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

THE 23RD CAMBRIDGE INTERNATIONAL SYMPOSIUM ON ECONOMIC CRIME

THE BUSINESS OF CRIME
THE ENTERPRISE OF CRIME AND TERROR
THE IMPLICATIONS FOR GOOD BUSINESS

MONDAY, SEPTEMBER 5, 2005

Good morning. Chairman Froomkin, Professor Rider, distinguished colleagues, ladies and gentlemen, I am honored to be a part of the 23rd annual Cambridge Symposium on Economic Crime and to share keynote responsibilities this morning with this distinguished panel of officials and experts in this field. True to the tradition of this great University, this Symposium is known the world over for its depth of intellectual pursuit of ways to address economic crime. This Symposium continues to be a premier forum where experts from around the world come to teach, learn and discuss the important developments on issues relating to economic crime. I am very pleased to again be a part of this program and I commend Professor Rider, Mr. Froomkin, Jesus College of the University of Cambridge and the other supporting and organizing institutions who all ensure that this important symposium remains relevant and valuable to those of us who deal with these important issues day to day.

The focus of this year's symposium is on the Business of Crime. Not only how criminal and terrorist organizations leverage or exploit financial and other business to further their illicit purpose – most of us here have known much about that for some time – but, also, on assessing just how this criminal exploitation of the financial system is affecting legitimate businesses and economies. The relevance of this topic is obvious. The blood spilled by terrorists this past summer in London is yet another reminder of the urgency with which we all must proceed.

So how do we begin that assessment? The global financial system, as it has evolved, is largely free and open. Every second of every day, transactions take place and contracts are satisfied between people on opposite sides of the world in a matter of seconds with very little, if any, interference. The advent of internet payment systems and developments in communication technology are examples of cutting edge mechanisms involving the movement of value. I suspect that most here would agree that the evolution of the global financial system is irreversible and, generally, a good thing certainly for legitimate business but also for the human condition. We all can accept the fact that the globe is continuing to shrink. Ways to move money around the world will continue to develop and will become accessible to more and more people around the world and I think we all agree that with the development of systems to move money, there will be more efforts to game this system for illegitimate purpose.

That is where people like me come in. For those of you that do not know me, I am the Director of the United States financial intelligence unit – the Financial Crimes Enforcement Network, or FinCEN as we are sometimes better known. The stated mission of my agency is to "safeguard the financial system from the abuses of money laundering, terrorist financing and other financial crime;" quite a lofty goal. My agency is responsible for administering the principal anti-money laundering and counter terrorist financing regulatory regime in the United States – the Bank Secrecy Act. Boiled down to its essence, this Act has one purpose: to increase the transparency of the U.S. financial system so that money laundering, terrorist financing and other economic crime can be deterred, detected, investigated and prosecuted. The Bank Secrecy Act attempts to achieve this purpose in two ways: First, by ensuring that financial institutions create policies, programs, procedures and systems that will help make our financial system more transparent, and will help protect financial institutions – and therefore, the financial system – from being conduits for financial crime through the proper identification of customers and the detection of suspicious financial activity; and, second, by making information available to the government – through a system of required recordkeeping and reporting – information that is highly relevant to the detection, prevention, deterrence and investigation of financial crime. Our regulatory regime in the United States is similar to other regimes in countries and jurisdictions around the world – particularly countries and jurisdictions that subscribe to the forty plus nine recommendations promulgated by the Financial Action Task Force.

Clearly, financial institutions and governments are spending great amounts of financial and human capital ensuring compliance with these regimes. Assessing the impact of that effort is a wise and timely thing to do. The question was placed before us very eloquently by the Co-Chairman of this symposium last night at dinner. The Co-Chair was describing the customer identification procedure he recently had to go though in a bank in his home jurisdiction of Bermuda in order to complete a financial transaction. The identification procedure sounded quite rigorous. And our Co-Chair had to go through that procedure even though there are only 64,000 souls residing on the island and most of those 64,000 – including the banker handling the transaction – know

our distinguished Co-Chair well. Basically, it is the same question asked by the U.S. Community Banker in a town of 5,000 people who files a currency transaction report on his friend and neighbor who happens to run the local Wal-Mart in town. The banker knows his friend and neighbor just happens to be in a business that draws a lot of cash. He knows his friend and neighbor is upstanding and the business he is conducting is legitimate. The banker knows his customer. The banker would know whether his friend was up to something untoward. So the banker wonders what possible good can come from the filing of this report with the government.

Moreover, today for legitimate financial businesses there is a significant regulatory and reputational risk associated with running afoul of anti-money laundering / counter-terrorist financing regulatory regimes. Over the past 15 months in the United States for example, we have had a series of significant, systemic failures on the part of financial institutions that have resulted in well-publicized actions with high civil money penalties. In some of those cases, our Department of Justice has followed with significant actions of their own to settle potential criminal culpability. These failures have been rightly featured and discussed in the pages of our most important news media. Couple this with the increase in the attention and rigor with which banking regulators have approached this regime and it is no wonder we have seen a significant increase in suspicious activity reports filed "defensively;" that is, filed not to document truly suspicious activity but to prevent some perceived regulatory or reputation risk posed to the institution. We are aware that the same phenomenon is occurring here in Europe.

This perception – or misperception – of risk has had dramatic consequences. By way of example, a large portion of the money services sector – particularly money remitters – are having their banking relationships terminated. Not only is this bad for the world economy, it forces certain remitters underground outside of the transparent banking sector.

Add to all of this is the question whether the systems we have built to ensure financial transparency – most of which were aimed at money laundering stemming from the illicit narcotics trade – are sufficient to provide governments with the information needed to vigorously detect, investigate and disrupt terrorist financing – arguably our most serious problem.

So, have the regimes we have created all been for naught? Have these regimes failed? Certainly not. Every day, the information we collect is in some way helpful to law enforcement and others in their efforts to detect and investigate financial crime – including terrorist financing. Law enforcement and our security services are consistently ratifying what we know from our analysis: that this information is critical to understanding, detecting, investigating, prosecuting and deterring money laundering, terrorist financing and other illicit finance. While the discipline and cost of customer identification and other anti-money laundering programs may appear in a particular instance unnecessary, this discipline has made financial institutions ultimately safer from

the abuses of financial crime and, if implemented correctly, have brought the institutions much closer to knowing their customers.

Those successes notwithstanding, we must recognize that there is clearly need for improvement – not only in the regimes, but in the way the regimes are implemented – if we are ever going to achieve the laudable goal of safeguarding the financial system from criminal abuse. Following are some of my thoughts about what we all need to do if we are to make this regime work better that, hopefully, will be worthy of your consideration as you continue through the symposium this week:

First, if I have learned anything since I have been in this job, I am convinced that if we are ever going to achieve our goal of truly safeguarding the financial system from criminal abuse under the current paradigm, the government and private sector must act in true partnership. What does that mean? The word "partnership" gets thrown around an awful lot these days, at least in the United States, and this tends to breed a great deal of cynicism. Partnership demands a commitment on both sides. For the private sector this means a commitment to develop and implement reasonable, risk-based programs to address the risks of financial crime posed by each private sector member's business lines and customer base. This program should result in the reporting of suspicious activity and other relevant information to the government when appropriate. The government, in turn, must educate the private sector about the risk and – most importantly – be willing to share information with the private sector so they can develop their programs to address the risks associated with their business and customers. Sharing relevant sensitive information with the financial sector in a deeper and richer way necessarily breaks several old and deeply entrenched paradigms. It brings the financial sector into a more collaborative relationship with the government while also minimizing the impact on legitimate commerce. The 20th Century paradigm of governments alone protecting their citizens from outside threats is no longer valid in a post-September 11th world. This paradigm simply no longer applies when enemies can melt into society and commandeer aircraft to use as missiles of devastation, or when a group of mad men board public transportation and murder innocent souls who are simply trying to live and work in the world. Good partners talk with one another. I am convinced that if we are to make the present regime work, government and the private sector need to be in a constant dialogue on these issues.

Secondly, we must continue to monitor and assess our regimes and make reasonable adjustments when required. The criminals who are attempting to game the system are nimble and flexible. We must keep our eyes on the goal. If a particular requirement is not working to achieve the goal, we should relieve the burden. Likewise, if we need to do something in a different way to achieve the goal, we should be willing to do that.

Finally, it is also important to remember that the movement of money in the 21st Century – legitimate or illegitimate – knows no borders. Economic crime, including terrorist financing, has a global reach. Both the government and the private sector must

pursue greater international cooperation and collaboration on these issues if we are to achieve our goal of safeguarding the financial system from criminal abuse.

The development of financial intelligence units is instructive here. In 1995 there were only a handful of operational units established pursuant to the Financial Action Task Force recommendation that nations set up a centralized entity to receive, review and make available to appropriate authorities financial transaction reports required by regulation and filed by financial institutions. A number of those units, or "FIUs" as they have become known, met at the Palais d'Egmont in Brussels in 1995 and created what we have come to know as the Egmont Group of Financial Intelligence Units. The goals of that first meeting were to "start finding practical ways for information sharing and practicable solutions for eliminating barriers to such exchanges" among Financial Intelligence Units.

The Egmont Group has collectively accomplished much toward those goals, in a pretty spectacular fashion. Right now that original handful of "FIUs," as they are known, has expanded to 101 nations and jurisdictions that have made a commitment to put the resources in place to accomplish what FATF envisioned. For the past ten years, the Egmont Group has been rightly focused on establishing standards for membership and on expansion. I am pleased to report that the Group's focus is changing from standards and membership to operations. In other words, how do we ensure that the sharing of information is occurring in a timely and effective way and how do FIUs around the world work together more collaboratively and cooperatively to ensure greater global financial transparency? Movement in this direction is essential, in my view. Wolfsburg is a fine example of the private sector doing the same thing.

We must also continue to collectively build competence and capacity. Significant areas of the world, South Asia and Africa for example, continue to lack the capacity and regimes to address the problems of economic crime. Whether it is regulating the diamond and precious gem cutting center in Mumbai or the banking sector in Nigeria, building regimes that ensure greater financial transparency continues to be incredibly important and should be pursued collectively with all urgency.

I very much appreciate your kind attention this morning. I hope my comments will give you something to think about as you proceed through the week. I look forward to listening, learning and discussing these important issues with you. Again, thank you to Professor Ryder, Mr. Froomkin and to Jesus College of Cambridge University for creating this terrific forum to discuss these critically important issues.