

**REMARKS OF WILLIAM J. FOX, DIRECTOR  
THE FINANCIAL CRIMES ENFORCEMENT NETWORK  
UNITED STATES DEPARTMENT OF THE TREASURY**

**PROVIDED TO THE**

**AMERICAN BANKERS ASSOCIATION / AMERICAN BAR ASSOCIATION  
MONEY LAUNDERING ENFORCEMENT SEMINAR**

**MONDAY, OCTOBER 25, 2004  
HYATT REGENCY CRYSTAL CITY  
ARLINGTON, VIRGINIA**

Good morning ladies and gentlemen. It is a pleasure for me to be with you here at the 2004 Money Laundering Enforcement Seminar sponsored by the American Bankers Association and the American Bar Association. I want to thank Seminar Co-chairs John Byrne and Gordon Greenberg and the Seminar Advisory Board Members for inviting me to speak to you this morning. It is also a pleasure for me to see so many faces that have become familiar over the past year. The association I have developed with many of you – a truly first class group of professionals and citizens – is one of the most gratifying aspects of my professional career to date. I wish to thank you for those associations and, on behalf of Secretary Snow, I wish to thank you all – financial institutions; law, accounting and consulting firms; and other organizations for your truly outstanding corporate citizenship. The financial sector has led the way in working to make our country safer and its financial systems more secure from the abuse by criminals and terrorists. I want you to know that we know and understand the commitment your institutions have made to this effort, and I want you to know that we appreciate it. Finally, thanks for getting up so early to hear me this morning.

My good friend John Byrne appropriately titled this morning's session as "FinCEN: Has it been a Year Yet?" As some of you may know, on this coming December 1<sup>st</sup>, I will have been at the Financial Crimes Enforcement Network for a year. There have been moments over the past year that I would have suggested a more apt title for this presentation, such as "FinCEN: Stop this Ride and Let Me Off." Thankfully, those moments have been fairly few and mostly far between and I think we have done some good work over the past year at FinCEN. To start, we have developed a new strategic plan that should be ready for publication around the first of the year. This plan will provide clear direction about where we are going and how we are planning to get there not only to the team at FinCEN but to our overseers, financial industry stakeholders and to our ultimate bosses – the American public. We have restructured FinCEN's organization to better reflect its mission and responsibilities. We have contracted with EDS to build and implement by next October the keystone of FinCEN's future technology architecture – BSA Direct – which will ensure that the collection, storage,

analysis and dissemination of information reported by your institutions is accomplished in a 21<sup>st</sup> Century state of the art environment that is efficient, easy to use, more secure and ensures a much more robust exploitation of the information you report. FinCEN was once known as a place where cutting edge technology was employed to address the complex problems of financial crime. With BSA Direct, we will be poised to become that place again.

We have also during the past 11 months, and maybe for the first time, taken our role as Administrator of the Bank Secrecy Act seriously. I believe we have established a more open and honest dialogue with the financial industry we regulate. A Memorandum of Understanding we reached with the Federal functional banking regulators is a manifestation of how we have changed the way we will interact with the regulators to whom we have delegated responsibility for examination. We have created an “Office of Compliance” in our Regulatory Policy and Programs Division and for the first time, have devoted a significant percentage of our analytical resources at FinCEN to our regulatory programs. We are working on publishing formal staff commentaries to our regulations; and, we have reinvigorated the Bank Secrecy Act Advisory Group, which is a critically important forum for the policy formulation and dialogue between the government and industry. We even may correct the “OFAC / SAR Guidance” published in the November 2003 *SAR Activity Review* – before its first year anniversary. Notwithstanding this good work, it is clearer to me than it was when I walked through the doors of that strange building out in Tyson’s Corner last December that we have a lot of challenges to meet and we have a long way to go.

I would like to highlight one such challenge for you today. I believe this is one of the most visible, and arguably one of the most significant challenges we are facing together as we try to implement the Bank Secrecy Act. But before we get to that, maybe it would be good to revisit why the government and the financial industry are spending tens of millions of dollars, if not more, on implementing and complying with the regulatory regime implemented under the Bank Secrecy Act – a regime that is critical not only to the safety and soundness of our financial system, but to the safety and soundness of your financial institutions as well. Indeed, if my work before I came to FinCEN taught me anything, it taught me that the proper implementation of the Bank Secrecy Act – as it has been amended by Title III of the USA PATRIOT Act – is critical to the national security of our country.

What was the Congress trying to achieve by passing the collection of statutes we have come to know as the Bank Secrecy Act? Has the Executive fully and faithfully executed those laws in a way to achieve the purpose of the Bank Secrecy Act? If it is true that this regulatory regime is critical to both our national security and to the integrity of our financial systems and institutions, then together we must ensure that we keep our collective eyes on the ball – we cannot tolerate failure, either in whole or in part.

The central purpose of the Bank Secrecy Act is to safeguard the U.S. financial system and the financial institutions that comprise that system from the abuses of financial crime, including money laundering, terrorist financing and other illicit finance.

The Bank Secrecy Act achieves this purpose in two principal ways: 1) by ensuring that financial institutions create policies, programs, procedures and systems that will help protect themselves from financial crime; and, 2) by making information available to the government – through required recordkeeping and reporting – that will be highly relevant to the prevention, deterrence and investigation of financial crime.

With these purposes in mind, let's go back to the challenge I would like to discuss today. This challenge is not picayune. It goes to the very heart of the purpose of the Bank Secrecy Act regulatory regime. I am certain we do not have all the answers to meet this challenge – I am also certain that the answers do not reside in the government alone. I believe that if we do not meet this challenge, our ability to fully succeed in implementing this country's anti-money laundering / anti-terrorist financing regulatory regime will be handicapped. The challenge is to address the phenomenon of "defensive filing" of suspicious activity reports. The "defensive filing" of suspicious activity reports results when an institution files a suspicious activity report on an activity or transaction that really is not suspicious. Our regulations require the filing of suspicious activity reports when an institution "knows, suspects, or has reason to suspect" that a transaction or an attempted transaction 1) involves funds derived from illegal activity or is intended to disguise funds derived from illegal activity; 2) is designed to evade the requirements of the Bank Secrecy Act; or, 3) has no business or apparent lawful purpose. We all know this phenomenon is occurring – we have both empirical and anecdotal evidence we can cite. We have seen financial institutions file reports in ever increasing numbers – often upon the recommendation of their lawyers or risk management teams – when the facts as presented do not meet this standard. I suspect that this over compliance is occurring for a reason. It is occurring because financial institutions are –justifiably in my view – unwilling to accept the regulatory or reputational risk associated with an action by the government that would make it appear that the institution is soft on anti-money laundering or, even worse, on terrorist financing.

I often hear, "why should it matter to you if the banks are filing on anything? Aren't you better off with more information?" From a purely investigative standpoint, the answer may be yes and may be no. It is true that we can handle the storage, and maybe even the filtering of additional information. Computer memory is fairly cheap these days, and we are developing technological tools that should allow us to separate the wheat from the chaff. The problem with this sort of filing is that it leads to a dilution of the value of suspicious reporting as a whole. This type of reporting becomes less valuable to law enforcement when the reports document activity or transactions that are not indeed suspicious. It also means we have reports on transactions or activity that have no business rattling around in a government computer. The privacy implications of defensive filings are clear.

In order to fully discuss this phenomenon in an honest and open way, we really need to talk about the pink elephant that plopped herself right in this very room – the affect of the significant civil enforcement and other actions that have been taken under the Bank Secrecy Act by regulatory and enforcement agencies of the government – including FinCEN – against financial institutions since last spring.

Civil enforcement actions taken by the government, if handled correctly, should result in greater compliance by the institution that was the target of the action. Such actions should also educate the rest of the financial sector and, therefore, result in greater compliance by the industry as a whole. For example, the actions we have taken this past year – which have been significant – have been taken against institutions that have been found to have had significant programmatic failures. These actions have certainly caught the attention of the targeted institutions, and we believe that the programmatic failures addressed by those actions are being addressed by these institutions. Moreover, and perhaps more significantly, the orders implementing these actions were written as a “road map” for other institutions to follow so they can prevent similar programmatic failures in their institutions. If that is not the case – in other words if our orders are not useful to other institutions as they assess their compliance programs – we need to hear it because that is a very important aspect of any civil enforcement action.

Unfortunately, often what gets communicated about a civil enforcement action to the broad community is the name of the institution, the size of the civil penalty and some vague description of the basis for the action, which usually gets distilled down to “failure to comply with anti-money laundering laws.” Even inside the “compliance community” I hear some pretty astounding misperceptions about the enforcement actions we have taken. These misperceptions reveal that those persons have not really taken the time to read let alone study our enforcement orders for the guidance that is contained therein. Or it may mean that we got it wrong when we issued those orders.

Other actions are contributing to the misperceptions about what it means to comply with the Bank Secrecy Act and, in a very real sense, are raising the stakes of non-compliance in a way that perhaps sends the wrong message to the industry as a whole. In a very recent action taken by the United States Attorney’s Office for the Southern District of Mississippi, an institution agreed to the forfeiture of \$40 million for failure to file suspicious activity reports and failure to file accurate suspicious activity reports. This action was taken at the same time we – FinCEN and the Federal Reserve Board – took action to address programmatic failures at the same institution. This forfeiture was made in the context of a “deferred prosecution agreement” where the government agrees to defer the criminal prosecution of an institution for a period of time until the institution takes certain corrective measures. Assuming that the corrective actions are taken, once the time period is up, the matter is dismissed, with prejudice.

Without commenting on this particular case, I have very serious concerns about what appears to be a trend to criminalize behavior designed to be governed by civil standards. The Bank Secrecy Act, like most regulatory statutes, has criminal provisions that are reserved for persons who commit the most egregious behavior – that is, those who willfully, with specific criminal intent – violate the provisions of the Act. And let me be clear . . . from my perspective, if an institution, or individuals in an institution engage in such egregious criminal activity, I believe that institution or individuals should be prosecuted and I suspect that most of the people in this room agree with me. However, if institutions begin to believe that they will routinely be targeted for criminal

investigation and prosecution for failure to properly implement the Bank Secrecy Act's regulatory regime, it is natural that institutions will take all steps necessary to ensure they are protected from such risk. It is not a large leap to understand why institutions are beginning to report on any transaction that is at all unusual, even if it is not necessarily suspicious as that term has been defined by our regulations. Certainly, fallout from these actions – particularly when they are misunderstood to mean something they are not – has contributed to the “defensive filing” phenomenon. One has to ask whether these actions are helping or hindering us in achieving the purposes of the Bank Secrecy Act that I outlined a few lines ago. Is our country safer when institutions are defensively filing suspicious activity reports? Does our financial system have more integrity when defensive filing occurs?

So what is the answer? From the government's perspective, I think we need to be very careful to properly communicate our message when we take enforcement actions. The message is not only to the targeted institution, but to the industry as a whole and we have to remember that. I think our enforcement actions should be public, and these actions should provide a written road map from which other institutions can learn. We cannot afford to have the tactical overtake the strategic. From the industry, it seems to me we need two things: 1) we need you to not overreact to our enforcement actions, but to read, study, and learn from the road maps we provide you when we take such actions. If our road maps are ambiguous, or if they leave questions, then we need you to ask those questions – I'll promise we'll get you the answers; and, 2) we need your continued commitment to institute programs, policies, procedures and systems to protect your institution and the U.S. financial system from the abuses posed by criminals and terrorists.

It's not just enforcement actions that are leading to the phenomenon of defensive filing. I think we can all agree that the increased attention bank examiners are providing to Bank Secrecy Act compliance has resulted in an increase in defensive filings. Examining for Bank Secrecy Act compliance has certainly become a higher priority for the banking regulators. Congressional oversight hearings this past year in both the Senate and the House have resulted in these issues receiving more and higher-level attention at these agencies. Policies such as “zero tolerance” and transaction testing have become *de rigueur* in the examination process. While I am completely comfortable that the policy makers at these agencies understand the difficulties and nuances associated with complying with the Bank Secrecy Act – particularly the provisions relating to suspicious activity reporting – it is often very difficult to translate these policies to the men and women who actually have to implement them. It is easy for me and my colleagues at the Fed, the OCC, the FDIC and the other regulators to talk about theory behind risk-based regulation and setting up programs, policies, procedures and systems to address financial crime. It is quite another thing for an examiner who has to operate on the ground to ensure that that theory is implemented. We hear too many stories of bank examiners evaluating institutions based upon the number of suspicious activity report filings made at similar sized institutions to ignore the problem or pretend it is not there. While I believe the bank regulators are doing a very good job, and while I welcome the increased profile and attention Bank Secrecy Act compliance has been given this past year, together we

must make sure that the examination program for Bank Secrecy Act compliance is being implemented correctly on the ground. I know this is easier said than done.

The good news is that we are working hard on the problem together. First, our new Office of Compliance, which William Langford will tell you more about later today, will be collecting information from the bank regulators to try to discern those systemic areas that need to be addressed through clarification, guidance or training. We have a dedicated subcommittee of the Bank Secrecy Act Advisory Group co-chaired by Bridget Neill of the Fed, John Byrne from here at the American Bankers Association, and Alan Sorcher of the Securities Industry Association. This group is studying ways we can increase the consistency in Bank Secrecy Act examinations and ensure examinations are focused on achieving the goals of the statute. Last, but certainly not least, the bank regulators, through the FFIEC, are currently reviewing Bank Secrecy Act examination procedures and training. The regulators have invited us to participate in that process and we have enthusiastically agreed to do so. With more and better information flowing, sharper policy guidance, better industry dialogue, and consistent exam procedures and exam training, I believe we will go far to ensure a better, more consistent, examination process for Bank Secrecy Act compliance. What we need from you is honest and candid feedback on how it is going, so we can assess our efforts and adjust course if necessary.

As I said earlier, I am sure that these are not all the answers to the problems associated with defensive filing. I am certain there are other ideas out there that we could all benefit from – ideas that can make this system better. Please make sure we hear them. You have my commitment and the commitment of my agency that we will listen to your ideas and do all in our power to make this system better. There are many other challenges I could have spoken about today. I could have spent half the conference talking about implementing Section 314(a) of the USA PATRIOT Act in a real way. But time forces me to address those challenges at another time. Again, I would like to thank John, Gordon and all those who work to make this conference what it is and for making me a part of this conference. I appreciate very much your kind attention this morning.