Remarks by

Thomas J. Curry
Comptroller of the Currency

Before the

American Bankers Association and American Bar Association
Money Laundering Enforcement Conference

Washington, DC

November 17, 2013

Thank you, it's a pleasure to be here with you today. Bank Secrecy Act compliance is an area that has been at the top of my agenda since I assumed office as Comptroller of the Currency 19 months ago, and so I'm very glad to see that the two ABAs sponsor a joint conference on the subject every year. In fact, I see that you have been doing so for a full quarter-century now, and that's a very impressive and helpful commitment of time and resources. As I'll discuss in greater detail a bit later, Bank Secrecy Act and anti-money laundering programs are imperatives that are likely to require more time, more resources, and more ingenuity and creativity from all of us, industry and government alike, in the future.

While Bank Secrecy Act and anti-money laundering compliance—or BSA/AML—has been a particular focus during my time as Comptroller, it's also been a regulatory priority for most of my years in bank supervision. Those years stretch back further than I care to remember—or at least that I care to say. In fact, I had barely begun my career in state government in Massachusetts when one of the most prominent banks in our state, The First National Bank of Boston, pled guilty to failing to report $1.2 billion in currency transactions with Swiss banks and paid what was then the largest fine ever imposed for BSA violations—$500,000. That was in 1985, and the case was the subject of months of headlines and

congressional investigations. It was probably the first time that most people outside the industry had ever heard of the Bank Secrecy Act, but that case and the dozens that followed it over the years made BSA part of the national lexicon.

In those days, the BSA was viewed as a vital weapon in the war on drugs and other illicit activity. It still serves that role. But more recently, the BSA and other anti-money laundering requirements have also provided critical support to those on the front lines in the fight against terrorism. These are all high-stakes issues that have a critical impact upon our families, our communities, and our very lives. So, everything that supervisors and regulated institutions alike can do to ensure compliance with the Bank Secrecy Act is time and money well spent.

In many ways, we have been successful. The vast majority of the banks and thrifts we supervise have programs in place that meet the requirements of the BSA and other anti-money laundering statutes. But everyone in this room can tick off a half-dozen or so recent cases involving large, well-known financial institutions that turned out to have inadequate BSA programs.

Given what's at stake, it's a bit surprising that BSA failures occur as often as they do, and that they so frequently involve some of our largest and most sophisticated financial institutions—banks and thrifts that have ample resources to devote to the task. These lapses have resulted in enforcement actions that have proven very costly for the institutions involved—and not just because of the financial penalties that some have carried. They've also taken a toll in the time and money spent rebuilding systems that should have been built right the first time, and kept up-to-date. They've exacted a cost in terms of lost management time that might otherwise have been spent on building the bank's business. And it's hard to overstate the price that institutions pay in terms of the cost to their reputation.

When we review these failures, we find a number of common threads, including the strength of the institution's technology and monitoring processes, and the effectiveness of its risk management. While I am by no means unmindful of the cost and complexity of BSA compliance, I have to say that I find that disappointing. Information technology is crucial to almost every aspect of a financial institution's success, and these systems need to evolve as risks grow and change. And it goes without saying that risk management is a discipline of fundamental importance throughout a banking organization.

However, two of the other root causes for inadequate BSA programs are equally disappointing—corporate governance processes that are too weak to support a culture of compliance and management unwillingness to commit adequate resources to the task. In the banks that we have cited for BSA violations, we very often find insufficient staffing, high turnover rates, and cutbacks in spending on compliance.

That's unacceptable, and it speaks to the quality and focus of management. It's the reason we've made BSA compliance one consideration in determining the "M" or Management component of the CAMELS rating for large institutions, much as we had already done for midsize banks. Entirely apart from the importance of BSA compliance to our nation's security, sound risk management, healthy corporate culture, strong corporate governance, and high quality IT systems are all hallmarks of good management, and their absence raises serious questions.

However, we are seeing progress, especially in terms of the priority that management at our large banks is placing on BSA compliance. Establishing an effective compliance culture starts at the top, and it is critical that the board and senior management set the right tone and that their message permeates the entire organization. Not only must the board and senior management send the right message, but they need to "walk the talk" by ensuring that there is an

alignment between good compliance practices and the bank's system of compensation and incentives. All managers—not just the ones who work in compliance—share in the responsibility for BSA/AML compliance, and those who engage in good compliance practices should be rewarded, while those who neglect their compliance responsibilities should not be, regardless of how much they have contributed to the bottom line.

Many of our largest institutions understand this, and have strengthened their commitment to BSA/AML compliance. For some of them, this has meant increasing the amount of resources and expertise dedicated to their BSA/AML programs. While the effectiveness of a bank's program is not always directly correlated to the amount of money it spends on BSA compliance, these types of commitments are nonetheless impressive and represent a step in the right direction.

Beyond committing resources, we are also seeing banks take a more holistic approach toward BSA. Rather than house responsibility for BSA/AML compliance in a single unit, they are beginning to disperse accountability throughout the organization so that every business line has some responsibility for evaluating BSA risk. That's crucial, because BSA isn't just a problem for the teller platform or the wire transfer room, it's a risk that manifests itself throughout the bank. This is particularly true in the M&A context, where some institutions have inherited significant BSA problems from the acquired institution, so it's vital that due diligence in an acquisition go beyond credit portfolios to include a look at the target institution's BSA program.

While regulated institutions are improving their BSA/AML programs, I think there is much more that we in government can do to make the system work better. An example of this is in the area of information sharing. The BSA/AML regulatory regime cannot be successful

without robust information sharing among institutions, from institutions to the government, and from the government to institutions. To this end, we have made a number of recommendations to promote better information sharing. For example, we've recommended legislation that would encourage the filing of Suspicious Activity Reports, or SARs, by strengthening the statutory safe harbor from civil liability for financial institutions that file SARs. That's important, because the courts have offered contrasting views of when the existing safe harbor protections would apply. One court decision held that a bank must have a "good faith belief" that a violation occurred, while other courts have provided banks and their employees unqualified immunity from civil liability upon filing a SAR.

This legislative fix would clarify that the filing of a SAR does not require a showing of good faith, which can sometimes be hard to prove. It's important to law enforcement that these SARs get filed, and this amendment would help by clarifying that financial institutions don't expose themselves to civil liability simply for complying with federal law.

We also support a broadening of the safe harbor for institutions that share information with each other about potential crimes and suspicious transactions. Presently, under section 314(b) of the PATRIOT Act, institutions can only avail themselves of the statutory safe harbor against civil liability if they share information that is related to money laundering or terrorist financing. We support expanding this to include all specified unlawful activities under the money laundering laws.

And finally, we have recommended that the government explore ways to provide more robust and granular information about money laundering schemes and typologies to institutions in a more timely way, perhaps using the mechanism created by section 314(a) of the PATRIOT Act, so that institutions can use that information to identify and report suspicious transactions.

While these types of fixes could make the Bank Secrecy Act work better, there is still more that could be done, especially with respect to the use of technology. I will have more to say about that later on, and I confess that I do worry that we may be spending too much time fighting the last war and too little time preparing for the next one, which will undoubtedly be more high tech and more reliant on systems that do not involve regulated financial institutions.

It's already a challenge to keep up with the pace of change. As banks' BSA compliance programs have evolved and changed over time, so has the sophistication and determination of criminal elements that are looking for access to our financial system. The technology, products, and services that banks and thrifts offer to give their customers better and quicker access to financial services can also be used by criminals to instantaneously and anonymously move money throughout the world, sometimes through the simple click of a keypad or the use of a cell phone app.

Risks are constantly mutating, as criminal elements alter their tactics to avoid detection. The bad guys have ample resources, and they move quickly from one base of operations to another, finding sanctuary in places where law enforcement, or sympathy for U.S. policy objectives, is weakest. Illicit funds are like flowing water in that they go to the point of least resistance and continually move and change direction from one institution to the next.
To assist and encourage this flow, money laundering schemes have had to become more sophisticated and complex, involving entities and individuals located in numerous jurisdictions worldwide. Consequently, banks, thrifts, and other financial institutions have had to devote increasingly larger amounts of resources to maintain effective programs to prevent this flow.

So clearly, it's going to be a challenge, for financial institutions, regulators, and law enforcement, to stay ahead of the curve. Right now, we're seeing a number of trends and areas of concern that warrant close attention by both regulators and banks.

First is the lack of compliance resources. In many of the most recent cases, our examiners concluded that the institution failed to commit adequate resources to its BSA/AML program. Austerity programs have led to a reduction of staff and other resources at some banks, and at others, programs have failed to keep pace with the institution's growth.

A second area involves international activities. Foreign correspondent banking, cross-border funds transfers, bulk cash repatriation, and embassy banking have all been high-risk areas that some banks have not managed effectively. Going back a few years, the failure of Riggs to manage its embassy-banking program ultimately led to the demise of one of the nation's most storied banks. Controls in this area need to be commensurate with the risks.

Third-party relationships and payment processors also require attention. BSA isn't the only area in which banks have stumbled because they failed to monitor work that was being done on their behalf by third parties, but it's one with perhaps the most significant consequences. The OCC has been monitoring this area closely over the years. Last month, we issued new guidance on third-party relationships and highlighted BSA/AML as an area that should be assessed in the planning process.

There's also a significant risk that these activities will migrate to smaller banks and thrifts as larger institutions improve their programs and exit businesses that present elevated levels of risk. Smaller institutions may lack the resources and personnel necessary to successfully manage higher-risk activities, and so they need to be especially vigilant.

And now, back to technology. The last trend I want to highlight involves how new technologies have affected BSA/AML compliance, particularly with respect to evolving payment activities. As banks and thrifts introduce new technology, it's vital that they understand the compliance risk.

Let's take the example of new payment systems, some of which exist outside the traditional banking and thrift industries. PayPal has become a familiar payment mechanism for many of us, especially when we make a purchase on the Internet, and a bank account today can effectively consist of nothing more than a plastic card that is capable of receiving paychecks, paying bills, and storing money.

These types of innovations add to consumer convenience, and financial institutions that want to remain competitive will find it necessary to offer products that take advantage of new technology. But some of them also bring compliance risk. How do we track illicit money when it can be quickly and easily moved throughout the world with nothing more than a cell phone? The emergence of digital currencies suggest that the future will be even more challenging.

I don't have any easy solutions to offer for addressing the BSA/AML risks presented by these types of emerging payment technologies. But just as emerging technology can create risks, it can also offer solutions. The same technologies that can be exploited for illicit purposes can also be employed to combat money laundering, terrorist financing, and other forms of illicit activity. Perhaps the time has come to explore these sources of technology as a means of providing more accurate, timely, and better information to law enforcement and regulators, and to reduce the significant costs and burdens imposed on banks and other financial institutions. I'm not saying that to suggest that the current system is in any way falling short, but only to

suggest that the challenges of the future are likely to grow exponentially more complex, and they may call for new approach and skill sets.

We've achieved a great deal in the area of BSA/AML compliance. But the challenges are growing along with the risks, and it will take all of our efforts – as well as all of the resources we can beg, borrow, or buy—to keep up.

Thank you. I'd be happy to now take your questions.