Remarks by

Thomas J. Curry
Comptroller of the Currency

Before the

FFIEC Compliance Examiners Conference
Arlington, Virginia

October 3, 2013

Good afternoon. I'm very pleased to be addressing the FFIEC Compliance Examiners Conference again this year. You know, if we aren't careful, this could become a habit. And if it does, I think that would be a very good thing. After going 15 years without a conference dedicated to compliance risk, I do believe that all of us will benefit, and by "all of us," I mean banks, their customers, and the examiners who work so hard to ensure that banks and thrifts adhere to laws and regulations.

It's a particular honor to be addressing you this year as not only the Comptroller of the Currency, but also as the current chairman of the FFIEC. I regard the FFIEC as a vital mechanism for promoting collegiality and collaboration among the state and federal financial agencies. That's especially important today, as we deal with so many new issues and concerns. It is my hope that we can use the FFIEC to an even greater extent in the future to address emerging issues and promote consistent standards across the regulatory landscape.

But whether we act through the FFIEC or on an interagency basis in our consideration of new issues, nothing matters more to America's consumers than you, the men and women assembled in this room. You are the ones who serve on the front lines of protecting bank

customers, and so, in a very important way, you are on the front lines of protecting the American financial system.

We see today that some of our largest banks have elevated their compliance and audit functions, granting them additional authority and shielding them from interference from the rest of the bank. I have to say, if they had taken that step years ago – if bank management had maintained a consistent focus on compliance requirements and responsibilities – they might have spared themselves some of the enforcement actions that we have taken recently.

But nobody knows that better than you, right? Nobody knows better than you how lapses in compliance can lead to weaknesses and activities that can harm consumers and result in supervisory actions, enforcement actions, lawsuits, and the kind of risk to a bank's reputation that lowers its standing in the community. And today, most banks recognize just how important compliance management is to their institutions. Too many of our large institutions are devoting senior management time to addressing problems from the past, when that time could be better spent planning for the future. I suspect that many of the institutions we supervise are looking at you these days with new found respect – and maybe even a bit of affection!

But some of the most important work you do can go unnoticed, at least until disaster strikes. A year ago, we had to postpone this meeting because of Hurricane Sandy and the destruction that super storm brought to the East Coast, particularly in New York and New Jersey. The damage was breathtaking in its breadth and in its severity.

In the days that followed, the importance of flood insurance became clear. With that realization, too, came recognition of how important it was that compliance examiners like you had made sure that banks and thrifts had required customers in flood plains to purchase

those policies. Before the hurricane, flood insurance might have seemed like one of the more mundane parts of a compliance examination, but the homeowners who lost everything to Hurricane Sandy would no doubt disagree. For them, it was everything, and I can't begin to think how many homeowners owe their economic well-being to you.

When I spoke to you at our last conference, I made a number of points about the importance of us all working together, something that is a virtual necessity in the post-Dodd-Frank regulatory environment. In part, that's because there is more overlap today in lines of responsibility. While some areas of responsibility for compliance supervision are clearly delineated, other areas are less easy to understand and may require even greater care in communications and coordination. So we need to be sure we are all talking to each other, and in that regard, conferences like this, that bring together compliance examiners from all of the banking agencies, are extremely useful. Communication, coordination, and collaboration are the hallmarks of an effective supervisory system in today's environment, and meetings like this promote all three.

I made one final point in my remarks at the last conference, and that had to do with the importance of staying abreast of emerging technologies. The Internet is the most obvious example, though it's not the only one. Think about the development of new payment systems, some of which exist outside the banking and thrift industries, such as PayPal. In fact, a bank account today can consist of nothing more than a plastic card that is capable of receiving paychecks, paying bills, and storing money.

While many of these innovations add to consumer convenience, they also introduce compliance risk. For those of you involved in Bank Secrecy Act exams, for example, the new payment system options present a variety of challenges. How do we track illicit money

when it can be loaded onto cards and moved over the Internet through systems that are not overseen by regulators?

Moreover, as mobile banking products proliferate along with the use of smart phones, risk is being introduced into the system because the phones are subject to viruses and malware and cannot be safeguarded physically, while messages between banks and customers may not be encrypted or may remain in memory even after they've ostensibly been deleted.

Given these challenges, cases of unauthorized account use will be difficult to resolve so, at a minimum, banks will have to provide disclosures that emphasize potential risk or develop new risk management procedures. Those might include transaction limits for mobile banking, encryption, and authentication measures such as PINs or passwords for the customer's mobile phone.

Today, I want to build on that theme of emerging technology and talk about an issue that some people might not associate with compliance supervision. However, it's an issue that's moved to the top of my list of concerns, and it's one that I think that almost every department in the bank – and every area of supervision – should be paying close attention to. That issue is cybersecurity.

I'm sure some of you must be thinking that cybersecurity is the domain of IT examiners. While it's true that IT specialists have great responsibility in this area, the fact is that cyberattacks on a financial institution pose operational risks that can have a direct impact on consumers. Cyber attacks can cause degradation or even complete disruption of services to customers, and in the worst case, they could lead to the destruction of systems and customer

data. These attacks can result in direct financial losses and damage to an institution's reputation, and over time, they could undermine confidence in the banking system itself.

We are getting a good handle on some issues. For example, we've identified the compliance risks posed by the use of social media by our financial institutions. As you know, in January the FFIEC issued proposed guidelines for the use of social media, noting several areas of potential compliance risk. While not all of them involved cyber-attacks or cybersecurity, it's clear that social media can facilitate attacks on computer systems. Not surprisingly, the proposed guidance addresses the need for banks to exercise vigilance to ensure that social media are considered when instituting controls meant to safeguard customer information from cyberattacks. It also stresses that the response of financial institutions to any security incident, such as a data breach or account takeover, should factor in a response via social media for compliance purposes.

As with other emerging fields, cybersecurity threats require all stakeholders to work together to mitigate and manage risks. Managing these risks requires a coordinated approach, not only within the bank or thrift itself, but between these institutions and their regulators.

And I would add, it requires a good deal of communication and coordination among the regulators. Over the past year, we've seen growing sophistication in the range of cyber threats, particularly in those that involve attacks aimed at disrupting online services. However, we are increasingly concerned that these attacks will move from disruption to destruction, and it's our job as supervisors to identify emerging risks, raise awareness among the institutions we supervise, and provide guidance to those institutions and to you, the

compliance examiners out in the trenches. We can't do that effectively as supervisors if we aren't communicating with each other.

Working together on an interagency basis has other benefits. Beyond sharing best practices and information, the better we know one another, the faster we can coordinate our response in the face of a crisis. This is critical, because cyberattacks demand quick responses.

In the aftermath of a cyberattack, whether it's the kind of denial-of-service attacks that are coming with greater frequency, or intrusions that cause damage to bank systems, compliance issues are likely to arise. The issues could range from the inability of a financial institution to properly process a customer's payments to the loss of access by customers to their accounts. While clearly creating an inconvenience, this could also result in a number of negative actions affecting customers, including fees or penalties charged to the customer's account. Of course, unauthorized access to a customer's accounts or other personal information is also a concern raised by a cyberattack. The routine activities associated with banking services –deposits, payments, and lending – are all potential targets in a cyberattack, and they can have a ripple effect on compliance issues for the bank and the consumer.

It's important that everyone in this room keep up with advances in, and new uses of, banking technology. If we don't know what products and tools are being used by the institutions we regulate, it's going to be difficult, if not impossible, to spot emerging problem areas. If you had told me 10 years ago that people would making deposits over cell phones by using the camera to photograph a check, I would have had some serious safety and soundness questions. But I'm from the generation that remembers bringing Christmas Club books to the bank on Saturday to make a $5 deposit. As we all know, keeping up with the

pace of technology can be a challenge, if not downright scary. One solution is to make yourself learn to use the technology in your daily life. At the very least, we all need to have a working knowledge of online banking and social media. If you're not a Millennial, then you might want to find one and ask some questions. It's old advice, but it still works.

On the other end of the spectrum, no doubt some of you have the latest gadgets that the wizards of Silicon Valley can cook up. You can send text messages, tweet, watch "Breaking Bad," and order dinner, all at the same time. For those in this category, the trick may be to avoid getting caught up in the gee-whiz excitement of the latest thing, because whether we're examining the newest banking methods and products or ones that have been around for centuries, there are things that always apply—such as the need for a healthy skepticism.

As for more ways to mitigate risk, perhaps it will be up to us to ensure that the banks we supervise are taking the proper steps to educate their customers on how to use technology in a safe and sound way—to save them from themselves, so to speak. After all, banking-related cyber crime is as likely to affect consumers as it is banks, if not more so. Certainly we can urge banks to be proactive about waiving service fees and penalties incurred by consumers whose payments are late because they cannot get online access to their accounts to make EFTs, either between their own accounts or to outside debt holders. EFTs are already a compliance area, so we have some built-in authority there.

We can continue to push banks to make better use of social media to alert customers to scams, and to provide information to consumers about how they can remediate any damage done to their accounts or their personally identifiable information. But we must also make sure these institutions realize the potential for misuse of customer data and take steps to prevent that, as required by the Gramm-Leach-Bliley Act.

Of course, when applicable, we will want to study the conclusions reached by our recently formed FFIEC Cybersecurity and Critical Infrastructure Working Group and look for lessons that can be applied to compliance. We created this group specifically to enhance communication and strengthen relationships among the agencies as we respond to the threat posed by two linked factors: the growing sophistication and volume of cyberattacks, and the ever-increasing reliance on telecommunications and technology.

One final point. There is a good chance that someone in this room will encounter a new product or situation involving technology that will make you wonder, "Could there be a compliance issue here?" I urge you to pay attention to those inner red flags. We can't assume that someone else has already thought of every possible contingency, not when the industry is changing every day. Recognize your own creativity, and take your own ideas seriously. Make sure they are passed up the line. Now more than ever, the American people are depending on you to recognize problems before they even exist.

Thank you. I believe we have some extra time, and I'd like to use it to hear from you and answer any questions you may have.