Remarks by

Thomas J. Curry

Comptroller of the Currency

Before the

Institute of International Bankers

Washington, D.C.

March 2, 2015

Thanks to Sally and thanks to everyone who has had a hand in making this event such a fine success, year after year. I am pleased to carry on what is by now a long OCC tradition of reaching out to the industry leaders who gather at the IIB this time every year.

I know I'm not alone among banking regulators when I say that the issues with which my OCC colleagues and I are increasingly preoccupied have a distinct international orientation. Yet community national banks and federal thrifts, which rarely have a conspicuous international presence, constitute by far the largest number of OCC-supervised institutions.

This may seem to be a paradox. But it isn't. Of course, the OCC also supervises some of the largest internationally active banks, including many that are represented here today. For these institutions, the complications and rewards of operating across national borders come with the territory, so to speak.

But it's all too easy to forget that smaller institutions are also affected by global trends—in some cases, profoundly so. At various levels, their customers' lives and business fortunes are tied to the ups and downs of the global economy—and, therefore, so

are the banks' fortunes. And all banks, large and small, confront operational risks that are inherently transnational, such as cybersecurity and Bank Secrecy Act/Anti-Money Laundering (BSA/AML) compliance. In short, the OCC focuses on global banking issues because they affect every bank we supervise.

Our operational priorities reflect this emphasis. We are deeply engaged in the community of international supervisors, bilaterally and through the Basel Committee and other groups, in the effort to identify emerging risks and share best practices and perspectives. For the OCC, information sharing is emphatically a two-way street. As an example of how we absorb as well as impart insights, we are implementing extensive changes in our large and midsize bank supervision programs, based in large part on the recommendations of a group of foreign supervisors we invited to study those areas.

Also, as you know, the OCC has supervisory responsibility for the 49 federal branches of foreign banking organizations in the United States, which are an active and vibrant component of our banking system. Last month, we held an outreach meeting with the managers of OCC-supervised federal branches. Attendees not only heard from our lead experts; they also had the opportunity to speak their minds to us about the issues that matter to them.

When I spoke to the members of this group—and I am glad to see so many of these folks here today—I touched on three closely related topics. First, I talked about the OCC's supervisory expectations for federal branches and agencies. Second, I emphasized the importance of clear communications and information sharing, not only between the OCC and foreign banking organizations, but also between the OCC and their home country supervisors. Finally, I discussed a source of risk that is a matter of particular and

growing urgency today: the requirements of the BSA/AML statutes. In this connection, I think it is extremely important that banks of all types and sizes understand the nature of BSA/AML risk, understand their BSA/AML regulatory obligations, and understand the importance of collaboration among financial institutions and sovereign supervisors to meet the rising BSA/AML risks.

Indeed, it is fair to say that banks face a serious challenge from terrorist and criminal organizations. I have often said that money is like water for terrorists; they need it to survive. It's our responsibility to deny it to them at the source, by stopping illicit money transfers and closing the gaps in cyberspace that can be exploited to fund their operations. Strong cybersecurity measures and BSA compliance are complementary and essential parts of this effort.

Obviously, this is an ambitious agenda—too ambitious for any one country to achieve on its own. But working within the community of nations, it is well within our grasp.

Combating the money laundering and terrorist threats requires each of us to do our part, individually and together. That means that every U.S. financial institution must adhere to strong risk management standards for BSA/AML. But it also requires that their foreign counterparts have equally high standards in place.

One of my highest priorities since becoming Comptroller in 2012 has been to strengthen the OCC's oversight of BSA/AML compliance in the banks we supervise. We have modified our examination procedures so that BSA deficiencies receive proper emphasis in our evaluation of each bank's overall safety and soundness. We have focused on the BSA/AML risks that can arise when third-party relationships are not properly

managed. We have demanded that OCC-supervised institutions provide adequate resources to their BSA/AML compliance functions and assign accountability for compliance across all business lines that entail BSA/AML risk. And, where we found serious problems and violations, we have taken appropriate enforcement actions.

National banks and federal savings associations have responded by committing resources and expertise to manage and control BSA/AML risk. While some banks still have a ways to go, the vast majority of our institutions have solid programs in place.

This progress is to be applauded. But unfortunately, it is merely a good start, and it is not static. Financial institutions here and around the world face multiple challenges on the AML and terrorist financing front, not the least of which is the constantly evolving nature of the threat, as criminal and terrorist elements alter their tactics to avoid detection and continue to penetrate our defenses.

Another challenge facing U.S. institutions relates to the Bank Secrecy Act itself. Although the law has been updated several times since it was enacted in 1970, the current regulatory regime provides for a process that is document-driven and that relies heavily on individual decision-making. In the time it takes to generate and investigate a Suspicious Activity Report (SAR), the criminal or terrorist may well have changed tactics and moved on.

Given the growing sophistication of terrorists and criminals, we have to make sure that the BSA is equal to the task. To this end, the OCC continues to discuss with our regulatory colleagues ways in which we can improve the system, including removing or amending regulations and requirements that may no longer be necessary or effective. We are also working with our colleagues to find better ways to use technology in advancing

our BSA/AML goals. Without question, technology is rapidly changing the way we do business. New payment systems are creating greater efficiencies and convenience, and virtual currencies offer the prospect of instantaneous transactions directly between individuals and entities on a global basis. These innovations are potentially revolutionary in their impact, and are advancing at a breakneck pace. The current regulatory regime, which is rooted in 20th century concepts and approaches, will need to change and adapt in order to remain relevant into the 21th century. While the task seems daunting, it is also foreseeable that, if properly employed, technology can be used by banks and the government to better meet the goals of the BSA, by providing more accurate and timely information to law enforcement and regulators, while simultaneously reducing cost and burden.

This need for innovation extends beyond the need for stronger cybersecurity measures. While often viewed as separate areas, the goals of BSA/AML and cybersecurity are increasingly converging. Terrorists, drug cartels, and cybercriminals all have a need to generate cash and move money, and it would seem that many of them would share some of the same goals. There are lessons to be learned from our decades-long experience in BSA enforcement that can be applied to the cybersecurity area, and vice versa.

Another critical element to combating money laundering, terrorist financing, and other financial crimes is information sharing. The OCC is supporting legislative measures designed to promote the information sharing that is so critical to our success. For example, we have recommended legislation that strengthens the statutory safe harbor from civil liability for financial institutions that file SARs. The courts have ruled

inconsistently on this subject, with some holding that banks must have a "good faith belief" that a violation occurred to enjoy immunity from civil liability while others interpret the law to confer blanket immunity. The legislation we are supporting would ensure that financial institutions do not expose themselves to civil liability simply for complying with federal law.

We also support an amendment that would extend the safe harbor for banks that share information about bad actors and financial crimes with one another. Under current law, a bank has immunity from civil liability if it shares information about suspected money laundering or terrorist financing. While this immunity is an important protection, it does not go far enough because it does not cover other crimes such as computer intrusions, credit card fraud, wire fraud, and other financial crimes. We would like to see this safe harbor broadly extended to cover an array of financial crimes, to give banks maximum protection and encourage more robust information sharing.

I'd like to close with some thoughts on a subject that has drawn considerable attention of late. It is true that some U.S. banks have closed the accounts of certain customers, and entire categories of customers, based on concerns about BSA/AML risk. Some of these customers are foreign banking organizations that are long-term customers of the U.S. bank. Understandably, these actions have elicited complaints from those foreign banking organizations, complaints that have often had the backing of their home governments. It has also caused unavoidable hardship for customers who find themselves unable to transmit funds to family members in troubled countries.

There are no easy answers to these problems and, indeed, those problems may well lie beyond the capacity of commercial banks and their regulators to resolve. But, to

the extent that it can, the OCC is committed to playing a constructive role in the dialogue and working with other parts of the U.S. government to address this important issue.

To be clear, the OCC does not encourage banks to terminate customer relationships without a careful analysis of the risks presented by that customer and the bank's ability to manage those risks. The OCC's mission is to ensure that the banks we supervise operate in a safe and sound manner. That means managing their risks appropriately, meeting the needs of their communities, complying with laws and regulations, and providing fair access to financial services and fair treatment of their customers. We require that banks' risk assessments take into account all the products and services they offer, as well as the customers and geographies they serve.

Within these parameters, we do not tell banks how to conduct their business. We certainly do not direct them to provide services to some customers and not to others. Still less, would we encourage banks to terminate entire categories of customers without regard to the risks presented. What is important—and what we do insist on—is that banks assess the risk posed by its customers and properly manage the assumed risk. This is no different in the BSA/AML area than it is in every other activity in which our banks engage.

The question we should perhaps be asking is this: what can be done to lower the risk profile of, and raise standards for, customers and counterparties in regard to anti-money laundering? Part of the assessment that banks conduct is an evaluation of their foreign correspondents' own risk management practices and comprehensive supervision. Obviously, where these practices are less effective and the applicable requirements less exacting, the adoption of a more comprehensive AML regime to which the foreign

correspondents would be subject, could help. This is an area that offers opportunities for fruitful collaboration between host and home country supervisors.

Perhaps what has not been articulated often enough is that current and prospective clients of U.S.-chartered banks should be prepared to offer sufficient and transparent information to allow these banks to make informed risk assessment decisions. If U.S.-chartered banks have a clear understanding of current and prospective clients' profiles, they may be more comfortable providing banking services, even those services that may have historically had higher risk.

To safeguard our financial system, we must leverage each other's strengths to address our weaknesses more effectively. Sharing information and ideas, as we are doing during this conference, is an important step toward ensuring that we have the tools we need to defend the system against those who would use it to do us harm.

Thank you.