

**Luke A. Bronin**  
**Deputy Assistant Secretary for Terrorist Financing and Financial Crimes**  
**U.S. Department of the Treasury**

**Hearing entitled: “Combating Transnational Organized Crime: International Money Laundering as a Threat to our Financial Systems”**

**U.S. House of Representatives**  
**Subcommittee on Crime, Terrorism and Homeland Security**  
**Committee on the Judiciary**

**February 8, 2012**

Chairman Sensenbrenner, Ranking Member Scott, distinguished members of this Subcommittee, thank you for the opportunity to appear before you today to discuss Transnational Organized Crime (TOC) and the threat that international money laundering poses to the integrity of our financial system.

In my testimony today, I would like to discuss, first, the nature and scope of the threat, second, the key vulnerabilities in the U.S. financial system that are being exploited, and finally, what we are doing about it.

**The Nature and Scope of the Threat**

In 2009, the United States completed a comprehensive interagency assessment of transnational organized crime. The assessment concluded that since 1995, TOC networks have expanded in scope and sophistication and are today taking advantage of the increasingly integrated international financial system to facilitate criminal activity and launder the proceeds of their crimes.

Transnational criminals engage in a wide range of illicit activity, including trafficking in drugs, persons, and weapons, as well as identity theft, financial fraud, cyber crime, and intellectual property theft. Transnational crime is a threat to national security, with clear links to other national security threats. We see terrorists and insurgents turn increasingly to crime and criminal networks for funding and logistics. We see proliferators and arms traffickers use the same methods as TCOs to pursue their illicit ends.

To combat the growing threat of TOC, President Obama announced in July 2011 a national Strategy to Combat Transnational Organized Crime (the “TOC Strategy”). The TOC Strategy observes that, “[n]ot only are criminal networks expanding, but they also are diversifying their activities, resulting in the convergence of threats that were once distinct and today have explosive and destabilizing effects.”

Most important for today’s hearing, the 2009 assessment and TOC Strategy also highlight the extent to which these groups have infiltrated legitimate commerce and economic activity. This infiltration of legitimate economic activity threatens the integrity of the international financial

system through subversion, exploitation, and distortion of legitimate markets. The scale of the threat is significant, as hundreds of billions of dollars of illicit proceeds are generated each year through transnational organized crime in the United States.

### **Vulnerabilities in the Financial System**

Access to the international financial system gives criminal organizations the ability to hide, move and make use of ill-gotten funds on a massive scale. The challenges in identifying and recovering proceeds of crime laundered through the U.S. and global financial system may be attributed in large part to ongoing and substantial criminal abuse of legal entities and a lack of insight into the beneficial ownership of those legal entities. In particular, TCOs make aggressive use of *shell companies* and *front companies* to facilitate illicit financial activity.

Shell companies are business entities without active operations or significant assets. Although shell companies can have legitimate commercial uses, the ease of formation and the absence of ownership disclosure requirements make them an attractive vehicle for those seeking to launder money or conduct illicit activity. TCOs also make aggressive use of front companies, which often conduct legitimate business activity, to disguise the deposit, withdrawal, or transfer, of illicit proceeds that are intermingled with legitimate funds.

In 2007, the Departments of Justice, Homeland Security and the Treasury jointly issued the National Money Laundering Strategy (2007 Strategy), which in part, identifies current and emerging trends in money laundering, as well as specific vulnerabilities. The 2007 Strategy specifically emphasizes the risks associated with shell companies and trusts, noting that the use of these entities for illicit purposes has become increasingly popular with criminal actors because of the “ability to hide ownership and mask financial details.” As asserted by a representative of the Asset Forfeiture and Money Laundering Section of the United States Department of Justice (AFMLS), law enforcement faces “considerable difficulties when investigating U.S. shell corporations due to the lack of beneficial ownership information available in the United States.”

The abuse of legal entities is an international problem; both foreign and domestic legal entities can be used for illicit purposes. Viktor Bout, an international arms merchant who was designated by the Treasury Department’s Office of Foreign Asset Control (OFAC), used U.S. shell companies to mask his ownership and facilitate his illegal arms trafficking activities. Law enforcement believes that the Sinaloa Cartel, one of the major Mexican drug trafficking organizations, uses both U.S. and Colombian shell companies to launder drug proceeds. Additionally, illicit actors use foreign shell companies to mask the involvement of designated persons and circumvent U.S. sanctions programs relating to Iran and North Korea.

In addition to abusing shell companies and front companies, TCOs exploit the following vulnerabilities to advance their criminal activity:

*Money services businesses (MSBs)*, including money transmitters, check cashers and currency exchangers, are vital service providers for millions of Americans. They are, however, vulnerable to exploitation. While the role of registered money services businesses in the U.S. economy is small relative to banks, as is their relative threat, U.S.-based MSBs are exploited by criminals for

many of the same reasons the transmitters are popular with their main customer base of legitimate consumers – competitive pricing, transmission speed, broad network reach, and in select cases, agent complicity and deficient anti-money laundering (AML) controls.

*Gatekeepers*, such as attorneys, accountants, and company formation agents, provide access to a variety of financial services and the means by which TCOs can use their ill-gotten gains. Gatekeepers can be used to create shell corporations, open bank accounts, acquire real estate, and make investments to conceal illicit assets and activity. While the vast majority of gatekeepers are legitimate and play a critical role in safeguarding the financial system from abuse, complicit or careless gatekeepers are vital to sustain criminal enterprises.

*Under-regulated jurisdictions* with weak AML oversight procedures and controls, or strict privacy laws, allow TCOs an easy entry point to the global financial system. TCOs also use free trade zones with lax safeguards to facilitate trade-based money laundering schemes. Of particular concern are jurisdictions that do not adequately supervise exchange houses that have direct or indirect access to the U.S. financial system.

### **Exploitation of the Banking Sector**

TCOs seeking to move and launder funds regularly exploit the vehicles and vulnerabilities discussed thus far. It is important to recognize, however, that shell companies, front companies, complicit or careless gatekeepers and lax jurisdictions are not alternatives to the regulated U.S. financial system, but rather points of access into the regulated financial system. Indeed, the most important battleground in the fight against money laundering remains the banking sector itself.

The U.S. has one of the strongest and most effective anti-money laundering regimes in the world, anchored by the customer due diligence and transaction recordkeeping and reporting required of financial institutions under the Bank Secrecy Act. Suspicious activity reporting and currency transaction reporting play a vital role, shining a light on illicit activity and supporting financial investigations by law enforcement.

To cite just one recent example, suspicious activity reports filed by banks helped law enforcement pursue a multi-million dollar drug trafficking investigation against a classic front company: a Texas retailer that had accepted tens of millions of dollars in cash from the sale of drugs over a two-year period, comingled those funds with legitimate earnings, and deposited them into a number of commercial bank accounts.

Despite the strength of the U.S. anti-money laundering regime, however, its effectiveness depends on vigorous implementation. And when banks let down their guard, the financial system can be compromised. A recent money laundering case that involved just one predicate crime – drug trafficking – in just one jurisdiction – Mexico – highlights the risk.

In 2010, the Department of Justice (DOJ), the Office of the Comptroller of the Currency (OCC) and the Financial Crimes Enforcement Network (FinCEN) took coordinated enforcement action against a major U.S. financial institution. As outlined in the 2010 Deferred Prosecution Agreement (DPA) between DOJ and the financial institution, the financial institution failed to

effectively monitor more than \$420 billion in cross-border financial transactions with thirteen high-risk Mexican currency exchange houses, commonly known as *casas de cambio* (*casas*), from 2004-2007, including millions of dollars that were subsequently used to purchase airplanes for narcotics traffickers.

This example should not necessarily be taken to suggest that all of those transactions were in fact illegitimate. But this case does illustrate a key vulnerability: when banks let AML/CFT controls slip, criminals operating in cash can potentially place large amounts of that cash through foreign financial institutions and integrate illicit funds into the regulated financial system through correspondent relationships with U.S. banks.

Other coordinated enforcement actions against U.S. banks similarly demonstrate that failure to implement effective AML programs can permit the introduction of illicit funds into the financial system. Most recently, in August 2011, DOJ, FinCEN, the FDIC and the Florida Office of Financial Regulation took coordinated enforcement against another U.S. bank for failing to establish an AML program. From 2001 to 2009, the U.S. bank processed more than \$40 million in suspicious activities in just five accounts, including accounts of three *casas* controlled by DTOs, at least \$10.9 million of which is known to be narcotics proceeds and all of which should have been identified as high-risk.

### **Strengthening the System's Defenses**

Let me stress again that the U.S. anti-money laundering regime is unparalleled. And the vast majority of banks implement their AML safeguards diligently and effectively. What the few examples noted just now tell us, however, is that even as the money laundering threat evolves, and even as TCOs become increasingly sophisticated, we should continue to remain focused on the "basics" of the anti-money laundering fight: promoting financial transparency and ensuring the effective implementation and enforcement of Bank Secrecy Act obligations.

Accordingly, Treasury has identified the following priorities in the fight to promote transparency in the financial system and to make it harder for TCOs to conceal their illicit activity:

*Clarifying Customer Due Diligence (CDD) Obligations.* The most basic AML precept of all for financial institutions is "know your customer." However, as highlighted above, criminal actors can easily disguise their activities by operating in the name of shell companies and front companies. When U.S. financial institutions open an account for a business, they are only explicitly required to identify the beneficial owner(s) of the legal entity in specific and narrow instances. We believe that the absence of a general obligation to collect beneficial ownership information, along with the lack of a clear CDD framework, has created some confusion and inconsistency across financial sectors.

To address this challenge, Treasury intends to clarify, consolidate and strengthen CDD requirements for financial institutions, including an obligation to collect beneficial ownership information. Such a requirement will harmonize the minimum expectations with respect to CDD policies, procedures, and processes, and make explicit the fundamental elements necessary for an

effective CDD program. As we work to clarify CDD requirements, we will continue to engage closely with regulators, with the private sector, and with our international counterparts.

*Passing Beneficial Ownership Legislation.* As highlighted earlier, one of the greatest challenges that both financial institutions and law enforcement face when trying to identify and disrupt illicit criminal activity is the lack of transparency in the beneficial ownership of legal entities.

That is why the President's TOC Strategy includes a commitment to work with Congress to adopt legislation that would require disclosure of beneficial ownership information in the company formation process. Treasury is working closely with our interagency partners, private sector stakeholders, and members of Congress to advocate for passage of such legislation. Passage of beneficial ownership legislation would make it easier for financial institutions to conduct appropriate customer due diligence, easier for law enforcement to follow leads generated by suspicious activity reports, and more difficult for criminals to hide behind front companies and shell companies.

*Protecting the International Gateways to the U.S. Financial System.* Foreign correspondent accounts – established by a U.S. financial institution to receive deposits from, or to make payments or other disbursements on behalf of, a foreign financial institution – are the most important international gateway to the U.S. financial system. That gateway must be protected.

Recent civil and criminal enforcement actions detail the misuse of, correspondent accounts at U.S. banks by TCOs to launder criminal proceeds. To protect this gateway, Treasury's Financial Crimes Enforcement Network (FinCEN) issued final rules implementing Section 312 of the USA PATRIOT Act, which requires certain U.S. financial institutions to apply due diligence to correspondent accounts maintained for certain foreign financial institutions. My office is focusing intensely on the risks posed by such foreign correspondent accounts, and considering whether additional guidance or information could be helpful to the private sector.

FinCEN also recently published a new rule to protect another important international gateway – foreign money services businesses with access to the U.S. financial system. Recognizing the risk that foreign MSBs with deficient AML/CFT policies and procedures pose, last summer FinCEN published a rule requiring certain foreign MSBs to comply with the same legal requirements as U.S.-based MSBs, including registration with FinCEN and recordkeeping, reporting, and AML program requirements.

This new rule will make it easier for civil and criminal authorities to take enforcement actions against foreign MSBs that use their access to the U.S. financial system to facilitate illicit activity – and may also prove useful in addressing the risk presented by virtual currency providers, which sometimes offer an opaque and anonymous means of moving money.

*Setting Standards for Gatekeepers.* As noted earlier, gatekeepers play a vital role in protecting against international money laundering. Treasury is partnering with the American Bar Association, among other organizations, to develop a comprehensive self-regulatory framework for attorneys. In addition, Treasury supports efforts to make company formation agents subject to appropriate oversight, including registering with FinCEN, as proposed in recent legislation introduced by Senator Levin and Congresswoman Maloney, respectively.

*Promoting Transparency Internationally.* TCOs operate globally and money laundering often occurs across multiple jurisdictions. Countering TCOs' illicit financial networks effectively therefore requires international coordination and, to the greatest degree possible, harmonization of AML/CFT standards. The key to that coordination is the Financial Action Task Force (FATF), the premier policy-making and standard-setting body in the international effort against terrorist financing, money laundering, and other illicit finance.

With respect to under-regulated jurisdictions, the U.S. government is working with the FATF and partner governments to engage jurisdictions of concern. This process involves identifying jurisdictions with significant deficiencies in their AML/CFT regime and coordinating an action plan to address them.

On a systemic level, it is particularly important that we do not neglect this international effort as we move forward in addressing the issue of beneficial ownership in the United States. A unilateral solution is an incomplete and ineffective solution. Without a coordinated global approach, a customer excluded from dealing directly with a U.S. financial institution due to beneficial ownership risk might nevertheless seek to access the financial system through foreign correspondent channels.

We are therefore working globally with our partners in the FATF to clarify and enhance the global implementation of international standards regarding beneficial ownership, and we expect new guidance with respect to the transparency of legal entities and customer due diligence obligations be adopted this month as part of the revision of the FATF standards.

### **Taking Targeted Action**

Even as we work to promote transparency and to strengthen the AML architecture both domestically and around the world, Treasury will continue to employ aggressively its targeted authorities to disrupt the financial networks of TCOs.

*Foreign Narcotics Kingpin Designation Act.* One authority specifically designed to target drug trafficking organizations is the Foreign Narcotics Kingpin Designation Act (the "Kingpin Act"). Since June 2000, over 1000 individuals and entities have been designated under the Kingpin Act, resulting in the blocking of millions of dollars worth of property in the United States.

Treasury has designated a significant number of exchange houses as part of a broader effort to target the financial networks of Mexican cartels. Outside of Latin America, and perfectly illustrating the nexus between TOC and other critical national security threats, Treasury last week used its Kingpin authority to designate three members of the Foreign Terrorist Organization, Partiya Karkerên Kurdistan (PKK). And last February, Treasury used its Kingpin authority to designate the Kabul-based New Ansari Money Exchange, a major money-laundering vehicle for Afghan narcotics trafficking organizations.

*Executive Order 13581.* To supplement and expand our authority to target transnational criminal organizations, last summer President Obama signed Executive Order 13581, "Blocking Property

of Transnational Criminal Organizations,” imposing sanctions against significant TCOs that threaten the U.S. national security, foreign policy, or economy and granting the Treasury Department the authority to designate additional individuals or entities. In the annex of E.O. 13581, the President identified and imposed sanctions on four significant TCOs: the Brothers’ Circle (a.k.a. Moscow Center), the Camorra, the Yakuza, and Los Zetas.

Treasury is working to designate entities and individuals related to the TCOs identified in the Executive Order. We are also working with our interagency and international partners to identify additional TCOs that pose a threat to the national security, foreign policy, and economy of the U.S. for potential designation.

*Patriot Act Section 311.* Finally, the Administration’s TOC Strategy calls for the use of Section 311 of the USA PATRIOT Act to combat TOC. This powerful tool allows the Treasury Department to take action to protect the U.S. financial system from specific threats. It authorizes the Treasury Department to identify a foreign jurisdiction, foreign financial institution, type of account or class of transactions as a primary money laundering concern, and impose any one or a number of special measures in response. In practical terms, Section 311 enables the Treasury Department to cut off foreign financial institutions from the U.S. financial system on the grounds that they facilitate transnational organized crime or other illicit activity.

In February 2011, the Treasury Department identified the Beirut-based Lebanese Canadian Bank (LCB) as a financial institution of primary money laundering concern for its role in facilitating the activities of an international narcotics trafficking and money laundering network operating across five continents. The LCB action was the product of close coordination and cooperation with the Drug Enforcement Administration, and exposed a vast trade-based money laundering scheme that co-mingled profits of used car sales and consumer goods with narcotics proceeds and funneled them through West Africa and into Lebanon.

Treasury remains vigilant and is working to identify additional financial institutions or jurisdictions that may merit action using this powerful authority. We will not hesitate to employ Section 311, as well as the full range of available tools, to protect the U.S. financial system from abuse and to expose and to disrupt TCOs’ illicit financial networks.

## **Conclusion**

The United States has one of the strongest and most effective anti-money laundering systems in the world. However, the size of the U.S. economy and the global importance of the U.S. dollar make the U.S. financial system a prime target for TCOs, and recent enforcement actions against U.S. financial institutions are a reminder that challenges remain. These enforcement actions send a clear message that we will not tolerate the misuse of the U.S. financial system to launder illicit proceeds.

At the same time, Treasury has a role to play in clarifying requirements and expectations. Accordingly, we are working with the regulatory community to provide for additional rulemaking to clarify and strengthen CDD requirements. Recognizing that a lack of transparency concerning the beneficial ownership of corporate entities has hampered U.S. financial

institutions' ability to protect themselves and the financial sector as a whole from illicit actors, we strongly support legislation that would require the disclosure of meaningful beneficial ownership information at the time of company formation.

And as we seek to strengthen our financial system's defenses, we will continue to employ – wherever and whenever we can – our targeted authorities to disrupt and damage the facilitation networks on which TCOs depend. To complement our own targeted authorities, we strongly support the work of our colleagues at DOJ and the important role they play in combating money laundering. The U.S. government requires the tools necessary to address the threat of TOC and to maintain the United States' leadership position in the fight against money laundering. As such, the Department of the Treasury strongly supports the proposed Proceeds of Crime Act which, among other things, would make all domestic felonies, and foreign crimes that would be felonies in the United States, predicates for money laundering.

To break the economic power of TCOs and protect the U.S. financial system from TOC penetration and abuse, we must continue to attack the financial underpinnings of the transnational criminals; strip them of their illicit wealth; sever their access to the financial system; expose their criminal activities hidden behind legitimate fronts; and protect strategic markets and the U.S. financial system.

Thank you.