Robert M. Morgenthau is the district attorney for New York County. He was elected to the position in 1975. Prior to that, he was the United States attorney for the Southern District of New York.

Adam S. Kaufmann is an assistant district attorney for New York County. He is also chief of the central investigations division in the office, responsible for leading complex white-collar and financial criminal investigations.

TESTIMONY BY

THE HONORABLE ROBERT M. MORGENTHAU
DISTRICT ATTORNEY FOR NEW YORK COUNTY, STATE OF NEW YORK

AND

ASSISTANT DISTRICT ATTORNEY ADAM S. KAUFMANN
CHIEF OF INVESTIGATION DIVISION CENTRAL
NEW YORK COUNTY DISTRICT ATTORNEY'S OFFICE

BEFORE THE UNITED STATES SENATE
COMMITTEE ON FOREIGN RELATIONS

HEARING ON U.S. STRATEGY REGARDING IRAN
WASHINGTON D.C.
MAY 6, 2009

We would like to express our appreciation for the work undertaken by the Committee, and our gratitude to the Committee, and Senators Kerry and Lugar, for the opportunity to appear on this important issue. There are few issues in international security policy more pressing than Iran's efforts to develop long range ballistic missiles and nuclear weapons. To the extent that the Manhattan District Attorney's Office has played a role in enforcing U.S. sanctions and the rule of law through the use of traditional law enforcement means, we welcome the opportunity to discuss two recent investigations.

The Office of District Attorney for New York County has a unique role in the law enforcement community. The office of a local prosecutor is charged with maintaining the safety and security of the public he or she represents. However, in the case of New York County, the task of protecting the public and maintaining the public trust includes policing the most important financial markets in the world, watching over the biggest financial institutions on the planet, and ensuring the integrity of the global financial system. From Main Street to Wall Street, from Harlem to the Financial District, the Manhattan D.A.'s Office endeavors to maintain that public trust. To put it another way, there is nothing like a good beat cop to keep the streets safe, and the District Attorney's Office is the beat cop for Manhattan's city streets and its financial markets and institutions.

Our international investigations have covered many areas, both in geography and criminal conduct. Our investigation and prosecution of members of BCCI in the early 1990's, a matter well known to Chairman Kerry from his investigation of the same group, shined a spotlight on corrupt banking practices and the undisclosed involvement in U.S. banking activities by secret interests in the United Arab Emirates and Pakistan. We could not have successfully prosecuted BCCI without the expertise and assistance of Senator Kerry and the staff of the Foreign Relations Committee. We investigated and prosecuted the looting of a Venezuelan-owned bank by its wealthy owners in the early 1990's, and also discovered their payments of illegal campaign contributions to U.S. political interests through intermediaries in the United States. More recently, we have brought cases to highlight problems associated with black market casas de cambio in Brazil, Uruguay, Paraguay and Argentina and the U.S. banks that turned a blind eye to their misconduct. These investigations tracked money flowing from the Tri-Border Area of South America to bank accounts associated with terror organizations in the West Bank; as well as the use of black market systems to launder millions of dollars of embezzled public funds from Brazil to secret accounts in Switzerland and the Isle of Jersey by Paulo Maluf, the corrupt former Mayor and current Congressman from Sao Paulo, Brazil. Other cases have included the use of electronic digital currency and U.S. shell companies by Russian organized crime to perpetrate identity theft and fraud, the use of offshore shell companies by a securities fraud ring to launder its illegal proceeds and hide its activities, and our ongoing efforts to target and bring to justice the tax cheats who use offshore accounts and shell companies to avoid paying their fair share of taxes.

All of these cases, and many others pursued by the District Attorney's Office, involve the misuse of New York banks by criminals to launder ill-gotten goods or otherwise violate the criminal laws of New York State. And, they share a common theme. In each case, the investigation of discrete criminal conduct by specific individuals served to illustrate black market or otherwise opaque financial systems that allowed criminals to move their money. Corrupt and illicit systems are often set up to facilitate tax evasion and capital flight, but are also susceptible to use for more sinister purposes by criminals and the financiers of terrorism. Once an underground system exists to help people move money anonymously, those in control of it become accustomed to not asking too many questions, and criminals and terrorists can, and will, take advantage of that. Bringing these criminal cases has exposed these systems to the strong light of day, and has contributed to the recognition of systemic problems by the financial industry and financial regulators. To paraphrase Justice Louis Brandeis, all of these cases demonstrated the powerful disinfectant ability of sunlight. This theme – of transparency – runs through all of these cases and is evident in the matters we will address today.

More recently we turned our attention - and brought a degree of sunlight - to dangers well known to this Committee: The threat to the United States and global peace posed by Iran's efforts to build nuclear and long range ballistics missiles. Our focus today is not on U.S. policy toward Iran *per se*, rather it is on the enforcement of the rule of law and the implementation of transparency in cross-border payments in the international banking system. The two investigations highlighted today examine the efforts of Iran and its providers of weapons material to move money through the international markets, including banks in New York, through deceit and fraud. Our efforts uncovered a pervasive system of deceitful practices and fraud designed to let Iranian banks skirt U.S. and international sanctions and move money all

over the world without detection. It is our hope that this hearing, and our testimony, will enhance efforts to curtail these practices and have an impact on the enforcement of sanctions and the adoption of transparent banking practices worldwide.

Our efforts have, thus far, led to two publicly announced investigations that culminated in a deferred prosecution agreement with a British bank and with the indictment of a Chinese citizen and his corporation. We will refer to these two matters as the Lloyds investigation and the Limmt indictment, respectively.[1]

One important goal of cases like the Lloyds investigation and the Limmt indictment is to encourage change from within the banking industry and bring change to the regulatory playing field. Regulatory schemes are generally, and appropriately, set up to work with industry to adopt government policies. However, there is a degree of clarification brought by criminal prosecutions that differs from any regulatory inquiry, particularly when addressing intentional misconduct. Targeted criminal prosecutions of serious misconduct can send a message of deterrence that regulatory schemes cannot match. And, as discussed below, it is the effect of this message of deterrence in the banking community that may prove to be the most valuable result of these prosecutions.

Law enforcement plays an important role in cases involving violations of sanctions and intentional fraudulent conduct. If the United States imposes sanctions and requires U.S. banks to follow them, then prosecutors can target and expose to the light of day those who would intentionally violate the law and defraud our financial institutions. If foreign banks, businesses and persons engage in conduct that violates New York and United States law, they should expect to be held accountable for their misconduct. And the threat of public accountability has a tremendous deterrent impact on the conduct of banks and financial institutions. A recent article in the periodical *Foreign Affairs*, by Rachel Loeffler, recognizes and articulates this point.[2] Ms. Loeffler examines various sanctions and actions brought to enforce them, and notes the importance of interaction between government policy and financial institutions to curtail the access of rogue regimes to international money centers. She comments that enforcement actions such as the Lloyds deferred prosecution agreement "provide a lever of influence when fewer and fewer seem to exist." A foreign bank that might otherwise ignore U.S. sanctions in its business model might be reluctant to do so in the wake of the Lloyds settlement. As discussed further

[1] Cases such as these are the result of difficult and long-drawn investigations. We wish to recognize the efforts of the following members of the District Attorney's staff for their contributions to these matters. For Lloyds: Senior Trial Counsel Richard T. Preiss, Assistant District Attorney Aaron Wolfson, Investigation Division Central Deputy Chief Gary T. Fishman, former Assistant District Attorney Laura Billings, former Intelligence Analyst Eitan Arusy, Financial Intelligence Director David Rosenzweig, and Paralegals Gregory Dunleavy, Aaron Davidowitz, Sarah Schoknecht, and former paralegals Melissa Clarke and Jamelia Morgan. In addition, the investigation was pursued jointly with the Asset Forfeiture and Money Laundering Section of the Department of Justice and the New York State Banking Department, and the efforts of the federal prosecutors and federal and state investigators assigned to the investigation should be recognized. For Limmt: Assistant District Attorneys Adam S. Miller and Aaron T. Wolfson, Investigative Analysts Lauren Lichtman and Max Adler, Intelligence Analyst Jasmine Sicular, Financial Intelligence Director David Rosenzweig and Investigators Jonathan Savel and Alex Arenas of the DANY Special Investigations Group. Assistant District Attorneys Marc Krupnick and Marc Frazier Scholl, Senior Investigative Counsel, also assisted. In addition, a parallel investigation was pursued by the Office of Foreign Assets Control of the Department of the Treasury that resulted in SDN designations for activities relating to weapons proliferation. The expertise of the staff at OFAC as well as at the Federal Reserve Bank of New York provided a tremendous contribution to the success of the investigation.

[2] *Bank Shots: How the Financial System Can Isolate Rogue Regimes*, Foreign Affairs (March/April 2009).

below, we have seen multinational banks change their behavior after the Lloyds settlement, which makes U.S. sanctions more effective, further isolates the Iranian regime, and hampers Iran's ability to obtain items needed for its weapons programs.

These themes – transparency, accountability and deterrence -- are explored in the two case studies presented below.

I. "Stripping" of Wire Transfer Date: The Lloyds TSB Investigation and Deferred Prosecution Agreement

The term "stripping" refers to the practice of removing wire transfer information that would identify that the transfers originated from a prohibited source. By stripping out the originator information, the wire transfers can pass through the screening software used by U.S. banks that would otherwise reject or freeze them for further inquiry. The stripping of wire transfer information in this manner effectively conceals that the parties involved are sanctioned entities.

The United States government places restrictions on certain countries, entities and individuals from accessing U.S. financial institutions and the U.S. banking system. These sanctions are administrated and enforced by the United States Department of the Treasury's Office of Foreign Assets Control ("OFAC"). OFAC imposes controls and administers economic sanctions against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States. Many of the sanctions are mirrored in United Nations and other international commitments, and involve close cooperation with governments around the world. The sanctioned entities are blocked from accessing the U.S. banking system and, with minor exceptions, U.S. citizens and institutions are prohibited from conducting financial transactions with them.

In the Spring of 2006, the District Attorney's Office discovered evidence of fraud in the processing of international wire transfer by certain European banks on behalf of their client Iranian banks. The Iranian banks maintained correspondent accounts with the European banks. Correspondent bank accounts constitute the relationships between banks that allow funds to move all over the world, and are a foundation of international commerce.[3] In the case of Lloyds, Lloyds maintained correspondent accounts on behalf of a number of Iranian banks, all sanctioned entities banned from doing business in the United States or with U.S. financial institutions.

The initial evidence of criminal conduct by Lloyds and other banks discovered by prosecutors from the District Attorney's Office consisted of information concerning individuals with close ties to the government of Iran located in the New York area. These individuals received wire transfers from Bank Melli and other Iranian banks. However, the incoming wire transfers to the U.S. accounts of these individuals did not contain any reference to the Iranian banks or individuals that originated the funds transfers.[4] Instead, the payment messages made it appear

[3] The role played by international correspondent banking in global finance and the risk of money laundering it can pose is ably described and analyzed in a report from the U.S. Senate entitled *Role of U.S. Correspondent Banking in International Money Laundering*, Senate Permanent Sub-Committee on Investigations, July 15, 2004.

[4] These payment messages consisted of communications sent by the Society for World Wide Interbank Financial Telecommunication, or "SWIFT." SWIFT is the predominant system used for international funds transfers with over

that the wire transfers originated from Lloyds (or from other European banks engaged in similar practices).

To ensure that U.S. banks and financial institutions that process international wire transfers do not engage in prohibited transactions, they use sophisticated computer systems to monitor and screen all wire transfer activities. Banks in New York that process most of the world's U.S. dollar payments depend on these automated systems to prevent sanctioned entities as well as terrorists, money launderers, and other criminals from gaining access to the United States banking system. In this way, the financial institutions are the first line of defense to protect our financial system.

The Lloyds investigation focused primarily on its handling of accounts for financial institutions from three designated countries: Iran, Sudan and Libya (Libya was removed from the list of sanctioned countries in 2004 and was less prevalent in Lloyds' stripping scheme). Knowing that they could not legally access U.S. banks, Iranian and Sudanese banks with accounts at Lloyds sought to evade these sanctions. Beginning in the mid-1990's, Lloyds began removing any information from Iranian and Sudanese wire transfers that would trigger the detection systems at the U.S. correspondent banks. This was a systemic, across-the-board operation on behalf of the sanctioned banks. To execute this policy, Lloyds payment center personnel removed any Iranian and Sudanese wire payment messages from the automated processing system, stripped out the identifying data, and then manually re-entered the payment information so that the transfer would be processed undetected by U.S. banks.

From 2001 – 2004, Lloyds' conduct allowed the illegal transfer of more than $300 million on behalf of Iranian banks and their customers to accounts in the United States. In addition, Lloyds sent *billions* of dollars in Iranian payments through U.S. banks in so-called "U-Turn" payments (payments that begin and end in foreign banks that merely transit through the U.S.). For example, a U-Turn payment would include a commercial transaction sent from the account of an Iranian bank at Lloyds, through a correspondent account at a U.S. bank, for payment to an Italian company for a commercial invoice. U-Turn payments also included overnight time deposits sent on behalf of the Iranian banks themselves from Lloyds through correspondent accounts at U.S. banks to banks in Cayman and elsewhere, and then processed back to Lloyds via the same route the next day. In our opinion, the U-Turn exemption constituted a glaring hole that undermined both the enforcement of, and the rational behind, the Iranian sanctions program. Effective November 10, 2008, the authority for the U-Turn exemption was revoked.

While Lloyds voluntarily exited the Iranian business by 2004, the Sudanese business, which resulted in the illegal transfer of approximately $30 million, continued into 2007 (after the beginning of the investigation by the District Attorney's Office and the Department of Justice). Also during the period from 2001 – 2004, Lloyds' conduct allowed one Libyan customer to transfer approximately $20 million to U.S. banks.

80% of the world's transfers executed by SWIFT message, or almost 15 million payment messages per day on average. SWIFT can be likened to a secure e-mail system used by banks to ensure that payment orders are sent and received with accuracy and security.

The District Attorney's Office and the Department of Justice agreed that the appropriate resolution of the Lloyds investigation was through joint Deferred Prosecution Agreements. As a result of the settlement and Deferred Prosecution Agreements with the District Attorney's Office and the Department of Justice, Lloyds agreed to adhere to best practices for international banking transparency, to cooperate with ongoing law enforcement investigations, to conduct an internal review of past transactions, and to pay $350,000,000 in fines.

The message of deterrence from the Lloyds resolution should not be underestimated. In many of the financial industry's international anti-money laundering conferences in the past few months, the top item on the agendas is cross-border payment issues and the Lloyds case. While somewhat apocryphal, this observation highlights the deterrent effect of a successful criminal investigation, which goes well beyond the deterrent effect of a regulatory finding. This is not intended to undermine the value of regulatory work. To the contrary, most matters involving financial institutions are best handled by regulators who can identify problems and work with the banks to rectify them. However, intentional and systemic misconduct resulting in fraud constitutes criminal conduct and should be treated as such.

As we assess the deterrent effect of the Lloyds settlement, we have begun to observe a ripple effect move through the international banking community. At a recent anti-money laundering conference, one of the assistant district attorneys from the Lloyds investigation participated in a debate as to whether the Lloyds matter was an unwarranted extra-territorial application of United States sanction laws to a non-U.S. bank. We argued that Lloyds case was simply the application of domestic (U.S.) fraud provisions to conduct that originated in Europe but exercised its fraud on correspondent banks in the U.S. From the prosecutorial analysis, the violation of sanctions law was the motive and reason for the fraud, but the fraud perpetrated on the U.S. clearing banks was the gravamen of the criminal conduct. The charge in the state deferred prosecution agreement reflects the duality of this analysis. The charge admitted by Lloyds was a violation of the New York State Penal Law charge of Falsifying Business Records in the First Degree, alleging that Lloyds caused false entries to be made in the records of the U.S. clearing banks, in furtherance of and to conceal the commission of another crime, specifically, the federal sanctions/IEEPA violation. The federal deferred prosecution agreement charged a violation of IEEPA outright, but other charges also could have been proffered. The criminal conduct alleged in the Statement of Fact would also support bank fraud and wire fraud charges, either of which could be a predicate crime for money laundering (just as Falsifying Business Records in the First Degree is a predicate crime for state money laundering charges).

The final assessment of success for the Lloyds investigation and resolution will come from the deterrent effect and whether we successfully change behavior on the part of international banks. Already we have seen some impact as Lloyds becomes the topic of the day in conferences and industry periodicals. The impact on the international banking community was well reflected in comments from the head of global anti-money laundering for a major UK banking institution. This gentleman, who is a leader in the field of global compliance, explained that it mattered not whether one agreed with this application of U.S. law, or whether one viewed it as a criminal fraud case, or whether one viewed it as a violation of U.S. sanctions, or something in between. As he saw it, what mattered was that the world was now on notice that it could not disregard any country's sanctions without running afoul of the analysis employed in Lloyds. The result for his

bank, as he explained it, was two-fold. First, his bank was now looking at sanctions with a fresh eye to make sure that cross-border transactions originating in one country and transiting another did not violate any local sanctions regimes. Second, his bank was withdrawing or curtailing international payment services for banks from sanctioned countries such as Iran and Sudan. When we speak of deterrent effect and making sanctions more effective, this may be the ultimate model of success.

II. The Proliferation of Weapons of Mass Destruction: China to Iran

In April of this year, the District Attorney's Office announced the indictment of a Chinese businessman named Li Fang Wei and his metallurgical production company, Limmt Economic and Trade Company, Ltd., on charges that they falsified the records of banks in New York and conspired to send illegal payments through New York banks (a copy of the indictment is attached). Defendant Li Fang Wei is the manager of Limmt, a provider of metal alloys and minerals to the global market. The investigation revealed that Limmt has two primary lines of business. First, Limmt sells standard metallurgical products to commercial customers throughout the world. Second, Limmt sells high strength metals and sophisticated military materials, many of which are banned from export to Iran under international agreements, to subsidiary agencies of the Iranian Defense Industries Organization (DIO).

In June 2006, the United States Department of the Treasury, Office of Foreign Assets Control (OFAC) sanctioned Limmt for its support of and role in the proliferation of weapons of mass destruction (WMD) to Iran. As a result of the sanctions, Limmt was banned from engaging in transactions with or through the U.S. financial system, and remains banned to this day. Subsequently, Li Fang Wei and Limmt used aliases and shell companies to continue Limmt's international business.[5] Li Fang Wei and Limmt's purpose in doing so was to use fraud and deception to gain access to the U.S. financial system, to deceive U.S. and international authorities, and to continue the proliferation of banned weapons material to the Iranian military.

The indictment charges that during the period from November 2006 through September 2008, Limmt sent and received dozens of illegal payments through U.S. banks by using aliases and shell companies. Because Limmt was banned from transacting with U.S. banks, any transfers sent in its real name would have been detected by the sophisticated wire transfer monitoring systems at the U.S. banks and blocked. By substituting aliases in the place of its true name, Limmt deceived U.S. banks into processing its transactions. Thus, Limmt's conduct was specifically designed to defeat these filters through the use of false information. The result was the falsification of the records of banks located in Manhattan relating to dozens of illegal transactions.

The investigation revealed that in the almost three-year period since Limmt's designation, Limmt used its aliasas to continue sending banned missile, nuclear and so-called dual use

[5] Aliases used by Limmt and Li included Li Fang Wei a/k/a Karl Lee, a/k/a Patric, a/k/a Sunny Bai, a/k/a K. Lee a/k/a KL, a/k/a David Li, a/k/a F.W. Li) and Limmt Economic and Trade Company, Ltd., a/k/a Limmt (Dalian ftz) Metallurgy and Minerals Co., Ltd., a/k/a Limmt (Dalian FTZ) Minmetals and Metallurgy co., Ltd., a/k/a Limmt (Dalian FTZ) Metallurgy and Minerals Co., Ltd., a/k/a Ansi Metallurgy Industry Co. Ltd., a/k/a Blue Sky Industry Corporation, a/k/a SC (Dalian) Industry & Trade Co., Ltd., a/k/a Sino Metallurgy and Minmetals Industry Co., Ltd., a/k/a Summit Industry Corporation, a/k/a Liaoning Industry & Trade Co., Ltd., a/k/a Wealthy Ocean Enterprises Ltd.

materials to subsidiary organizations of the DIO. The investigation identified subsidiary organizations set up by the DIO to procure and produce high-tech weapons systems, including: Amin Industrial Group, Khorasan Metallurgy Industries, Shahid Sayyade Shirazi Industries, and Yazd Metallurgy Industries.[6]

Some of the materials shipped from Limmt to the DIO front companies included:

- 15,000 kilograms of a specialized aluminum alloy used almost exclusively in long range missile production
- 1700 kilograms of graphite cylinders used for banned electrical discharge machines
- more than 30,000 kilograms of tungsten-copper plates
- 200 pieces of tungsten-copper alloy hollow cylinders
- 19,000 kilograms of tungsten metal powder
- 24,500 kilograms of maraging steel rods
- 450 metric tons of furnace electrodes, and
- 1,400 metric tons of high carbon ferro-manganese.

In addition, Limmt and the DIO engaged in negotiations to have Limmt send the DIO 400 Gyroscopes, 600 Accelerometers, and 100 pieces of Tantalum. Gyroscopes and Accelerometers are crucial technology for Iran's development of long range missiles, and Tantalum in the form indicated can be used to manufacture armor-piercing projectiles of the sort found in improvised explosive devices (IEDs).

Limmt conducted its non-military commercial business primarily with U.S. dollar payments. These payments were processed, or "cleared," by U.S. banks. These payments, although from non-military customers, were nonetheless illegal under U.S. law because of Limmt's status as a proliferator of WMD. Limmt's Iranian military shipments were paid for primarily in Euros. For all of these payments, from both the Iranian military subsidiaries and Limmt's commercial customers, Limmt used its aliases to complete the transactions. The District Attorney's Office has been in contact with European law enforcement personnel to continue the investigation into Iran's use of European banks to clear its Euro transactions. Many of the Euro transactions relate directly to the procurement of weapons materials by the Iranian military front companies in clear violation of international law. It is unclear at this time whether the European banks acted intentionally or whether these transfers violated any laws of the countries where they occurred. We are working with foreign law enforcement and regulatory authorities in the specific countries to find answers to these questions.

In addition, the District Attorney's Office has made preliminary contact with the Chinese government concerning both the role of the Chinese banks as described in the indictment and the illegality of Limmt's conduct under Chinese law. In all of Limmt's transactions, the wire payments were sent to and from a limited number of Chinese banks that handled the accounts of Limmt's front companies. It is unclear whether these banks acted intentionally or knew the true identity of Limmt as the true interest behind the alias/front companies. However, it is clear that

[6] As a result of our joint effort with OFAC, these entities are now on the Treasury Department's list of sanctioned entities.

some of Limmt's shipments to Iran violated Chinese export control laws. We have stated our willingness to share this information with the Chinese authorities. We note that there is no extradition treaty between the United States and China, so that if Mr. Li is to face justice, it will be before a Chinese tribunal for his violations of Chinese law.

Many of the items shipped by Limmt in China to Iran were so-called "dual-use" items, suitable for both civilian commercial as well as military uses. In this case, certain communications made clear that the items were intended for military use by the Iranians, but the circumstantial evidence was equally strong. When the materials are sent to front companies set up by the Iranian military, and Limmt procured false end-user certificates for the shipments, the intent to use these materials for military purposes is readily inferred.

One communication from Li Fang Wei to an agent of the Iranian DIO in 2007 was especially telling. Li Fang Wei discussed with the Iranian agent the difficulties in producing certain aluminum alloys as requested by the Iranians. He went on to relate that there should be little doubt as to the quality of the alloy, as Limmt's factory had supplied the alloy for customers for many years, including for the Chinese military and for the Iranian Aerospace Industries Organization [another part of the Iranian military, responsible for development and procurement of long range ballistic missiles]. Certainly this conversation demonstrates that despite his public protestations to the contrary, Mr. Li and his company were, in fact, intentionally selling weapons materials to the Iranians. In public statements to the media, Mr. Li denies his relationship with the Iranian military and denies supplying them with weapons materials. The factual record developed by our investigation and presented to a grand jury belies these self-serving claims. Mr. Li has supplied the Iranian military with weapons material for years while scoffing at international agreements restricting such trade. For Mr. Li and his co-conspirators, "business as usual" meant violating the law and providing materials for weapons of mass destruction to a dangerous regime.

III. Conclusions

Sanctions, both from the United States and from the international community, are an important tool to deter rogue regimes and encourage the path of diplomacy. Nations such as Iran need to be engaged in dialogue, and need to be invited to become responsible members of the global community, but also need to know there are ramifications for ignoring the path of responsibility. Sanctions provide an important arrow in the quiver of diplomacy. The question we face is how best to make sanctions effective, to deter misconduct, and to encourage adherence by the private sector. Regulatory actions are an important part of enforcement, but some matters, criminal in nature, need to be redressed through the mechanisms of criminal justice. OFAC does a tremendous job identifying threats to the national security and bringing civil enforcement actions. Prosecutors should not become involved in this area lightly. Slight violations or ambiguous behavior do not lend themselves to criminal enforcement. But where there is systematic and pervasive intentional misconduct, criminal prosecutions are necessary. Criminal prosecutions of financial institutions send a strong message of deterrence.

Banks that provide access to the world's financial systems to criminals, proliferators and terrorists should expect that they will be found out and prosecuted. Sanctions are effective only if they are enforced. We may not be able to shut down Mr. Li's factories, but we can shine a spotlight on his conduct and the conduct of the foreign banks that permit these types of operations to flourish.

This fight will be won only if there is strong resolve on the part of the world's major economic and military powers to stand firm against Iran's efforts. We are working with federal law enforcement, regulatory and intelligence agencies to develop more leads and to use the information we have already gathered, and we are also reaching out to law enforcement agents in foreign countries to target this conduct and to shut down the pipeline of weapons to Iran.

These are important matters that need to be addresses in a global framework. Law enforcement efforts should be part of the global equation to make sure that sanctions are enforced and illegal conduct deterred. Through strong and resolute action, this crisis may still be averted, but we do not have the luxury of waiting any longer.