

ABA/ABA Money-Laundering Keynote Address  
Monday, November 14, 2011  
Washington, D.C

REMARKS AS PREPARED FOR DELIVERY

I want to thank the American Bankers Association and the American Bar Association for organizing this conference, and for inviting me here today. It is a great pleasure to speak to you this morning about our shared goals of protecting financial institutions from criminals who use them to launder illegal proceeds. We are committed to working with the financial community to detect and prevent financial crime.

Most importantly, I thank you all for coming here today. Your presence here suggests that you are as interested in finding ways to work together as I am. I think we share certain goals. Free markets. Fair competition. And capitalism that works to fuel economic growth and investment. The message we deliver today is one of partnership with those in this room who believe in good corporate citizenship to not just help keep our markets fair, but also our communities secure. My personal message is that I believe we share those same goals, and the challenges we all have to address is how — together— we will achieve them.

The work of compliance professionals has never been more crucial than it is today, because today in America, distrust of financial institutions has reached levels not seen since the Great Depression. We see resentment toward the financial sector in blogs and on late-night TV shows and in rallies and sit-ins. But that's only half the story. We also see deep distrust of financial institutions within the financial sector itself, as investors wonder whether they can trust ratings agencies, regulatory bodies, or even the conclusions of their own research staffs.

Banks and financial institutions need to have a meaningful understanding of their risk exposure. And when they do not, there is uncertainty in markets, and that uncertainty is what causes credit markets to freeze and investor confidence to plummet. And you know that when banks stop lending the crisis can — and very nearly did — bring down a great economy. At this point in time, particularly, the work you do in your institutions' anti-money laundering departments and compliance offices is as important as any profit center. Your work is crucial to the survival of your institutions, just as your work is crucial to the function of credit markets, to the advancement of commerce and business, and to our economy as a whole.

Certainly, your work is crucial to law enforcement. This morning I would like to offer some examples of how the work that you and your colleagues do every day brings to light major fraud, protects the integrity of our economy, and helps us — as the chief state prosecutor's office for the county that holds the most important street in the world for global finance — build the cases that act as a deterrent to double-dealing in the financial markets.

It starts with the voluminous Suspicious Activity Reports your institutions file each day. Many in your compliance departments must believe SARS are like letters to Santa Claus; you send them in, but you don't know if anyone reads them. Well, let me start by putting that issue to rest.

Many of you know Rich Weber, who ran the Asset Forfeiture and Money Laundering Section at DOJ, and who now heads my Major Economic Crime Bureau. Rich formed a SAR Action Team within my office that sifts through SARs literally on a daily basis, searching for evidence of serious crimes.

Rich estimates that over the last ten months his team has culled for analysis over 1400 SARs. Already, that meticulous work has launched more than 20 new grand jury investigations, helping us solve cases involving not just fraud, but even violent crime. One SAR, for example, alerted us to financial activity that related to an open homicide in the Bronx. Another led us to a “free-riding” scheme, in which the defendant opened multiple trading accounts and, by taking advantage of the delay in clearing transactions, sold stock he did not own, skimming the profits while walking away from the losses. In this manner, the defendant conducted more than \$60 million worth of illegal stock trades, and left six broker-dealers with substantial losses. The defendant in that case used fictitious shell corporations and accounts at disreputable offshore banks, but those accounts were cleared through an unknowing and legitimate US financial institution.

In yet another case, a single SAR, filed by a financial institution like many of yours, led us to a stolen art ring and enabled us to seize \$15 million in proceeds from the sale of stolen art, and millions more in artworks.

As you might imagine, by examining these SARs in real time and following the trails they begin, my office often sees new trends in money laundering and fraud as they develop. This is information you and your institutions may need to know. And so we’ve begun a bank share forum, put together by Rich Weber along with the Chief of our White Collar Investigation Division, Adam Kaufmann. This forum allows us to share with financial institutions, in a small and informal setting, the intelligence we glean from our investigations. Already we’ve had meetings with members of more than ten financial institutions, and so far the feedback has been enthusiastic.

Many issues have been discussed during these meetings, including hot topics like health care fraud, mortgage fraud, cyber crime and identity theft. But I would like to focus on just one topic, because it is of great urgency.

The free world has just received its most urgent warning that Iran is on the verge of developing weapons of mass destruction. The only way short of war to stop this threat is economic sanctions. But economic sanctions are only as effective as you, in the financial sector, and we, in law enforcement, are vigilant. There is a huge financial incentive for arms merchants and nuclear proliferators to bypass international sanctions, and an enormous desire by terrorists to see that they succeed.

Some of you may be aware of the actions my office has taken over the past four years, in partnership with the U.S. Department of Justice and the Treasury Department, to investigate foreign financial institutions engaged in the practice we have come to call “stripping.” Wire transfers are stripped of the codes indicating the source of funds, and so your financial institutions may unwittingly process these transfers, unaware that they are in aid of terrorism, nuclear proliferation, or human rights abuses.

The investigations we have brought to successful conclusion are likely well-known to most in this room: Lloyds TSB, Credit Suisse, and most recently Barclays. And, we hope to have more announcements before the end of this calendar year.

Often what grabs headlines in these investigations are the monetary settlements. To date, these cases have resulted in the forfeiture of over one billion dollars, a critical deterrent to wrongdoing. But even those financial settlements pale in comparison to the crucial principle of respect for international sanctions. It is not hyperbole to say that the most important values in the international community – respect for human rights, peaceful coexistence, and a world free of terror – depend on the effectiveness of those sanctions.

Make no mistake, the foreign banks that were processing these payments for customers in Iran, Sudan, Libya and other rogue nations violated the law, and undermined international security by enabling their US correspondents to process wire payments that otherwise would have been rejected; and they did so systematically, intentionally, and as part of their daily business.

In addition, their actions deprived our intelligence communities of crucial information about the people and entities supporting these rogue regimes. For example, transactions processed on behalf of Iranian banks and businesses can help identify the companies that deal with the Iranian Defense Industries Organizations, and the shell companies that the Iranian military hides behind. Stripping hides the Iranian presence, and frustrates any efforts by the international community to monitor Iranian transactions.

Why is this so important? It is because whenever we disrupt a chain of financing, we reap potential benefits for intelligence operations. Quite simply, if one bank or shell corporation is removed from the pipeline that a terrorist organization or rogue nation uses to move funds, another bank or entity must take its place. And these actions develop further leads, because it is during this period of frantic adaptation that we may be able to identify the parties moving the money or materiel used for terrorism and proliferation.

Something just like that occurred in our recent Iranian shipping line investigation. In 2008, sanctions were imposed against the Islamic Republic of Iran Shipping Lines, for two very good reasons: the shipping lines were a major source of revenue for the regime; and the ships themselves were being used to transport the ingredients of Iran's nuclear weapons program. The response of the shipping lines was simple: they changed the ownership — in name only — of most of their vessels to avoid the sanctions, and created shell companies and corporate alter egos to hide their identities and defraud U.S. banks into doing business with them.

Essentially, U.S. banks were deceived into executing transactions on behalf of Iranian entities seeking to advance Iran's nuclear ambitions. Working with the Office of Foreign Assets Control – OFAC – we were able to pierce the veil of these re-flagged vessels in order to bring charges against those who sought to circumvent the sanctions. In so doing, not only did we help put teeth into the sanctions, we also gained valuable intelligence about aspects of Iran's proliferation efforts, intelligence we were able to share with our partners fighting terrorism.

Some critics have asked why my office – a local prosecutor’s office – gets involved in investigations that reach all the way across the globe. The better question is how we could not. I believe we have no choice, and every obligation to act. Manhattan is a center for global finance, and the Manhattan District Attorney has a long history of policing the world’s markets and financial institutions. Financial transactions that begin and end on foreign shores are very often cleared just a few blocks from my office.

By virtue of who we are, and where we sit, we are essential partners with you in the fight against money laundering, fraud, and international terrorism. By leading the fight against international financial crime, and working cooperatively with our federal brethren, we strive to preserve the integrity of our markets, the strength of our financial sector, and the security of our City and Nation.

Our efforts to keep our city safe must also recognize a threat closer to home and far more immediate: the difficult problem of increasing radical activity at home. Our foreign enemies have done all they can to leverage our own freedoms against us. Through slick online publications, such as Al Qaeda’s INSPIRE, foreign terrorist organizations attempt to recruit our own citizens to take up armed jihad against their neighbors. Our challenge is to balance constant vigilance and preparedness against the preservation of the liberties that define who we are as a civil society. To do this we employ the tried and true techniques that have served us as an office for decades: we follow the rule of law and we act aggressively, but responsibly.

In the fight against a shifting and difficult to identify local terror threat, there is an important role for local prosecutors, working in tandem with our federal counterparts. In one case filed earlier this year, my office obtained an indictment of two New York City residents under New York state terrorism laws, the first time those laws had been used. And we continue to work within the law, and to employ all tools available to us to prevent a local terrorist attack and to keep our citizens safe.

My office handles over 100,000 cases a year – more criminal cases in a year than the U.S. Department of Justice handles annually, nationwide. This volume of cases presents an incredible wealth of intelligence – intelligence that we use to drive our prosecution strategies and to track criminal trends. Let me illustrate this point by turning to the fastest growing classification of crime that we handle: Cyber Crime & Identity Theft.

In some police precincts, it is most frequently reported crime. I know you have seen these cases, because oftentimes funds are withdrawn from your institutions, or credit is obtained, under assumed identities. In some cases, large identity fraud rings have reached into your institutions to corrupt personal bankers and tellers as part of their scheme.

Every month some 300 cases come into our office based on summary arrests for identity theft. Each of these cases is entered into a database, and the data is scrubbed for patterns and connections. Before we created the Cybercrime and Identity Theft Bureau, each of these cases was simply a minor felony offense for possession of a forged credit card or a fake ID. But by tracking and analyzing these cases, we are now able draw connections that reveal broader organized criminal conspiracies. And, as I noted, these criminal networks often extend far beyond our City or even our nation.

We are seeing a shift in the face of cyber crime and identity theft criminals. A few years ago, identity theft was a white collar crime with strong ties to Russia and Eastern Europe. While this remains true, we also have seen a shift in the local face of identity theft. More and more, we see traditional street gangs turning to embrace this new form of criminal income. And just as we once saw organized drug gangs with very specific roles – lookouts, hand-to-hands, enforcers, managers, and bosses – so too are we now seeing the same kind of organization for cyber crime and identity theft rings.

Corporate, bank, and business insiders are recruited to steal personal identification information from customers and clients. They are paid for the information by the recruiters, who in turn give the information to their managers. The managers have technicians who manufacture credit cards and ID, which are given to shoppers. The shoppers buy high-end products which are turned over to the managers, who then sell the products to online fences who peddle them through the internet all over the world. The so-called grey market for internet goods is a multi-billion dollar market, much of it based on goods stolen from identity theft and other criminal schemes.

The managers also traffic in stolen personal identification information in a global online market, buying and selling stolen identities with identity thieves all over the world.

These are difficult cases that require lengthy investigations, and demand a deep knowledge and expertise in cyber crime and computer forensics, coupled with the most sophisticated investigative techniques. To address our fastest growing local crime, we are using all of our resources and taking on criminal networks that exist on a global scale.

How does this relate to you? Because once again, it is financial institutions that have proven one of our best allies in rooting out and eradicating the scourge of identity theft, a crime that knows no borders, and affects so many of us.

In all of these areas, we look forward to partnering with you and the institutions you serve. And I hope that this morning I have given you a sense of how, working together, we can remain one step ahead of those who seek to use your banks as unwitting instrumentalities of their crimes.

But above all, I hope I leave you with my sense, as a prosecutor, of the critical importance of the work that you do every day, and the value I place on our partnership.

On November 30th, the Manhattan DA's Office, in conjunction with the Federal Reserve Bank of NY, will host our second annual Financial Crimes conference. The focus of this year's conference will be on financial crimes and cyber security. We expect to attract more than 350 participants from industry and enforcement – and I hope some of you are able to join us in New York.

It is said that risk managers spend 99% of their time contemplating events with less than 1% likelihood of occurring. But we are living in days in which we have already witnessed the occurrence of too many such extraordinary events. We all know the stakes are enormous. So it remains to us – all of us here today – to remain vigilant, focused, and to act in concert.

Together, I am utterly confident we can not only better ensure the integrity of financial institutions, protect the viability of markets, increase the effectiveness of international sanctions, and safeguard the health of our economy, and the prospects for a brighter future.

###