Department of Justice

STATEMENT FOR THE RECORD OF

JENNIFER SHASKY CALVERY
CHIEF
ASSEST FORFEITURE AND MONEY LAUNDERING SECTION
CRIMINAL DIVISION

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY
COMMITTEE ON THE JUDICIARY
UNITED STATES HOUSE OF REPRESENTATIVES

ENTITLED

"COMBATING TRANSNATIONAL ORGANIZED CRIME: INTERNATIONAL MONEY LAUNDERING AS A THREAT TO OUR FINANCIAL SYSTEMS"

FEBRUARY 8, 2012

Statement for the Record
Jennifer Shasky Calvery
Chief
Asset Forfeiture and Money Laundering Section
Criminal Division
U.S. Department of Justice

Subcommittee on Crime, Terrorism, and Homeland Security
Committee on the Judiciary
United States House of Representatives

"Combating Transnational Organized Crime: International Money Laundering as a Threat to Our Financial Systems"
February 8, 2012

INTRODUCTION

Mr. Chairman, Ranking Member Scott, and distinguished Members of the Subcommittee, thank you for inviting me to speak with you this morning about transnational organized crime, and specifically the threat international money laundering poses to our financial system. In my testimony, I will describe the nature of this threat, the variety of methods transnational organized crime groups use to generate and launder money, the efforts of the Department of Justice to address the threat, and steps Congress can take that will assist in these efforts.

In his recent testimony on worldwide threats, Director for National Intelligence Clapper characterized transnational organized crime as "an abiding threat to U.S. and national security interests." Therefore, the fight against transnational organized crime is one of the highest enforcement priorities of the Department of Justice and the Administration. As chief of the Department of Justice's Asset Forfeiture and Money Laundering Section (AFMLS), I know firsthand the seriousness of the danger posed by transnational organized crime generally, and to our financial system in particular.

Transnational organized crime represents a uniquely modern threat to our financial and national security. While global markets and technology combine to make the world seem smaller, transnational criminal organizations have exploited these advancements to expand their operations and influence and to evade justice. As a result, these organizations are growing increasingly more sophisticated in both their ability to commit revenue-generating crime and to subsequently launder the proceeds of that crime. I commend you for holding this hearing and shining a spotlight on an often overlooked and underappreciated threat that demands the full attention of the U.S. government.

Transnational Organized Crime Threatens U.S. and International Security

In December 2009, the United States government completed a comprehensive review of transnational organized crime (TOC) – the first such assessment since 1995. The Administration concluded that TOC networks continue to expand dramatically in size, scope, and influence,

posing significant new and increasing threats to U.S. national security. Striking new and powerful alliances and engaging in a range of illicit activities as never before, transnational organized criminals threaten our interests in a variety of new and sinister ways. In years past, TOC was largely regional in scope and hierarchically structured. Today's TOC groups have adapted to the realities and opportunities of globalization, and have evolved from traditional hierarchical structures toward looser networks that are more complex, volatile, and destabilizing.

TOC groups have also become increasingly sophisticated in penetrating financial systems, manipulating securities and commodities markets, harnessing cyberspace to perpetrate high-tech crimes, and carrying out numerous other schemes that exploit our institutions, and threaten the national security of the United States. TOC in its highest form is far removed from the streets. The use of fast-paced trading, the Internet and electronic payments – money, communications and inducements can be exchanged in milliseconds – allows leaders of TOC groups to operate from foreign safe havens to exploit international borders and regulatory gaps. Transnational organized criminals perpetrate a broad array of crimes significantly impacting the average U.S. citizen, ranging from cyber crime, drug trafficking and associated violence, identity theft, intellectual property theft, and sophisticated frauds which include schemes targeting government programs like Medicare. In October 2010, the Department of Justice announced charges against 73 members and associates of an Armenian-American organized crime group, with ties abroad, in five states for a scheme responsible for more than $163 million in fraudulent billing to Medicare. Among those convicted of racketeering was Armen Kazarian, who is alleged to be a "Vor," a term translated as "Thief-in-Law" and refers to a member of a select group of high-level criminals from former Soviet Union countries, including Armenia. This was the first time a Vor had been convicted of racketeering in the United States.

In some jurisdictions, transnational criminal organizations also undermine political institutions and stability, by insinuating themselves into the political process through bribery, even becoming alternate providers of governance, security, and livelihoods to win popular support. TOC penetration of foreign governments is deepening, leading to co-option in some jurisdictions and weakening of governance in many others. The nexus in some jurisdictions among TOC groups and elements of government – including intelligence services personnel – and big business figures threatens the rule of law and transparent business practices, and undermines our ability to compete in key world markets.

Crime, in general, and TOC, in particular, have always been an important source of funding for some terrorist organizations and their deadly acts. In FY 2010, the Department of Justice identified 29 of the 63 top drug trafficking organizations as having links to terrorist organizations. In July 2011, the Department announced charges resulting from a DEA narco-terrorism undercover operation, charging three defendants with conspiring to provide various forms of support to Hizballah, the PKK, and Pejak. Two defendants were arrested in Bucharest, Romania, where they were detained pending extradition to the United States; the third was arrested in the Republic of the Maldives. This investigation was supported by Romanian authorities who identified Kurdish PKK members that were selling heroin to support their terrorist organization. It also identified Pejak elements in Iran that were utilizing the drug trade to finance operations and Hizballah elements that were attempting to purchase military-grade weaponry. This investigation is continuing.

TOC Strategy and the Threat to the U.S. and Global Economy

In response to the growing threat posed by TOC, in July, 2011, the Administration released its Strategy to Combat Transnational Organized Crime ("TOC Strategy"), which sets forth a whole-of-government response to these pervasive threats. Among the threats identified in the TOC Strategy, the most relevant for this hearing is the threat to the U.S. and world economy. Through the profits of its illicit activities, TOC is increasing its subversion of legitimate financial and commercial markets, threatening U.S. economic interests, and raising the risk of significant damage to the world financial system.

As evidence of TOC's global economic might, one need only consider the most recent estimates of the amount of money laundered in the global financial system - $1.6 trillion, of which an estimated $580 billion is related to drug trafficking and other TOC activities, according to the United Nations Office on Drugs and Crime's Research Report published in 2011. These staggering amounts of money in the hands of some of the worst criminal elements create a terrifyingly vicious cycle – money enables TOC to corrupt the economic and political systems in which they operate, thereby allowing them to consolidate and expand their power and influence, which gives rise to more opportunity to commit crime and generate revenue.

To cite just one example of an elaborate TOC financial scheme, in August 2009, Italian police and prosecutors thwarted a multi-billion dollar securities scheme orchestrated by the Sicilian Mafia which targeted financial firms in the United States and elsewhere. The local authorities arrested as many as twenty people across the globe, including in Italy, Spain, Venezuela and Brazil. Among those arrested was Leonardo Badalamenti, son of a famous organized crime boss who died in a U.S. prison in 2004. According to investigators, Badalamenti and his crew planned to use phony securities to obtain credit lines totaling as much as $2.2 billion from several reputable financial firms, including HSBC in London, and the Bank of America in Baltimore. As part of the scheme, false Venezuelan bonds were allegedly authenticated by corrupt officials within the Central Bank of Venezuela.

But while the ability to generate vast sums of money motivates, sustains, and empowers TOC, it can also be their Achilles heel. Transnational organized crime is a business, and like any business, profit is the primary motivation. Profit drives their diversification into whatever area of criminal activity and with whatever criminal alliance generates proceeds. Those proceeds then fuel the organizations as operating capital and allow them to continue to grow their criminal activity, their personal wealth, their influence, and their ability to corrupt on a national scale. Because money is the foundation on which these criminal organizations operate, our money laundering laws are our primary means to stop them. It is their core vulnerability. By taking their operating capital through money laundering prosecutions and forfeiture, we take away their ability to operate.

Specific TOC Money Laundering Techniques

Generally speaking, money laundering involves masking the illegal source of criminally derived proceeds so they appear legitimate, or masking the source of monies used to promote illegal conduct. This process is of critical importance, as it enables criminals to enjoy these profits without compromising themselves or jeopardizing their ongoing criminal activities. To

accomplish this, money laundering generally involves three stages. It begins with the placement of illicit proceeds into the financial system. For cash proceeds, placement usually happens either via direct placement through structured deposits or indirectly by smuggling illicit proceeds out of the U.S. and back in order to allow the money to be deposited in U.S. banks. The next stage is layering, which is the process of separating the proceeds of criminal activity from their origin. The final stage is integration, which is the process of using an apparently legitimate transaction to disguise the illicit proceeds. Once illegal proceeds have entered the banking system the integration and layering stages make it very difficult to track and trace the money as it moves globally, often through a web of shell companies.

Money launderers have what seems like an infinite number of ways to disguise and move money, and there appears to be no limit to their ingenuity. Disguised in the trillions of dollars that is transferred between banks each day, banks in the U.S. are used to funnel massive amounts of illicit funds. But rather than address the full landscape of money laundering techniques employed by today's criminals and the critical role that our banking system plays in that landscape, I will instead focus on those methods most frequently utilized by TOC networks to move money around the globe, including into and out of the United States, and where we have specific vulnerabilities that we need Congress to address.

Tools for Concealment

There are countless variations on money laundering schemes and they are only limited by the imaginations of those who perpetrate them. Nonetheless, there are certain tools for concealment that are common to such schemes.

i. Shell Companies

One common vehicle used to conceal the source, ownership, and control of illegal proceeds as they move through the financial system is a shell company. A shell company can be loosely defined as a legal entity that exists primarily on paper, with no place of business or significant operations or assets. Many jurisdictions around the world – including the United States – allow individuals to form and operate such companies without providing any information about the beneficial owner. Organized criminals exploit this weakness and establish bank accounts in the names of shell companies, and then send money globally from one financial institution to the next, disguised as legitimate business activity, which may include import-export or other trade transactions.

In addition to the United States, the British Virgin Islands, Seychelles, Belize, and Panama are some other popular jurisdictions for the creation of shell companies with little or no information about who owns or controls the entity. None of these countries are fully compliant with the international standards set forth by the Financial Action Task Force on the transparency of legal entities. This marks an unfortunate role reversal for the United States, which historically has led by example when it comes to the implementation of rigorous anti-money laundering standards.

ii. Front Companies

TOC groups also use front companies to mask their crimes and conceal their profits. Unlike shell companies, which are merely an artifice, front companies are actual functioning businesses that may be wholly or in part legitimate, but are controlled or operated on behalf of criminals. Front companies serve not only to obscure the source, ownership, and control of illegal proceeds involved in trade transactions, but the commingling of legitimate money with illegal proceeds can frustrate our ability to untangle the legitimate monies from the criminal proceeds. Such commingling is a purposeful technique used by some of the most advanced money launderers as a means to confuse law enforcement and exploit gaps in anti-money laundering regimes.

iii. Offshore Financial Centers

An offshore financial center is a country or jurisdiction that provides financial services to nonresidents on a scale that is disproportionate with the size and the financing of its domestic economy. Typically associated with strict commercial and bank secrecy laws and a low tax environ, offshore financial centers specialize in providing corporate and commercial services to non-resident companies. Because money is taxed at a low rate and the identities of bank accounts holders are strictly protected, such offshore havens are a magnet for TOC to hold their illegal proceeds for the long-term. Thus, it is not uncommon to see the money trail for any particular series of money laundering transactions end in such a locale.

iv. Free Trade Zones

Free trade zones (FTZs) are designated areas within a country in which incentives are offered to support the development of exports, foreign direct investment, and local employment. Along with the positive aspect of boosting economic opportunity comes the unfortunate reality that these incentives also create opportunities for money laundering. Some of the systemic weaknesses that make FTZs vulnerable to abuse include: weak procedures to inspect goods and register companies, including inadequate record-keeping and information technology systems; lack of adequate coordination and cooperation between zone and Customs authorities; relaxed oversight; and a lack of transparency.

v. Jurisdictions Offering an Air of Legitimacy

One of the goals in using any money laundering scheme is to conceal the money's illegal past. However, money that moves through certain offshore havens or originates in certain high crime jurisdictions is likely to garner more law enforcement and regulatory attention. In order to avoid this unwanted attention and give their money an air of legitimacy, transnational organized criminals commonly design transactions so that money flows through jurisdictions that are active in foreign trade and have a reputation for integrity in their financial systems. The United States, in particular, is popular for this reason. It is far easier for TOC groups needing to move significant amounts of money to hide it in the wide stream of legitimate U.S. commerce. The efficiency of our banking system and the ease of obtaining anonymous U.S. shell companies add to the popularity of the United States as a place to and through which to launder money.

Trade-Based Money Laundering

One of the most popular methods used by TOC groups to move their money around the world is through trade-based money laundering schemes. Trade-based money laundering is a method by which criminals move illegal proceeds, often through the formal banking system, disguised as legitimate trade transactions. In the process, criminal organizations are able to exploit the complex and sometimes confusing documentation that is frequently associated with legitimate trade transactions.

This method is utilized extensively by Colombian drug cartels to repatriate drug proceeds through a trade-based scheme commonly referred to as the Black Market Peso Exchange. These organizations can accomplish settlement by purchasing commodities in one country and then transferring them to another country where the commodity is sold and the proceeds remitted to the intended recipient. The Black Market Peso Exchange has been copied and adapted to local conditions by numerous criminal organizations all across the globe. Recently, we have also seen evidence of a trade-based money laundering schemes involving the illegal trade of pirated goods.

The Ayman Joumaa DTO/Lebanese Canadian Bank case illustrates a trade-based money laundering scheme. Cocaine shipments were sent from South America, through West Africa, and on to markets in Europe and the Middle East. Proceeds from the drug sales, in the form of millions of dollars in bulk currency, were sent back to West Africa and on to Lebanon via money couriers. These undeclared cash shipments were then transferred to exchanges houses throughout Lebanon, and later deposited into Lebanese banks. Wire transfers were then sent to the United States to purchase used vehicles, which were in turn shipped to West Africa and sold. Proceeds from the car sales were co-mingled with drug proceeds and the cycle began anew.

In addition, wire transfers were also sent throughout the world to pay for goods that were subsequently shipped to Colombia and Venezuela and sold. These payments are representative of the Black Market Peso Exchange, and the Black Market Bolivar Exchange trade-based schemes.

Money Remitters

Despite the continuing prevalence of money laundering through banks, criminals also use non-bank, financial institutions, such as money remitters, check cashers, and issuers of prepaid access. Unregistered money transmitters that settle through the transfer of value, which masks that they are in the business of transferring funds through the international financial system, have been a particular challenge for the Department of Justice to prosecute. These remitters often relay transaction information to foreign counterparts only through e-mails or text that without wiretap authority make it difficult for investigators to follow the money and connect to underlying criminal activity and organizations.

Money transmitting businesses, or money remitters, receive money from customers to send to the place or person designated by the customer. The transmission can be domestic or foreign and can be sent through a variety of means. Money remitters are particularly attractive as money launderers for a variety of reasons. They are subject to far less regulatory scrutiny than banks, generally have a more fleeting and limited relationship with their customers, and provide

the anonymity vital to criminal activities for lower value transactions. Money remitters therefore represent a key law enforcement vulnerability in the financial system because they are gateways to our financial system. They can be in the business of laundering money themselves, they can knowingly provide assistance to money launderers, and money launderers can use their services without the remitters' knowledge.

Because of this vulnerability, and to promote greater transparency for these businesses, the law requires that they register with the Financial Crimes Enforcement Network (FinCEN), in addition to many state licensing requirements to remit money. The registration requirement is intended to assist law enforcement and supervisory agencies and to prevent these businesses from engaging in illegal activities. Under 18 U.S.C. § 1960, a money laundering statute, it is a federal crime to operate a money transmitting business without registering with FinCEN, or complying with state licensing requirements, or to be involved in the transportation or transmission of funds the defendant knows are derived from a criminal offense or intended to be used to promote unlawful activity.

Check Cashers

Another trend is criminals using the check cashing industry as a method of money laundering. In particular, check cashing stores around the country are being used to cash large checks or a series of smaller checks on behalf of professional criminals. This is particularly prevalent in the health care arena, where check cashers are becoming a prime mechanism to convert billions of dollars in fraudulently obtained Medicare reimbursement checks into cash – which is in turn used to pay kickbacks to complicit doctors, durable medical equipment providers, and for profit. Many of those identified as laundering proceeds of healthcare fraud through check cashing companies have been linked to Eurasian organized crime groups.

In summary, the scheme works as follows: federal regulations require a report to be filed anytime a check is cashed for over $10,000. This report is known as a Currency Transaction Report or a "CTR." The reporting obligation falls on the person or entity receiving and providing cash for the check – such as a check cashing business. Specifically, the check cashing company receiving a check to be cashed over $10,000, or series of checks exceeding $10,000, must fill out a CTR that contains the identity of the person cashing the check, and the identity of the person or entity on whose behalf the check is being cashed. Once this information and other background information is obtained, the CTR is filed with FinCEN at the Department of Treasury and used by law enforcement to detect money laundering activities.

In order to avoid detection, check cashers are either knowingly filing CTRs that include false identifying information, or are avoiding filing CTRs altogether. Because they are exempt from Suspicious Activity Report and recordkeeping requirements, check cashers can purport to be blind to fraudulent activity even as they process inherently suspicious transactions. The money laundering of healthcare fraud checks is just one example of how check cashers are being utilized by professional criminals. More often than not, the same check cashers who launder the proceeds of health care fraud are also involved in the laundering of proceeds of other crimes as well.

Prepaid Access Devices

In the past decade, the use of electronic transactions, both for personal and business purposes, has increased dramatically. While only a few years ago most payments went through some type of banking institution, that is no longer the case today. Mobile payments, virtual and digital currencies, online payment systems, mobile wallets, and prepaid cards have emerged as the payments vehicles of the future. These new payments offer TOC the ability to move money easily and expeditiously across jurisdictions that may not have effective regulations.

Prepaid access devices essentially allow access to monetary value that is represented in digital format and that is stored or capable of being stored on electronic media in such a way as to be retrievable and transferable electronically – such as through prepaid cards or mobile wallets. While the most recognizable form of prepaid access in the United States is a prepaid card, it is becoming increasingly apparent that the plastic card entails only one possible method of enabling prepaid access. Today, prepaid access can be provided through a card, a mobile phone, a key fob or any other object to which relevant electronic information can be affixed. In some contexts, there may even be no physical object, as access to prepaid value can be enabled through the provision of information over the telephone or the Internet. Prepaid cards appear in many forms – the most recognizable being the ubiquitous gift cards that can be purchased almost anywhere. However, the prepaid card that is the most likely to be used in money laundering is the open system general purpose reloadable card. This card, which is normally branded using a Visa, MasterCard, American Express or Discovery logo, allows the user to make purchases and access the global payment networks through ATMs worldwide. These cards can be loaded with cash, drained, and then re-loaded.

The United States only began to define providers and sellers of prepaid access as money services businesses and to impose anti-money laundering obligations on these providers and sellers last year, and has yet to require the reporting of monies represented by prepaid cards to be declared when they are taken across the border in substantial amounts. Despite our new regulations, we believe prepaid cards present abundant opportunities for criminals to launder money. Prepaid cards can be purchased for currency, transferred from one person to another, reloaded, resold or monies transferred from one card to another with a telephone call or a computer stroke. Prepaid cards are often used in tandem with the digital or virtual currencies as a mechanism to either purchase the digital currency or to change the digital currency into a country's currency. Digital or virtual currencies are a form of online payment service that involves the transferring of value from one person to another through the Internet. These currencies may be backed by gold, silver, platinum, or palladium, such as the digital currencies offered by Liberty Reserve or Webmoney, or, as in the case of Bitcoin, they may be backed by nothing at all. Criminals use these currencies because they often allow anonymous accounts with no limit on either the account or the value of the transaction.

The Royal Bank of Scotland (RBS) case provides an example of how TOC hackers were able to manipulate a bank's internal accounting systems and then use prepaid cards and digital currencies to access the funds in tampered accounts and to launder money computer hackers operating in Estonia, Moldova, and Russia were able to infiltrate RBS's prepaid payroll card system and issue themselves 44 prepaid payroll cards with the loading limits removed. In just 12 hours, "cashers" used the cards to withdraw almost $9 million from 2100 ATMs throughout the

world. The cashers were allowed to keep a percentage of the cash but the remainder was moved into one of the digital currencies and transferred to the hackers.

While the vulnerabilities presented by the new payment methods vary by the type and provider, all present a high risk for money laundering, terrorist financing, and other financial crimes. The primary advantage that they give the criminal is speed with which to move illegal proceeds from one jurisdiction to another, often anonymously. This ability to move money so quickly from card to card, from card to phone, from phone to a digital currency, presents a significant challenge for law enforcement. Eventually our laws will need to be updated to give law enforcement the flexibility to respond to these ever evolving payment methods.

Updating our Anti-Money Laundering Laws to Combat TOC

Adopting the TOC Strategy's whole-of-government approach, the Department of Justice is part of a multifaceted effort to disrupt the ability of these criminal organizations to move and access their funds. The Departments of Justice, Treasury, Homeland Security, and State all employ their unique authorities in anti-money laundering enforcement, forfeiture, sanctions, regulatory enforcement, customs, and international standard setting and engagement toward this end. Of course, the effort is not limited to the government, as we also rely on the private sector, and particularly the banking community, as a true partner in preventing criminal elements from exploiting our financial system. Only through a coordinated effort can we hope to succeed in diminishing the financial strength and resources of TOC.

By leveraging these coordinated efforts, and through aggressive use of our anti-money laundering laws, the Department of Justice can report some notable successes in combating the financial networks of TOC. But in far too many instances, investigations of TOC have revealed deficiencies in our current legal regime that limit or undermine completely our ability to dismantle these organizations, prosecute their members, and seize their assets. Accordingly, the Administration has put forward a comprehensive anti-money laundering and forfeiture legislative proposal entitled the Proceeds of Crime Act (POCA). As I will now discuss, POCA includes a number of provisions that would address existing gaps in our law and significantly enhance our ability to combat TOC.

<u>Modernizing Anti-Money Laundering Laws to Account for Globalization of TOC</u>

While TOC criminal conduct predominantly takes place abroad, the proceeds of those crimes are often directed toward the United States, as I have previously explained. The purpose may be to move the money through the U.S. financial system to cleanse it of the taint of illegality, to purchase real estate or other assets in the United States, or to promote further illegal conduct. While any of these scenarios amount to *de facto* money laundering, whether they actually constitute a violation of our money laundering laws depends on the nature of the underlying criminal conduct.

Congress has recognized certain foreign offenses as money laundering predicates under U.S. law, so long as the activity is a crime in the foreign jurisdiction. *See* 18 U.S.C. § 1956(c)(7)(B). Thus, an individual who commits one of the listed offenses abroad, for example, extortion, and then moves the proceeds of that offense into or through the United States, can be

charged with money laundering under U.S. law. A notable case brought under this provision involved Pavel Lazarenko, Ukraine's Prime Minister from 1996-1997, who in 2004 was convicted of money laundering in U.S. district court for moving the proceeds of his extortion crimes in Ukraine through the U.S. financial system.

Unfortunately, section 1956(c)(7)(B) does not cover the full range of foreign offenses, including a number of revenue-generating crimes favored by TOC, such as computer fraud and the trading of pirated goods. Indeed, in the Lazarenko case, although we could trace millions of dollars that he obtained from fraud in the Ukraine, we were unable to charge those transactions as money laundering because general fraud committed in a foreign jurisdiction is not a predicate under our money laundering statutes. The effect of such gaps, in both our domestic and foreign money laundering predicates, is to provide TOC and other criminals with a roadmap for how to launder money in the United States with impunity.

To address this gap we have put forward a legislative proposal that would make all domestic felonies, and foreign crimes that would be felonies in the United States, predicates for money laundering. This amendment would enable us to more readily prosecute trade-based money laundering schemes that rely on customs fraud and the trade of pirated goods, and in the process bring the United States into greater compliance with relevant international standards.

In addition to moving criminal proceeds into the United States, TOC is also able to exploit a gap in our law to launder proceeds of crime committed in the United States abroad. If criminal proceeds generated in the U.S. are deposited directly into a foreign account, and then laundered in the foreign country by a non-U.S. citizen with no part of the laundering occurring in the U.S., we lack jurisdiction to prosecute the money launderers. Our proposed amendment to section 1956 would extend extraterritorial jurisdiction to address this gap.

Harmonizing the Definition of Money Transmitting Businesses

Because the movement of money, particularly internationally, is an essential part of money laundering by TOC groups, money remitters play a vital role in their operations. The successful prosecution of Victor Kaganov for operating an illegal money transmitting business under 18 U.S.C. § 1960 illustrates how money transmitters are used by transnational organized criminals. Kaganov operated out of his residence in Oregon as an independent money transmitter without registering with FinCEN and without a state license. In order to move money into and out of the United States, Kaganov created various shell corporations under Oregon law and then opened bank accounts into which he deposited money he received from his Russian clients. He would then wire the money out of the accounts based on wire instructions he received from his clients. From July 2002 through March 2009, Kaganov conducted over 4,200 transfers, moving more than $172 million into and out of the United States.

Although section 1960 is a powerful tool to combat money laundering by TOC, some remitting businesses, such as check cashers, currency exchangers, and the providers of prepaid access devices, are not included in the scope of section 1960. Thus, while these remitters are still technically required to register with FinCEN, they are not subject to prosecution under section 1960 for failing to do so. Our proposed amendment closes this gap by harmonizing the

definition of "money transmitting business" in section 1960 with the full scope of the registration requirement.

Extending Wiretap Authority to Schemes Reliant on Electronic Communications

Our enforcement of money laundering activity is further hampered by a gap in our wiretap authority, which extends to virtually all money laundering offenses but not to section 1960. Arguably, it is section 1960 cases in which wiretap authority is *most* needed, given that remitting schemes invariably require telephonic or electronic communication among multiple individuals to direct the movement of the transmitted funds. Consider, for instance, the use of hawala to transfer money. Not only is the communication the only evidence of the transaction, but the communication effectively is the transaction. And yet because there is no wiretap authority for section 1960, law enforcement has no means of obtaining this critical evidence when this technique is used to launder money. Our proposed amendment would add section 1960 and bulk cash smuggling to the list of offenses for which we have wiretap authority.

Confronting the Problem of Commingled Funds

The use of front companies by TOC serves not only to obscure its criminal activity, but whatever legitimate money is generated by such companies can frustrate our ability to bring money laundering charges when it is commingled with illegal proceeds. Section 1957 of title 18 prohibits the spending of more than $10,000 of illegally derived money. In both the Fifth and Ninth Circuits, courts have held that when a defendant transfers over $10,000 from a commingled account containing clean and dirty money, the defendant is entitled to a presumption that the first money moved out of the account is legitimate. This "criminal proceeds -- last out" standard is contrary to all other accepted rules of tracing, and effectively prevents the government from pursuing section 1957 charges where illegal proceeds are moved through a commingled account – such as in the trade-based money laundering scheme discussed earlier.

To prevent this marginalization of section 1957, we have proposed an amendment that would clarify that when a defendant transfers funds from a bank account containing commingled funds, the presumption is that the transfer involves the illegally obtained money.

Promoting Corporate Transparency

The final legislative proposal I would like to highlight is not in POCA but is necessary to identify a problem specifically identified in the TOC Strategy – the lack of beneficial ownership information about companies formed in the United States.

As previously noted, one way in which transnational criminal organizations are able to penetrate into the U.S. financial system is through the use of shell companies. For example, Viktor Bout, notoriously known as the "Merchant of Death" and recently convicted of conspiracy to sell weapons to kill Americans, used U.S. shell companies to further his illegal arms trafficking activities. The Sinaloa Cartel, one of the major Mexican drug trafficking organizations, is believed by U.S. law enforcement to use U.S. shell companies to launder its drug proceeds. And Semion Mogilevich, an individual based in Russia and named to the FBI's

Ten Most Wanted Fugitives List, and his criminal organization, are charged with using U.S. shell companies to hide their involvement in investment activities and money laundering.

We are also seeing an increase in the use of shell companies as vehicles to conduct human trafficking. In 2001, in a case in the Western District of Missouri, a number of individuals pleaded guilty to charges involving illegal importation and forced labor after establishing two shell companies to obtain work authorization for foreign nationals and to conceal the unlawful proceeds of the criminal enterprise.

These examples all involve the relatively rare instances in which law enforcement has been able to identify a criminal using a shell company to further a criminal enterprise. In the vast majority of cases, the lack of available ownership information means that investigations involving U.S. shell companies hit a dead end. This same lack of information also hampers our ability to respond to requests for assistance from our foreign counterparts, thus undermining the U.S. role in the global offensive against the financial networks of TOC.

We believe the solution to this problem is a legal requirement that mandates disclosure of beneficial ownership information in the company formation process that will enable us to identify the living, breathing beneficial owner of a legal entity in the United States at its incorporation.

Other TOC Legislative Fixes

Exterritorial application of the RICO and VICAR statutes

As I have stated, today's criminal activity does not respect boundary lines, and we are increasingly confronting serious criminal conduct that routinely crosses national borders. The United States is the target of criminal activity emanating from all parts of the world, as member and leaders of organized criminal groups direct and conduct criminal activity from abroad that threatens the United States, its citizens, its instrumentalities of commerce, its institutions, and its national security. Transnational organized crime groups engaged in drug trafficking, violent crimes, cybercrime, money laundering, smuggling, counterfeiting, and other criminal activity all reach into the United States from outside to commit their crimes and move and hide the proceeds of their crimes.

The Racketeer Influenced and Corrupt Organizations (RICO) (18 U.S.C. §§1961-1968) and Violent Crimes in Aid of Racketeering (VICAR), (18 U.S.C. § 1959), statutes have long been, and continue to be, among the most powerful tools in the fight against organized criminal conduct and other types of serious criminal activity. The United States has used the RICO and VICAR statutes in criminal prosecutions where part of the criminal conduct and/or some of the defendants were outside of the United States. Convictions under RICO in this context include the leaders and many members of several major international drug trafficking organizations responsible for multi-ton shipments of cocaine being imported and distributed in the United States; numerous members of smuggling schemes emanating from Asia that brought in millions of dollars of counterfeit United States currency and that agreed to bring in military-grade weaponry; individuals who embezzled millions of dollars from the Bank of China and laundered

the money in the United States; and members and leaders of an organization that trafficked in fraudulent identification documents and arranged for the commission of a murder in Mexico.

Pending indictments in this context include the 2003 indictment of the aforementioned Semion Mogilevich for directing from Eastern Europe a multi-million dollar securities fraud and money laundering scheme that targeted U.S. citizens; the indictment of leaders of MS-13 for, while incarcerated in El Salvador, ordering murders and other attacks by MS-13 members in the Washington, D.C., area by cellular telephone; and the indictment of leaders and members of the Barrio Azteca gang that operates on both sides of the U.S.-Mexico border selling drugs, laundering money, and committing acts of violence, including the murder of a U.S. consulate employee in Mexico.

Given the increasing cross-border nature of crime and the threats posed by transnational organized crime, it is vital that the RICO statute and its companion VICAR statute continue to be applicable to enterprise leaders and members who direct the affairs of a criminal enterprise from a foreign country and order criminal conduct, including violent crimes, in the United States, as well as enterprise leaders and members in the United States who order murders in foreign countries or send criminal proceeds to foreign countries. However, recent decisions in several United States District Courts and in the United States Court of Appeals for the Second Circuit in the context of private civil RICO cases have held that the RICO statute does not apply extraterritorially. While at least some of the courts have explicitly expressed no opinion on the extraterritoriality of RICO in cases brought by the government, these cases have the potential to create confusion and uncertainty as to the extraterritorial application of RICO in criminal prosecutions. Indeed, the United States Court of Appeals for the Second Circuit held that RICO does not apply extraterritorially even though Congress included in the definition of racketeering activity several statutes that themselves have extraterritorial application. In fact, some of these statutes apply *only* extraterritorially, such as Section 2332 relating to murder and other violence against United States nationals occurring *outside* of the United States.

Once these courts determine that RICO does not apply extraterritorially, they look at the particular case to determine if it involves a permissible territorial application or an impermissible extraterritorial application of the statute. In making this determination, some courts have held that the "nerve center," or upper level management and decision making authority of the enterprise, must be located within the United States or the case is dismissed as an impermissible extraterritorial application. The Department disagrees with this test and believes that a RICO claim involves a territorial application of RICO either if the enterprise is located or operating in the United States or if a pattern of racketeering activity occurs within the United States. Moreover the "nerve center" test is inconsistent with the Supreme Court's requirements relating to the attributes of an enterprise under RICO. Nevertheless, court holdings such as this have the potential to wreak havoc with our ability to prosecute leaders and members of some of the very groups that pose the greatest threat to the United States today. Leaders and members of terrorist groups, organized crime groups, violent gangs, cyber crime organizations, and drug trafficking groups would be able to escape prosecution under some of our most useful criminal statutes simply because the leadership of the group directed its activities from outside of the United States, even where the enterprise is itself operating in the United States and a pattern of racketeering activity is committed within the United States.

Among the Department's legislative proposals are clarifications that both the RICO and VICAR statutes have extraterritorial application in cases brought by the United States. The clarification of RICO's extraterritorial reach and the addition of some new types of racketeering activity will allow us to prosecute the members and leaders of transnational groups for the full range of their criminal activity. The proposed legislation includes provisions that this extraterritorial application of RICO is limited to cases brought by the United States and is not available in private civil RICO cases. The legislative proposal also includes several other amendments to update and clarify RICO and VICAR that the Department would be happy to discuss with you at a later date.

Narcotics

South America is the primary source of cocaine (and significant amount of the heroin) that is illegally imported into the United States. Particularly with regard to cocaine, international drug trafficking organizations (International DTOs or TOC) based in Colombia and Peru manufacture the illicit drug and then transport it to Central America and Mexico, where Mexican traffickers take possession. Another significant route includes the distribution of the drug from Colombia to buyers in the Caribbean. The Mexican or Caribbean traffickers then illegally import the drug shipment into the United States.

Under current law, to prosecute DTOs in the United States for their extraterritorial activities under the "long arm" statute, 21 U.S.C. § 959, we must demonstrate that the particular defendant manufactured or distributed the drug "knowing or intending" that the drug would be illegally imported into the United States. Years ago, the Colombian cartels controlled the routes from South America to the United States, and therefore, it was not a significant burden to acquire evidence in the course of the criminal investigation, and to present such evidence in court, that the defendants knew the ultimate destination of the cocaine. With the rise of the Mexican cartels, however, it has become much more difficult to prove that the South American traffickers knew the ultimate destination of the drugs that they have sold to their Mexican customers. In addition, because the traffickers have become much more sophisticated about how cases are prosecuted in the United States due to the success of our obtaining the extradition of foreign drug traffickers who have been prosecuted in the United States, the foreign traffickers now commonly avoid all discussion of the ultimate destination of their drug shipments.

The Targeting Transnational Drug Trafficking Act of 2011 addresses this problem by amending the Controlled Substances Act at 21 U.S.C. § 959 to render it unlawful for an individual to manufacture or distribute a controlled substance knowing, intending or "having reasonable cause to believe" that the substance will be illegally imported into the United States. This common sense amendment holds international drug traffickers accountable for their activities when the circumstances of the transaction would give them reasonable cause to believe that the ultimate destination of the illicit substance was the United States. For instance, if the drug transaction is financed using U.S. dollars, the package branding suggests a U.S. destination, and/or the drug route suggests that the ultimate destination is the United States, then the government can present that evidence to demonstrate that the traffickers violated the drug trafficking long arm statute.

This piece of legislation also would amend section 959 to better address the international trafficking in chemicals used to make the controlled substances that are unlawfully introduced into the United States. Presently, the United States' extraterritorial authority extends only if the overseas manufacture or distribution of the chemical results in the smuggling of the chemical itself into the United States. The amendment will prohibit manufacture and distribution of the chemical when an individual intends or knows that the chemical will be used to make a controlled substance and intends, knows, or has reasonable cause to believe that the controlled substance will be unlawfully brought into the United States. Thus, those who provide such critical material support to drug traffickers based abroad who target the United States will incur a term of imprisonment of up to 20 years.

In addition, as part of the TOC Strategy, we have asked Congress to direct the U.S. Sentencing Commission to establish a better defined sentencing scheme for violations of the Foreign Narcotics Kingpin Designation Act (the Kingpin Act). The Kingpin Act (21 U.S.C. §§ 1901 – 1908, 8 U.S.C. § 1182), administered by the Department of the Treasury, prohibits transactions by U.S. persons, or U.S.-based transactions, that involve property or interests in property of designated foreign narcotics traffickers, including foreign persons designated for materially assisting in, providing financial or technological support for or to, or providing goods or services in support of a designated foreign narcotics trafficker, and foreign persons designated for being owned, controlled, or directed by, or acting on behalf of, a designated foreign narcotics trafficker. A violation of the Kingpin Act carries a statutory penalty of 10 years imprisonment generally, but it can reach up to 30 years in some circumstances, in addition to a range of fines. Currently, there is no established sentencing scheme in the guidelines. We propose guidelines that would result in a sentence of approximately three years, with enhancements in cases where individuals know or have reasonable cause to believe that the assistance will further drug trafficking activity and in certain cases that involve the provision of weapons such as firearms or explosives.

CONCLUSION

In closing, I would like to once again thank this Subcommittee for holding this hearing and bringing attention to the threat transnational organized crime poses to our financial system. The first step in combating this threat is to understand the nature and scope of TOC and the myriad ways in which it generates and then launders its vast profits. The term "TOC" encompasses a wide swath of organizations engaged in a diverse range of criminal activity all around the world, and yet what unites them all is their need for money. Going forward, with the help of this Committee, and in conjunction with our domestic and international partners, disrupting the financial infrastructures of TOC will remain a top priority of the Department of Justice.