JUSTICE NEWS

Assistant Attorney General Caldwell Remarks at the ACAMS Anti-Money Laundering & Financial Crime Conference

Hollywood, FL, United States ~ Monday, March 16, 2015

Thank you for the kind introduction.

I am honored to open this important event, which commemorates the 20th year of ACAMS's anti-money laundering conference, and serves as an opportunity for all of us – financial institution representatives, regulators, and law enforcement personnel – to reflect on the relationship between anti-money laundering efforts and the integrity of the worldwide financial system.

The health of the global economy depends on both creating access for a wide range of participants and preventing abuse and corruption. To accomplish these goals, banks and other financial institutions must maintain robust, effective anti-money laundering and other compliance programs that account for international business realities.

And the increasingly global nature of business means that corporate entities, including banks and other financial institutions, must be attuned to complying with the laws of all the countries in which they operate.

As cross-border crime continues to proliferate, prosecutors and other law enforcement must be prepared to find evidence and witnesses all over the world, and to work in coordination with our law enforcement partners abroad. The international law enforcement and regulatory communities must continue to work together to prevent, identify, punish and deter financial crime.

Today, I will speak about what we expect of businesses operating internationally, and how we are investigating and prosecuting crimes involving international conduct, particularly within and among financial institutions.

Since last May, I have had the tremendous pleasure of leading the Criminal Division of the Department of Justice. The Criminal Division includes approximately 600 attorneys who investigate and prosecute federal crimes, help develop criminal law and formulate law enforcement policy.

While the 93 U.S. Attorneys around the country focus on investigating and prosecuting crime in their respective districts, the Criminal Division tends to focus on issues that affect the nation as a whole and on investigations that are international in scope.

As a result, the Criminal Division currently has people stationed in more than 45 countries. Among other work, those folks facilitate collaboration and cooperation with our law enforcement partners in those locations.

In addition, the Criminal Division's Office of International Affairs obtains foreign evidence needed in U.S. investigations, seeks extradition of people wanted for federal and state prosecution in the United States and responds to extradition and mutual legal assistance requests from foreign governments.

Among the sections and offices that make up the Criminal Division is the Asset Forfeiture and Money Laundering Section, known as AFMLS. AFMLS attorneys pursue criminal prosecutions and forfeiture actions against financial

institutions and corporate officers engaged in money laundering, Bank Secrecy Act violations, and sanctions violations.

They also prosecute facilitators or third-party money launderers who move money for transnational criminal organizations.

In addition, AFMLS forfeits the proceeds of high-level foreign corruption through the Kleptocracy Asset Recovery Initiative, which seeks to recover ill-gotten gains from corrupt foreign officials. Once secured, the forfeited assets are used, whenever possible, for the benefit of the citizens of the victim country.

The increasingly global scope of the Criminal Division's work – in particular the international nature of the investigations and prosecutions handled by AFMLS and our Fraud Section – is a direct product of the increasingly global nature of both U.S.-based and foreign-based entities, including financial institutions.

When U.S.-based corporate entities, including financial institutions, conduct business beyond our borders and, conversely, when foreign-based entities operate in the U.S., law enforcement must adapt.

The international nature of our work also is driven by the global reach of the Internet. Increasingly, we seek data such as email from companies' operations all over the world and often have to navigate a thicket of data privacy rules that may vary greatly from country to country.

I am not here to discuss cyber threats, but I would be remiss if I did not note that the internet also has allowed foreign criminals to carry out crimes in the U.S., sometimes on a massive scale, without ever having to set foot in our country. And the victims of those crimes have included many financial institutions.

This is not just a U.S. problem, but a global one. And we are working closely with our foreign counterparts to try to thwart cyberattacks before they happen, as well as to catch and bring to justice cybercriminals.

Identifying and prosecuting overseas cybercriminals, however, is not easy, and companies must protect themselves.

If your companies have not already done so, you need to make state of the art cybersecurity a top priority, and compliance with cybersecurity policy, a major priority. Cybersecurity compliance is critical, because even a single human error, such as one person opening the wrong email and thereby allowing access to a company's computer systems, can have devastating consequences.

Likewise, companies must protect themselves against violations of the law. Your institutions' compliance teams are the first line of defense against money laundering and other financial crime. The importance of your work cannot be overstated.

Robust compliance programs are essential to preventing fraud and corruption. But they also are an important factor for prosecutors in determining whether to bring charges against a business entity that has engaged in some form of criminal misconduct.

Prosecutors look at "the existence and effectiveness of the corporation's pre-existing compliance program". We also look at what remedial measures were taken by the company once it became aware of the misconduct.

As all of you know, there is no "one size fits all" compliance program. Rather, effective anti-money laundering and other compliance programs are those that are tailored to the unique needs, risks and structure of each institution. But, in general, here are some hallmarks of effective compliance programs in our view:

• An institution must ensure that its directors and senior managers provide strong, explicit and visible support for its corporate compliance policies.

• The people who are responsible for compliance should have stature within the company. Compliance teams need adequate funding and access to necessary resources.

• An institution's compliance policies should be clear and in writing. They should be easily understood by employees. That means that the policies must be translated into languages spoken in the countries in which the companies operate. That sounds simple, but it is important and sometimes is not done.

• An institution should ensure that its compliance policies are effectively communicated to all employees. The written policies should be easy for employees to find. And employees should have repeated training, which should include direction regarding what to do or with whom to consult when issues arise.

• An institution periodically should review its policies and practices to keep them up to date with evolving risks and circumstances. Especially if a U.S.-based entity acquires or merges with a foreign entity, all compliance policies should be reviewed and revised.

• There must be mechanisms to enforce compliance policies. Those include incentivizing compliance and disciplining violations. And any discipline must be even handed. The department does not look favorably on situations in which low-level employees who may have engaged in misconduct are terminated, but the more senior people who either directed or deliberately turned a blind eye to the conduct suffer no consequences. Such action sends the wrong message –to other employees, to the market and to the government – about the institution's commitment to compliance.

• An institution should sensitize third parties like vendors, agents or consultants to the company's expectation that its partners are also serious about compliance. This means more than including boilerplate language in a contract. It means taking action – including termination of a business relationship – if a partner demonstrates a lack of respect for laws and policies. And that attitude toward partner compliance must exist regardless of geographic location.

These are just some of the elements of a strong compliance program. When the Criminal Division evaluates a company's compliance policy during an investigation, we look not only at how the policy reads "on paper," but also on the messages conveyed to employees, including through in-person meetings, emails, telephone calls and compensation.

We look at whether, as a whole, a company meaningfully stressed compliance or, when faced with a conflict between compliance and profits, the company chose profits.

In the anti-money laundering and sanctions contexts, in particular, effective compliance requires more. I'd like to highlight a few points.

First, of course, is "know your customer." An institution must ensure that its anti-money laundering, sanctions and other compliance policies and practices are tailored to identify and mitigate the risks posed by its portfolio of customers, and that those customers are providing complete and accurate information.

Second, if a financial institution operates in the U.S. – whether it is a U.S.-based bank or a U.S. branch or component of a foreign bank – it must comply with U.S. laws. This may sound straightforward in principle, but we have seen that it is all too often not implemented in practice.

Part of that compliance is sharing information about potentially suspicious activity with other branches or offices.

For example, if a foreign branch of a U.S. bank identifies suspicious activity related to an account held by a customer that also maintains an account with the bank in the U.S., compliance personnel in the U.S. should be alerted to the suspicious activity.

In our view, to effectuate these practices, financial institutions with a U.S. presence should give U.S. senior management a material role in implementing and maintaining a bank's overall compliance framework.

Third, all regulated companies and, in particular, financial institutions, must be candid with regulators. When we investigate companies, we look closely at the information the companies provided to regulators about the violation. We look at whether the companies were forthcoming, or not.

The vast majority of financial institutions file Suspicious Activity Reports when they suspect that an account is connected to nefarious activity. But, in appropriate cases, we encourage those institutions to consider whether to take more action: specifically, to alert law enforcement authorities about the problem, who may be able to seize the funds, initiate an investigation, or take other proactive steps.

Some banks take more action by closing the suspicious account, but sometimes that may just prompt the criminals to move the illicit funds elsewhere. So, we encourage you to speak with regulators and law enforcement about particularly suspicious activity.

The department appreciates that the global economy, and the international nature of the banking and financial services industries, present a compliance challenge, and often institutions must bridge a cultural, as well as a geographic, divide. But such challenges do not justify non-compliance.

Overall, we expect financial institutions to take compliance risk as seriously as they take other business-related risks. Although compliance may not be a profit center, investment in compliance will pay off – and it's the right thing to do.

The importance of global financial institutions having effective compliance programs – particularly policies that facilitate or mandate information sharing between foreign and domestic branches or components -- is evidenced by the global resolution reached just last week with Commerzbank AG, a global financial institution based on Frankfurt, Germany, and its New York branch Commerz New York.

The bank agreed to forfeit $563 million, pay a $79 million fine and enter into a Deferred Prosecution Agreement with the Department of Justice for violating the International Emergency Economic Powers Act and the Bank Secrecy Act. The bank also entered into settlement agreements with the Treasury Department's Office of Foreign Assets Control and the Board of Governors of the Federal Reserve System.

According to the resolution documents, from 2002 to 2008, Commerzbank knowingly and willfully moved approximately $263 million through the U.S. financial system on behalf of sanctioned entities in Iran and Sudan. To do so, Commerzbank used "cover payments," which concealed the involvement of the sanctioned entities in transactions processed through Commerz New York and other financial institutions in the U.S. Internal bank emails show that Commerzbank knew that its practices violated U.S. law. Commerzbank's senior management was warned about the violative payments and internal auditors "raised concerns," but those concerns were not shared with their U.S. counterparts. Instead, Commerzbank intentionally hid from its New York branch that it was processing payments on behalf of Iranian clients. So the bank ignored warnings from the internal managers charged with ensuring compliance, then concealed the transactions from its own branch office.

In addition, according to court documents, from 2008 until 2013, Commerz New York violated the Bank Secrecy Act by failing to maintain adequate compliance policies and procedures both to detect and report suspicious activity.

Specifically, Olympus, the Japanese camera maker, used Commerzbank and Commerz New York to conceal hundreds of millions of dollars in losses from auditors and investors. To perpetuate the fraud, Commerzbank, through its branch and affiliates in Singapore, loaned money to off-balance-sheet entities created by or for Olympus.

Although numerous bank executives and compliance officers expressed suspicion about the nature and structure of the Olympus transactions, Commerz New York failed to file Suspicious Activity Reports as required or to conduct adequate "know your customer" due diligence.

The potential consequences of having weak, or unenforced, compliance programs also are illustrated by the department's recent, landmark criminal resolution with BNP Paribas (BNPP) – the fourth largest bank in the world.

Between 2004 and 2012, BNPP knowingly violated the IEEPA and the Trading with the Enemy Act by moving more than $8.8 billion through the U.S. financial system on behalf of Sudanese, Iranian, and Cuban entities subject to U.S. economic sanctions. The majority of the transactions facilitated by BNPP were on behalf of entities in Sudan, which is subject to a U.S. embargo due to the Sudanese government's role in facilitating terrorism and committing human rights abuses.

BNPP's criminal conduct took place despite repeated warnings expressed by the bank's own compliance officers and its outside counsel. In response to the concerns identified by compliance personnel, high-ranking BNPP officials explained that the questioned transactions had the "full support" of BNPP management in Paris. In short, VBPP expressly elected to favor profits over compliance.

Ultimately, BNPP pleaded guilty to conspiracy to violate IEEPA and TWEA, and agreed to pay record-setting financial penalties of over $8.9 billion. And the company admitted its misconduct – including its disregard of compliance advice – in a detailed statement of facts that was made public.

Those are just two examples of recent cases we have handled involving financial institutions and their international businesses. The Criminal Division has recently resolved financial fraud and sanctions violations investigations with several other major financial institutions, including Standard Chartered, HSBC, UBS, RBS and Barclays, just to name a few. In those cases, we have often entered into deferred prosecution agreements or non-prosecution agreements – known as DPAs and NPAs – with the banks.

DPAs and NPAs are useful enforcement tools in criminal cases. Through those agreements, we can often accomplish as much as, and sometimes even more than, we could from a criminal conviction. We can require improved compliance programs, remedial steps or the imposition of a monitor. We can require that the banks cooperate with our ongoing investigations, particularly in our investigations of individuals. We can require that such compliance programs and cooperation be implemented worldwide, rather than just in the United States. We can require periodic reporting to a court that oversees the agreement for its term. These agreements can enable banks to get back on the right track, under the watchful eye of the Criminal Division and sometimes a court.

And these agreements have teeth – not just because they are overseen by the Department of Justice and sometimes a court, but because of the potential penalties triggered by a breach.

Let me be clear: in the Criminal Division, we will hold banks and other entities that enter into DPAs and NPAs to the obligations imposed on them by those agreements. And where banks fail to live up to their commitments, we will hold them accountable.

Just like an individual on probation faces a range of potential consequences for a violation, so too does a bank that is subject to a DPA or NPA.

Under DPAs and NPAs, we have a range of tools at our disposal. We can extend the term of the agreement and the term of any monitor, while we investigate allegations of a breach, including allegations of new criminal conduct. Where a breach has occurred, we can impose an additional monetary penalty, or additional compliance or remedial measures. Most significantly, we can pursue charges based on the conduct covered by the agreement itself – the very conduct that the bank had tried to resolve through the DPA or NPA.

Make no mistake: the Criminal Division will not hesitate to tear up a DPA or NPA and file criminal charges, where such action is appropriate and proportional to the breach.

DPAs and NPAs are powerful tools. They can't be ignored once they're signed, and they can't be followed partially but not completely. We will take action to ensure that banks are held accountable for DPA or NPA violations. And where a bank that violates a DPA or NPA is a repeat offender with a history of misconduct, or where a violating bank fails to cooperate with an investigation or drags its feet, that bank will face criminal consequences for its breach of the agreement.

Many of the cases we have handled with financial institutions involve coordination with regulators and other law enforcement around the world. To successfully investigate and prosecute cases involving global entities, including financial institutions, we work closely with our foreign law enforcement counterparts and foreign regulators. Cooperation and coordination with foreign authorities strengthens our collective ability to bring transnational criminals to justice – whether they are multi-national corporations, corporate executives, corrupt political officials, drug or human traffickers, terrorists or hackers behind computer screens.

In May 2013, the department announced charges against Liberty Reserve, a digital currency system that was incorporated in Costa Rica and created for the express purpose of assisting cybercriminals and others in anonymously laundering illicit proceeds through the U.S. and global financial systems.

At the time, Liberty Reserve had more than one million users worldwide who conducted transactions involving more than six billion in funds, which encompassed suspected proceeds of credit card fraud, identity theft, investment fraud, computer hacking, child pornography, narcotics trafficking and other crimes.

But, due to the coordinated efforts of law enforcement authorities in the U.S., Costa Rica, the Netherlands, Spain, Sweden and Switzerland, justice prevailed. Liberty Reserve permanently is out of business, and the government also charged seven individuals connected to Liberty Reserve, including its founder Arthur Budovsky, information technology manager Maxim Chukharev and chief technology officer Mark Marmilev.

To date, four defendants have pleaded guilty. In December 2014 and January 2015, Marmilev and Chukarev were sentenced to serve five years in prison and three years, respectively. Budovsky was extradited from Spain to the United States and will stand trial in November.

Our kleptocracy cases are other examples of our cooperation with international authorities to remediate fraud, abuse and corruption. Through the department's Kleptocracy Asset Recovery Initiative, we work with law enforcement agencies to forfeit the proceeds of foreign official corruption and to use those recovered assets to benefit the people harmed by the acts of corruption and abuse of office.

One of our kleptocracy cases involves Chun Doo-Hwan, the former president of South Korea, who was convicted in 1997 of receiving more than $200 million in bribes from South Korean businesses and other companies. President Chun and his relatives laundered some of the corruption proceeds through a web of nominees and shell companies in the U.S. In coordination with South Korean law enforcement authorities, since 2013, the department has assisted in the recovery of over $27.5 million in corruption proceeds from Chun's associates. Earlier this month, the department secured the forfeiture of another $1.2 million in assets in the U.S. traceable to corruption proceeds

accumulated by Chun.

Also in connection with the Kleptocracy Asset Recovery Initiative, in October 2014, the department settled a civil forfeiture action against assets in the U.S. of the Second Vice President of the Republic of Equatorial Guinea Teodoro Obiang Mangue. Obiang looted his own government and solicited and received bribes and kickbacks from businesses to support a lavish lifestyle while his fellow citizens lived in extreme poverty. In all, Obiang amassed more than $300 million in assets through corruption and money laundering. Among the assets he purchased with corruption proceeds were a $30 million mansion in Malibu, California; a Ferrari and various items of Michael Jackson memorabilia. Under the terms of the settlement, Obiang was required to disgorge over $30 million, $10 million of which was to be forfeited, and another $20 million to be used to benefit the people of Equatorial Guinea through a charity.

There have been suggestions – perhaps by some in this room today – that the Department of Justice, in collaboration both with U.S. regulators and foreign law enforcement authorities, are unreasonably targeting financial institutions for investigation and prosecution. That is not the case.

Simply put, banks and other financial institutions continue to come up on our radar screens because they, and the individuals through which they act, continue to violate the law, maintain ineffective compliance programs or simply turn a blind eye to criminal conduct to preserve profit. If the government learns of such action (or inaction), it is our obligation to investigate and follow the evidence wherever it may lead. And we will prosecute banks and other financial institutions for willful failures to maintain effective anti-money laundering programs and for other financial crimes.

I strongly encourage the representatives of banks and other financial institutions participating in this conference to take the opportunity – both during the next few days and once you return to your respective offices – to reflect on whether your institutions have effective anti-money laundering programs and other compliance policies and practices to prevent or mitigate financial crime. The integrity and viability of the global financial system require that you do.

Thank you.

Component:
Criminal Division

Updated March 16, 2015