the supervisory agencies as well. I can tell you that, at the OCC, our supervisory staff doesn't like to lose even one bank.

But while those failures were tragic, what I think is more telling is that the overwhelming majority of community banks and thrifts supervised by the OCC successfully weathered the storms of the last decade. So it makes sense to ask why? What separates those banks that thrive from those that merely survive – or worse – are forced to close?

One fundamental dividing line between the winners and losers involves the quality of a bank's risk management. I spoke about this in my last appearance before this convention, so I won't dwell on it again. But I would encourage you to take a look at our booklet, *A Common Sense Approach to Community Banking*. The booklet is available on our Web site at OCC – dot – gov, and it outlines, among other things, the Risk Assessment System that our examiners use to evaluate risk in the institutions they supervise and how you can use it to identify and manage risk. It's a good tool for benchmarking yourself, which is something winners always do.

One other set of OCC risk-management products I would encourage you to look at while you're on Banknet are the stress test tools we've developed for analyzing commercial real estate, agriculture, and other loan portfolios. They're intended to help community banks understand how their portfolios will stand up in times of stress and under different economic conditions. I can't think of a more fundamental risk management practice than subjecting your credit book to rigorous testing.

But while you need to attend to the traditional areas of risk, it's crucial that you keep your eyes focused on emerging areas of risk. And no area of emerging risk is more important today than the cyber threats that are increasingly common in our interconnected environment.

You can gauge the growing importance of this threat by reading our *Semiannual Risk Perspective*, or, for that matter, you can just pick up a newspaper or watch the evening news. I doubt there are many consumers who didn't hear about the data breaches at Target and Neiman Marcus, and a healthy percentage of them went to the Internet to search their account statements for signs of fraud.

These were significant events, with significant costs for everyone involved. The retailers took a hit to their reputations. Consumers experienced the inconvenience of having to monitor accounts for signs of fraud and the stress of worrying that they might fall victim to identity theft. And of course banks and thrifts pay a financial price, not just because they are on the hook for fraudulent charges, but because they bear the cost of monitoring accounts for unusual activity, responding to customer questions and concerns, and replacing those cards.

That includes community banks, even though none of you are responsible for the technology used in the retail point-of-sale payments system, and even though none of you had any responsibility for the lapses that led to the data breaches. And yet, when cyber thieves steal debit or credit card data from large retailers, you are the ones stuck with the cost of replacing those cards for your customers.

The cost to banks for these security breaches—which the Consumer Bankers Association recently estimated at $172 million and climbing—is a concern at a time when earnings are already under pressure. Fortunately, there is renewed discussion about strengthening information security across the banking and retail sectors. In the past couple of weeks, the ICBA

announced a new cybersecurity partnership involving leading trade associations representing the merchant and financial services industries. This is a good start, and I hope that bankers and merchants can develop solutions to improve security and address cost sharing.

But while you can't control the standards or security programs for retail payments system technology, you **can** manage the security of your own data and systems. And it's important that you protect your data and systems, because the impact of a successful cyberattack on your bank or your service provider could be even more disruptive than a data breach at retailers. It's one thing for your customers to worry about whether someone is making charges on their credit card, as troubling as that might be. It's quite another for your customers to worry about whether the accounts that hold their life's savings or grocery money are secure.

Many community banks look to third-party service providers for IT services, in the area of data security, among others. That can be an effective tool, but while you can outsource the activity, you can't outsource the risk. It's good, because third-party relationships help you acquire and leverage specialized expertise that you can't afford to develop on your own. But these relationships bring important risk management considerations with them. Third-party relationships have to be managed very closely. Third parties can be the weak link in your information systems security and resiliency; and especially where that third party is providing security services, you'll want to make sure they are up to the task and performing to your expectations.

This is an important topic, and we recently issued updated guidance on this subject. We don't want to steer you away from using third parties as a part of your business strategy, but we do expect you to understand the very significant risks that can arise from third-party relationships and to ensure that you have risk management practices that are commensurate with that risk.

The due diligence required here can sometimes be substantial. You have to assess not only the vendor; you may also have to assess the vendor's relationships. 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, thereby introducing more complexity as well as new and different weaknesses into the system.

As a supervisor, I have a number of other concerns about third-party relationships. One is the extent to which service providers are consolidating, which means that more financial institutions are dependent upon a single vendor. Where that happens, deficiencies at one vendor have the potential to affect a large number of banks simultaneously.

A second, and related, trend that concerns me is the increased reliance by banks, directly and indirectly, on foreign-based subcontractors to support critical activities. Third-party service providers and subcontractors of third parties that operate in foreign jurisdictions present unique problems. Banks need to consider the legal and regulatory implications of where their data is stored or transmitted, and make a determination as to whether geographic limitations are needed in their contracts.

Finally – and perhaps most important – I am concerned about 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. Banks are particularly vulnerable to events that erode trust, and once an institution's reputation is damaged, it can take years to repair.

We want to help. In my capacity as chairman of the Federal Financial Institutions Examination Council, I called for the creation of a working group on cybersecurity, and I hope to

use it as a vehicle to raise awareness across community banks about cyber threats and how you can protect your banks and your customers.

In addition, there are other things we are doing right now. As you may know, the banking regulators examine a category of vendors designated as Technology Service Providers, or TSPs, and we have authority under the Bank Service Company Act to issue enforcement actions when necessary. In December, we issued a formal order against one of these firms, requiring it to take action to address deficiencies that prevented it from restoring services to banks promptly after Super Storm Sandy.

Of course it does little good for you to find out about a service provider's deficiencies after the damage is done. I think it's important for you to have access to information from our exams as early in the process as possible, and we're exploring ways to get those reports into your hands faster.

However, there is no substitute for doing your own due diligence. Ultimately, it's your responsibility to ensure that your third-party providers have appropriate controls in place to secure your bank's information and that of your customers. User groups, and yes ICBA conventions, are useful forums for you to compare information and gain better insight into your third-party relationships.

The OCC stands ready to help in any way we can. 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 – on an interagency basis and through public-private partnerships – in a collegial and collaborative way for the good of our country.

Thank you for allowing me this time to be with you today.