Department of Justice

STATEMENT

OF

STUART NASH
ASSOCIATE DEPUTY ATTORNEY GENERAL
UNITED STATES DEPARTMENT OF JUSTICE

BEFORE THE

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
OF THE
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

CONCERNING

"FAILURE TO IDENTIFY COMPANY OWNERS IMPEDES LAW ENFORCEMENT"

PRESENTED ON

NOVEMBER 14, 2006

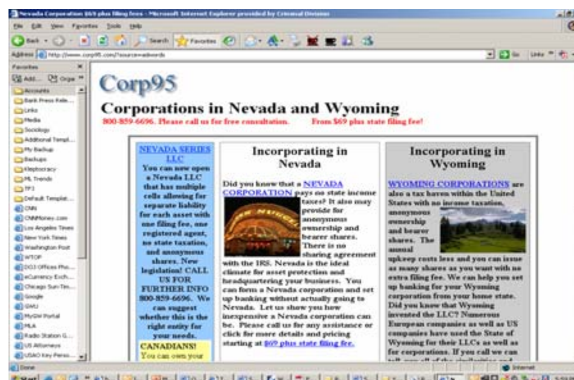
Testimony of Stuart Nash

Associate Deputy Attorney General
United States Department of Justice
November 14, 2006

Before the Permanent Subcommittee on Investigations
Committee on Homeland Security and Governmental Affairs
United States Senate

Chairman Coleman, Ranking Minority Member Levin, Members of the Subcommittee, I am pleased and honored to appear before the Permanent Subcommittee on Investigations to discuss the important topic of company formation in this country, especially in the context of the highly informative report this Subcommittee commissioned from the Government Accountability Office (GAO) earlier this year.

The words "shell corporation" often trigger the image of offshore financial centers and money laundering havens. Many people are surprised to learn that an Internet search on the words "shell corporation" will bring up dozens of domestic websites touting the anonymity, speed, and ease of using their services to incorporate in various states. For example, when we recently searched "shell corporation," the <u>first</u> website returned was one advertising corporations in Nevada and Wyoming. (See http://www.corp95.com/?source=adwords).



This website advertises that a Nevada corporation "may provide for anonymous and

bearer shares," and that, "There is no sharing agreement with the IRS." With respect to Wyoming, the website promotes anonymous ownership and bearer shares. Such corporations can be opened for $69, plus state filing fees. If you would like to purchase a "Shelf Corporation" that has a history, the website offers such aged corporations for an extra fee, and notes that, "You can have these complete companies by TOMORROW MORNING!"

In my testimony this morning, I would like to discuss with you some of the difficulties that we in the law enforcement community encounter both in our domestic investigations and in our ability to assist our foreign law enforcement counterparts in investigating their cases, as a consequence of the exponential increase in the formation of such domestic shell corporations. I would point out, however, that in this day and age, except for the most local of cases, the categories of "domestic" or "foreign" law enforcement cases are almost archaic. Virtually every major "domestic" investigation involving an organized criminal group has an international dimension, and many major "foreign" cases, if nothing else, involve the transfer of funds through the U.S. financial system. Whether the case involves narcotics trafficking, fraud, or terrorism financing, the funds involved in these cases circle the globe and have an impact on several continents. So, while it is helpful in some respects to discuss the impact of the corporate formation process in terms of the impact on our domestic cases and on our ability to assist our foreign colleagues, in the end, there is little distinction. United States law enforcement and our foreign counterparts are joined in a global offensive against organized crime and terrorism, and we must consider this problem in that broad context.

In addition, beyond the law enforcement context, I will also discuss the impact of our corporate formation policies on our standing and reputation in the global community. As I will discuss in more detail later in my testimony, the Financial Action Task Force (FATF),

the pre-eminent and highly respected multilateral group that focuses on combating money laundering and terrorist financing, identified shortcomings in our corporate formation process as an area of vulnerability in its recent evaluation of the United States' anti-money laundering regime.

Background

Corporate vehicles play a complex, varied, and essential role in modern economies. Legal entities, including corporations, trusts, foundations, and partnerships with limited liability characteristics, conduct a wide variety of commercial activities and support a broad range of entrepreneurial activities in market-based economies. However, despite the important and legitimate roles these entities play in the global economy, they may, under certain conditions, be used for illicit purposes, including money laundering, bribery and corruption, improper insider dealings, tax fraud, financing of terrorist activities, and other forms of illegal activities.

In order to move money obtained through criminal activity, or intended to promote or facilitate criminal activity, criminals must have access to accounts at financial institutions. Of course, criminals could simply open up such accounts in their own names, but as we know, criminals do not like to do business in their own names, nor do they like to identify themselves or provide any identifying information. One way to conceal their identities is to form a legal entity and open a bank account in the name of the legal entity.

In order to form a corporation, a company principal or someone acting on the company's behalf submits formation documents to the appropriate state office. Documents may be submitted in person, by mail, or, increasingly, online, and "the process can take anywhere from 5 minutes to 60 days." *Company Formations: Minimal Ownership Information is Collected and Available* (GAO-06-376) (*GAO Report).* The *GAO Report*

notes that, "A minimal amount of basic information generally is required to form a company." (*GAO Report*, p.7) Typically, the documents must give the company's name, an address where official notices can be sent to the company, share information for corporations, and the names and signatures of the persons handling the incorporation process.

As the *GAO Report* indicates, "Most states do not require ownership information at the time a company is formed," and only a few states require ownership information on annual or biennial reports in those states that require such periodic reports. (*GAO Report,* p.13) While all states require corporations to prepare a list of shareholders and maintain the list at the corporation's principal or registered office, this information is not always accurate or up to date. (*GAO Report*, p.43) The list could include nominee shareholders (*i.e.*, the shareholder on record may not be the beneficial owner), and a few states (according to the *GAO Report*, Nevada and Wyoming) allow "bearer shares" where the names of the shareholders are not on the stock certificates because ownership passes to whoever is physically holding the stock certificates.

While most states reviewed incorporation filings for the required information and fees, and checked to see if the proposed corporate name was available, none of the states reported verifying the identities of incorporators or company officials. (*GAO Report,* p.21) Not one state reported that it used federal criminal records or watch lists to screen the names of the incorporators. In sum, a person from within or outside of the United States, without any verification of identification, can submit the appropriate paperwork to form a corporation, and establish a corporation within as little as five minutes. The corporation is then a legal entity that can engage in business and open a bank account. Yet, some of the most important information about the corporation – its ownership – is nowhere recorded. If that corporation were to engage in fraudulent or negligent activity, it would be very difficult, or even

impossible, to identify its beneficial owners. If a subpoena were to be issued to the state office that keeps the register of corporate information, that office would not have any information about the beneficial owners of the corporation. If the incorporation process was handled by a third-party agent, that agent would probably not have any information concerning the identity of the beneficial owners. Domestic or foreign law enforcement agents would be stymied in their attempts to conduct an investigation because they would be unable to find out who is behind the illegal activity.

Abuse of Shell Corporations

As the discussion above indicates, shell corporations provide an opportunity for criminals or terrorists to engage in criminal activity while concealing the identities of the persons involved in the illegal activity. When business or financial transactions are conducted under the guise of a shell corporation, the identities of the persons actually conducting and benefiting from the transactions are concealed and may be difficult or impossible to identify. As the case examples below will illustrate, the use of shell corporations to facilitate criminal schemes has evolved over time. Initially, criminals used to open shell corporations and trusts in offshore jurisdictions to conceal their ownership of assets. They would then open bank accounts in the names of these corporations or trusts. As banks began to scrutinize offshore shell corporations more closely, criminals realized that they could obtain some of the same benefits of offshore corporations from U.S. domestic shell corporations, with the added benefit that the U.S. corporations would not receive the same level of scrutiny.

However, after the enhanced customer identification requirements that resulted from the USA PATRIOT Act, U.S. banks began to require more information about domestic corporations that opened accounts at their institutions. This additional scrutiny resulted in the

most recent phenomenon whereby criminals – domestic and foreign – are opening shell corporations in the United States and then opening bank accounts in the names of these corporations in foreign countries where U.S.-based corporations have an aura of legitimacy. As we know, and as the examples below demonstrate, criminals are always quick to adapt to changes in the regulatory and law enforcement environment.

"Daisy Chain" Schemes

The practice of using U.S. shell companies to hamper criminal investigations is not new to U.S. law enforcement authorities. In the late 1980s and early 1990s, Russian and Italian organized crime groups, often working in concert with one another, developed elaborate schemes using U.S. shell companies to defraud the federal government, as well as several state governments, of hundreds of millions of dollars of motor fuel excise taxes due and owing on the sale of gasoline and diesel fuel. These schemes, commonly known as "daisy chain" schemes, were designed to give the appearance that fuel was sold through a series of distributors prior to reaching the end-user, making it difficult for federal and state revenue authorities to assess and collect the taxes, and to trace the proceeds of the scheme. *See e.g., United States v. Macchia*, 35 F.3d 662, 665 (2d Cir. 1994); *United States v. Morelli,* 169 F.3d 798, 801 (3d Cir. 1999*); Enright v. United States*, 347 F. Supp. 2d 159 (D.N.J. 2004).

Several of the distributors making up a "daisy chain" were merely shell companies, or front companies, that never took possession of, or title to, the fuel, but were inserted in the distribution chain solely to generate false invoices and to conceal the identities of the individuals and entities who were actually buying and selling bootleg fuel – that is, fuel on which the excise taxes had not been paid. The fuel was ultimately sold to unwary retailers for an amount which included the cost of the tax, but instead of properly paying the tax to the

government, the conspirators kept the funds for their personal enrichment.

The daisy chain schemes were structured so that the relevant excise tax liability appeared to be incurred by one of the shell companies, which usually consisted of little more than a mail drop, a telephone and a fax machine. When IRS agents and state revenue examiners attempted to assess and collect the taxes, they were typically frustrated because the company had essentially disappeared, and only listed nominees as the officers and directors. Likewise, bank accounts held in the names of these shell companies were used to launder the proceeds of the schemes, which were often wired to offshore accounts. The operation of these schemes was most prevalent in the northeastern United States. Many of these shell companies were incorporated in Delaware and Pennsylvania.

United States v. Semion Mogilevich

Semion Mogilevich and his co-conspirators are presently wanted in the Eastern District of Pennsylvania to stand trial for racketeering, fraud and money laundering, in connection with a multi-million dollar scheme responsible for defrauding thousands of investors in the United States, Canada and abroad in the stock of YBM Magnex International, Inc. ("YBM"), a public company headquartered in the United States.

The Indictment, filed on February 26, 2003, alleges that Semion Mogilevich funded and controlled the "Mogilevich Enterprise," which consisted of a network of individuals and companies throughout the world. Between 1993 and September 1998, these defendants conspired to defraud investors of over $150 million through a sophisticated scheme designed to create an illusion that YBM was a highly profitable international business, engaged primarily in the magnet industry. YBM operated in over twenty different countries including the United States, Canada, England, Hungary, Russia, the Ukraine, and Israel. The scheme ultimately collapsed in May 1998 with the execution of federal search warrants in

Pennsylvania and the suspension of the trading of YBM stock by the Ontario Securities Exchange.

The scheme made extensive use of shell companies to conceal the involvement of Mogilevich and his associates as the beneficial owners of YBM, to fraudulently inflate the value of YBM stock, to create false financial books and records, to control ownership of the stock, and to launder proceeds from the scheme. For example, approximately ten U.S shell companies incorporated in New York and Delaware appeared on the false books and records of YBM as buyers of YBM products, or as vendors of raw materials needed to manufacture magnets. The actual ownership and operation of the companies were located in Eastern Europe. However, these shells (with U.S. addresses) allowed YBM to misrepresent to securities regulators, auditors and the investing public that YBM was a lucrative investment opportunity with substantial sales in stable North American markets. This served to raise the value of the YBM stock. In reality, the conspirators were only using the shell companies as conduits to launder the proceeds from the sales of artificially inflated stock.

Securities Fraud Cases

Shell corporations have proved to be a popular mechanism to facilitate other securities fraud schemes as well. For example, in an FBI undercover operation labeled "Operation Uptick," 120 defendants, including members of all five New York City Mafia crime families, were indicted for participating in a securities fraud scheme that cost investors $50 million. Charges included racketeering, securities fraud, pension fund fraud, bribery, extortion, money laundering and witness tampering. The investigation involved the sale of fraudulent private placement offerings to the investing public. The subjects marketed the private placements to investors as an opportunity for investors to get in early on new growth companies. In reality, these domestic shell companies were often fronts designed to give the impression of

legitimate companies. The investors' proceeds were stolen by the principals of the sham companies. In addition to the stolen funds, brokers were paid cash kickbacks to push these offerings on unwitting clients. The kickbacks were paid by promoters and insiders of the thinly-traded stocks so that they could take advantage of the falsely-inflated price and sell off their shares before the price crashed. Payments of kickbacks to brokers on these stocks were made through numerous shell companies. As a result of the investigation, 157 individuals were convicted and $153 million was seized for forfeiture.

Tax Cases

Michael Hogan Case

Shell corporations are frequently used in income tax evasion schemes to hide money from the Internal Revenue Service (IRS). While our IRS colleagues are also testifying today, I would like to highlight two cases that demonstrate how domestic shell corporations have been used in tax evasion schemes. The first such case involved two brothers named Michael and Terrence Hogan, who were indicted in Ohio in 1998. Michael Hogan operated various airline-related businesses. At some point in his life, Michael Hogan decided that he was no longer going to file income tax returns. According to the indictment, in the early 1990s, Hogan began setting up front companies in Nevada and Delaware, and he transferred airplanes and other assets into the names of those corporations. He then purported to lease the airplanes to his company, Miami Valley Aviation (MVA), thereby creating false lease payable deductions for MVA and a mechanism by which he could siphon funds from MVA. Hogan opened bank accounts in the names of the front companies to stash his money. He opened numerous accounts in Ohio, Nevada, and Georgia, and later opened accounts in offshore jurisdictions including the Cayman Islands, Costa Rica, and the British Virgin Islands. Between 1991 and 1995, MVA evaded paying taxes on $3.8 million of income.

Hogan and his brother pled guilty to tax evasion charges in 1999. Hogan received a 36-month sentence.

The use of the domestic shell corporations in this case made it difficult to prove that the funds deposited in the shell corporation's bank accounts and the assets purchased in the names of the shell corporations were actually income and assets that belonged to Michael Hogan. The government was required to prove that, despite the cloak of the corporations and their nominees, Michael Hogan owned and controlled the funds and the assets. This proof required extensive use of subpoenas for documents and testimony, and made the investigation much longer and more difficult, especially if one compares how much easier it would have been to meet our burden of proof if either (1) the corporations were in Michael Hogan's business's name, or (2) the corporate records explicitly identified him as the beneficial owner.

Terry Neal Case

The second tax fraud case involves a defendant named Terry Neal, who was convicted of tax-related offenses in the District of Oregon. On April 23, 2003, a grand jury returned a thirteen-count indictment against Terry Neal and others. The indictment alleged that, since at least 1995, the defendants conspired to hide assets, income and expenditures from the IRS, for themselves and their clients. The defendants established foreign and domestic shell corporations for themselves and their clients, and then established domestic and foreign bank and securities accounts for the corporations, and devised a variety of ways they and their co-conspirators could use the funds in the United States without making the funds easily traceable to the true owner or paying taxes on them. These methods included "income stripping," the use of "warehouse banks," offshore credit or debit cards, false mortgage loans, false insurance policies, and offshore brokerage accounts.

The "income stripping" scheme involved setting up a Nevada corporation, which then billed the client's legitimate business for fictitious consulting or other services. The legitimate business would fraudulently deduct the payments as a business expense on its tax return. A "warehouse bank" account is a bank account at a regular commercial bank in which all clients' funds are commingled or pooled, for the purpose of concealing the clients' respective ownership interests of the funds. Clients would send instructions to Neal or his co-conspirators, who would conduct the transactions at their direction. Similarly, offshore bank accounts were used to conceal a client's funds, with credit or debit cards issued by an offshore bank used as one means for repatriating monies as needed.

The defendants also advised clients to purchase an "insurance policy" from a fictitious foreign insurance company. The client's legitimate business would deduct the insurance premium as a business expense on its tax return. The money would be sent offshore to the defendants, who kept six to nine percent as their fee. After a year, the balance of the funds would be deposited to one of the client's foreign bank accounts and would again be available to the client for withdrawal by debit card or other means.

In order to further conceal the scheme, the defendants prepared false, fictitious, and fraudulent documents to create a veneer of legitimacy to their clients' tax evasion. These documents included alleged false invoices for "consulting" or "services," promissory notes, consulting agreements, and insurance policies. They also prepared and filed false tax returns for the clients' Nevada corporations. These tax returns usually showed little or no tax due. When clients were contacted by the IRS, the defendants advised the clients to lie about their connection to the Nevada and offshore corporations and to destroy documents. The defendants charged substantial fees for their services.

Neal was sentenced in March 2006 to 60 months in prison and three years of

supervised release for his role in the operation of an offshore tax fraud scheme. At least fourteen clients of this fraudulent tax scheme have pled guilty in connection with their involvement. According to the Government's Supplemental Sentencing Memorandum, "Defendant (Neal) is directly responsible for defrauding the United States out of millions of dollars in taxes. His tax fraud was, quite simply, massive and on a scale rarely seen in this district. . ." The government's calculation of the tax loss was over $22 million.

Russian Money Laundering Schemes

In the cases discussed above, the criminal activity was primarily directed against the United States. However, over the past several years, we have seen numerous cases where domestic shell corporations have been established to facilitate foreign criminal activity. Several of these cases have involved activity designed to move money outside of Russia, either to evade Russian taxes or else to facilitate organized crime schemes.

Bank of New York

The Bank of New York (BNY) case was an early example of such a scheme. The BNY investigation in the Southern District of New York focused on misconduct related to the opening in 1996 of accounts at a retail branch of BNY in the names of Benex International Co., Inc. ("Benex") and BECS International LLC ("BECS"), two shell corporations that had no real legitimate business. These corporations were formed offshore. The bank accounts were opened by Peter Berlin, a Russian émigré, with the assistance of his wife, Lucy Edwards, also a Russian émigré, who was a BNY vice president. During the next three and one-half years, approximately $7 billion originating in Russia flowed through the Benex and BECS accounts to third-party transferees around the world.

The Benex and BECS accounts were part of an underground money transfer business that was operated by a bank located in Moscow and a company located in Queens, New

York. From a small single-room office in Queens, company employees executed hundreds of wire transfers per day from the Benex and BECS accounts, using electronic banking software provided by BNY to carry out wire transfer instructions provided by the Moscow bank. Despite the obvious money laundering risks associated with such an operation, BNY failed to conduct adequate due diligence or make "know your customer" inquiries with regard to Berlin or the Benex and BECS accounts. BNY also failed to monitor adequately the activity in the Benex and BECS accounts, which were the highest fee-producing accounts in the One Wall Street Branch where they were located.

These compliance lapses resulted in BNY entering into a non-prosecution agreement with the United States Attorneys' Offices for the Southern and Eastern Districts of New York in November 2005 to resolve two separate criminal investigations. BNY admitted its criminal conduct, agreed to forfeit $26 million to the United States, and to pay $12 million in restitution to victims of a fraud scheme in the Eastern District case. The bank also agreed to make sweeping internal reforms to ensure compliance with its antifraud and money-laundering obligations, and to be subject to monitoring by an independent examiner.

United States v. Garri Grigorian

A more recent case that followed the pattern of the scheme in the BNY case but utilized domestic shell corporations is the case of Garri Grigorian. On August 8, 2005, Garri Grigorian, a 43-year old Russian national living in Sandy, Utah, was sentenced to 51 months imprisonment and ordered to pay $17.42 million in restitution to the Russian government for his role in laundering over $130 million on behalf of Moscow-based Intellect Bank and its customers through bank accounts located in Sandy, Utah.

The criminal charges arose out of a relationship between Grigorian and Intellect Bank that began in 1998. In order to carry out the scheme, Grigorian, his co-conspirators, and an

associate established three U.S. shell companies and then opened bank accounts at banks in New York and Utah in the names of these shell companies. The shell companies never did any actual business. They formed two Limited Liability Corporations (LLCs) in Utah and one corporation in New York. These companies were acquired so that bank accounts could be established in their names, and thus make it appear as though wire transfers to and from those bank accounts were in furtherance of legitimate foreign trade with a U.S. company.

Grigorian and his co-conspirators opened bank accounts in business names, at local bank branches in Utah, to enable Intellect Bank to conduct U.S. dollar wire transfers on behalf of its customers. Intellect Bank regularly transferred large amounts of funds to the business bank accounts on behalf of Intellect Bank's customers. Intellect Bank would transmit instructions to Grigorian and his co-conspirators in Utah, directing where to wire transfer the funds deposited in the business accounts. Deposits were then made to the business accounts in bulk amounts on a daily basis. Then, Grigorian admitted, he and his co-conspirators transferred the funds out of the accounts to a large number of third-party transferees located around the world. Typically, there were numerous wire transfers in a single day to and from the business accounts. The investigation disclosed that there were more than 5,000 wire transfers to and from the business accounts in Utah from in or about October 1998, up to and including in or about January 2001, totaling more than $130 million.

Records from the Utah state agency provided limited details of the owners of the shell companies. Documents for the first company formed provided only the names of a registered agent and two managers of the company. Documents for the second company formed provided the name of a registered agent and a manager of the company. While a name was provided for the owner of the company, no address other than Moscow, Russia was listed. It was only through the verification of bank records that investigators were able to determine

that the actual owners of the companies were two individuals listed on the documents as a manager and an officer. Thus, the name provided on the state agency documents as the owner was merely a nominee name used in an effort to conceal and disguise the true owners. It was only because the true owners established bank accounts in the names of the shell companies and the fact that the bank maintained information that was not accessible from the state agency, that the true perpetrators of the scheme were revealed.

However, while the investigators could get to the owners of the Utah shell companies, the money flowing through the account was linked to numerous other U.S. shell companies. The fact that we could not determine the owners of those companies made it difficult to charge Grigorian with money laundering because we were unable to determine the source of the funds. Had we been able to ascertain the owners of those companies, our investigation could have proceeded further. We attempted to get details on the beneficial owners of the accounts from the banks, but most of the money went through correspondent accounts of foreign banks so that was a dead end. We had allegations of corrupt foreign officials using these shell accounts to launder money, but were unable -- due to lack of identifying information in the corporate records -- to fully investigate this area.

Recent Developments in Domestic Law Enforcement Cases

Criminals have learned from the Bank of New York and Grigorian prosecutions, and devised a more complicated version of the same scheme to evade law enforcement. Criminals who establish shell corporations in the United States are now increasingly opening bank accounts for those corporations in offshore jurisdictions where customer identification requirements may be less rigorous. However, these corporations are still able to gain access to the U.S. financial system if the foreign bank has a correspondent account at a U.S. financial institution. As the *GAO Report* noted:

> Customer Identification Program (CIP) requirements implemented by the USA PATRIOT ACT in 2001 establish minimum standards for financial institutions to follow when verifying the identity of their customers in connection with the opening of an account. Under these standards, financial institutions must collect the name of the company, its physical address (for instance, its principal place of business), and an ID number, such as the tax identification number. . . . One representative said that his institution also checked names against the OFAC [Office of Foreign Assets Control] list and requested photo identification from all signers on the account.

GAO Report, p.44.[1]

Thus, now the criminals establish U.S. shell companies in the names of nominees and through intermediaries. The criminals then establish bank accounts in the name of the U.S. shell companies in foreign jurisdictions. Latvia remains a popular jurisdiction for opening such bank accounts, but other jurisdictions are used, as well. Because the customer is a U.S. corporation, the customer has a certain aura of legitimacy. The foreign bank, in turn, has a correspondent account with a U.S. money-center bank in New York. The criminals then run the same scheme, described above, through the foreign bank, using the U.S. correspondent account to facilitate transactions.

On the surface, it appears as though wire transfers are being made to further foreign trade with a U.S. company that has a bank account in New York. In actuality, the criminals are running an underground banking channel in which it is nearly impossible to determine the source, nature, or destination of the money moving through it (which by all estimations amounts to billions of dollars). U.S. law enforcement agencies cannot determine who is

---

1 With respect to beneficial ownership of the corporation, representatives of the financial community told the GAO investigators that, although they are not required to obtain ownership information in all cases, as a result of our "risk-based approach" to customer identification requirements, financial institutions routinely investigate high-risk applicants in order to uncover the ultimate beneficial owners. They further said that conducting the necessary due diligence on a company can be expensive and time-consuming because "institutions must sometimes peel back layers of corporations or hire private investigators to find the actual beneficial owner or owners of a company." *(GAO Report*, p.45) The result is that financial institutions, through their due diligence obligations, end up having to compensate for the fact that little or no due diligence is conducted when a corporation is established by a state agency.

perpetrating the scheme by reviewing the records maintained by the state where the U.S. shell company was formed because the criminals use nominees on the paperwork and purchase the shell company via an intermediary. Law enforcement also cannot determine who is perpetrating the scheme by reviewing the U.S. bank account records. The U.S. bank account records only identify the account holder of the correspondent account (*i.e.*, the foreign bank, itself). The records do not identify who controls the accounts within the foreign bank. U.S. law enforcement must get this information from the foreign country.

Getting such information from foreign countries is time consuming at best and often very difficult for a variety of reasons, including the prerequisites for Mutual Legal Assistance Treaty (MLAT) requests and lack of cooperation from some foreign countries. Even under the best of circumstances, the MLAT process is time-consuming. In some cases, following the money trail requires MLAT requests or other formal outgoing requests to multiple countries to obtain the necessary evidence. The combination of using domestic shell companies, where little or no useful information is available, with foreign financial institutions, where information can be difficult or time-consuming to obtain, makes these cases very difficult for us to investigate and prosecute.

Incoming Mutual Legal Assistance Requests

The use of domestic shell corporations in criminal schemes not only frustrates our domestic law enforcement efforts, but also frustrates the efforts of our foreign law enforcement counterparts. When the perpetrators use U.S. shell corporations to open bank accounts in foreign countries to launder money or otherwise facilitate criminal activities in those countries, foreign law enforcement will go to the foreign bank to obtain information about the owners of the accounts. If the bank account is in the name of a U.S. corporation, foreign law enforcement will have to request information on the beneficial owners of the

corporation from the United States. This is most commonly done through an incoming request pursuant to an MLAT with the United States if one is in effect, or else through the more cumbersome Letters Rogatory process.

The Office of International Affairs (OIA) in the Criminal Division of the Department of Justice is the central authority for handling incoming requests for assistance from foreign countries. When OIA receives a request for assistance, it will usually transmit the request to the U.S. Attorney's Office in the district in which the evidence is located unless it appears that all the evidence sought in the request in that district could be obtained without a subpoena. Requests for corporate records are transmitted to the FBI because the information is generally available without a subpoena. However, depending on what other assistance is sought in the request, the request may be transmitted to the U.S. Attorney's Office to execute in coordination with the FBI field office. In Delaware, because of the volume of requests, OIA relies upon the U.S. Attorney's Office for the District of Delaware to execute all of these requests. However, because of the lack of adequate disclosure or reporting requirements at the state level, the corporate records filed with the state agency -- either the articles of incorporation or the periodic reporting records -- will not identify the beneficial owners of the corporation. Moreover, it is not uncommon for the corporations to be inactive, so any information may be out of date. Consequently, the foreign investigation may be stymied at this point.

While the Department of Justice does not maintain statistics based on legal assistance requests specifically related to shell corporations, OIA, as the central authority for executing requests for international evidence, gains intelligence which both corroborates and illuminates the scope of the U.S. shell corporation problem. A review of MLAT requests received during 2004 and 2005 disclosed that, over the past several years, OIA has received

an increasing number of incoming legal assistance requests which, in the course of being executed, are revealed to involve U.S. shell corporations. This survey indicated that in 2004, OIA received 198 legal assistance requests from Eastern European countries, and that 122 of these requests involved U.S. shell corporations. In 2005, those figures increased to 281 requests received from Eastern European countries, with 143 of those requests involving information involving U.S. shell corporations. The majority of those requests came from Russia and the Ukraine. In most of those cases, OIA had to respond by saying that information about the beneficial owners of the corporation is not available. At a time when we are trying to foster good relationships with our law enforcement counterparts and encourage international cooperation, such responses are counterproductive and damaging to our credibility.

Company Formation Agents

Another factor that contributes to the frustration of law enforcement when investigating shell corporations is the use of company formation agents. Company formation agents help individuals or companies form companies by filing formation documents and other paperwork with the appropriate state agencies. In some cases, these agents perform other services as well, such as serving as an agent for service of process, or even serving as a director of the newly-formed corporation. As the *GAO Report* points out, there is very little oversight of these agents by the states. The agents rarely collect information on ownership since the states do not require it. States generally do not require the agents to verify the information collected from clients. Some of the company formation agents open thousands of corporations and market these corporations around the world. In response to an incoming request for assistance in a foreign investigation, a registered agent told U.S. authorities that he estimated that he opened more than 8,000 companies for a foreign company broker over a

ten-year period, primarily in Delaware and Oregon, without meeting anyone personally or having any knowledge about the business purposes for these entities. These foreign brokers are then able to sell the U.S. corporate entities to anyone willing to pay the price for a U.S. corporation.

Our colleagues at the U.S. Immigration and Customs Enforcement (ICE) have advised us that their special agents have encountered several cases where third-party agents incorporate vast numbers of businesses in various states. When ICE encounters cases involving the use of shell corporations, it is usually incidental to other violations, such as money laundering or fraud.

In one such case, the investigation began with information (a Suspicious Activity Report or SAR) received from a bank that an individual received over $1 million in his account from various banks in Latvia, Russia, and Lithuania. The amount of money moving through the accounts seemed unusual because the individual listed his occupation as a self-employed construction worker. One of the financial transactions was conducted on behalf of a company registered in both Austria and Salem, Oregon. The registered agent for the company in Oregon was identified and interviewed for information in November 2003.

During that interview, the third-party agent outlined his involvement in registering companies. Basically, he advertises his status as a third-party agent on the Internet and responds to requests from overseas to register companies in the U.S. The agent receives $80 for every corporation he establishes. Over the course of several years in that business, the agent registered over 2,000 corporations, over 1,200 of which were still active companies at the time of the interview. The registrations took place mostly in Oregon, but also in Arkansas, Colorado, Idaho, Iowa, Kentucky, Montana, South Dakota, Washington, and West Virginia.

Most of the requests to the third-party agent for incorporating businesses in the USA involved “Eastern Europeans.” According to the agent, Oregon maintains some of the lowest costs for forming corporations, and Oregon law requires very minimal information when forming corporations. Also, once he completes the paperwork and forwards the information to the requesting party, he no longer has a part in the business.

ICE ultimately closed this case because the main target of the original case had moved and could not be found. However, many investigations lead to a similar fate. Banks file numerous SARs disclosing suspicious movements of money by corporations, and investigations initiated on the basis of these SARs frequently lead to a dead end because the case involves a U.S. shell corporation that has opened an account at a foreign bank, and sufficient information concerning the purpose or the true nature of the transaction cannot be obtained.

The Financial Action Task Force

The FATF is the preeminent multilateral group that addresses money laundering issues. The United States is one of the founding members of FATF. Since its creation in 1989, the FATF has spearheaded the effort to adopt and implement measures designed to counter the use of the financial system by criminals. It established a series of 40 Recommendations in 1990 that set out the basic framework for anti-money laundering efforts and are intended to be of universal application. These Recommendations were revised in 1996 and in 2003 to ensure that they remain up to date and relevant to the evolving threat of money laundering,

In reviewing the rules and practices that impair the effectiveness of money laundering prevention and detection systems, the FATF found that:

Shell corporations and nominees are widely used mechanisms to launder the

> proceeds from crime, particularly bribery (*e.g.* to build up slush funds). The ability for competent authorities to obtain and share information regarding the identification of companies and their beneficial owner(s) is therefore essential for all the relevant authorities responsible for preventing and punishing money laundering.

See FATF Report on Misuse of Corporate Vehicles, p.5 (October 2006) (available at http://www.fatf-gafi.org/pages/0,2987,en_32250379_32235720_1_1_1_1_1,00.html).

Consequently, several of the 40 Recommendations address steps that nations should take with respect to shell corporations, most notably Recommendation 33:

> Countries should take measures to prevent the unlawful use of legal persons by money launderers. Countries should ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities. In particular, countries that have legal persons that are able to issue bearer shares should take appropriate measures to ensure that they are not misused for money laundering and be able to demonstrate the adequacy of those measures. Countries could consider measures to facilitate access to beneficial ownership and control information to financial institutions undertaking the requirements set out in Recommendation 5.

Probably the most unique element of the FATF, and a major contributor to its success, is the process of peer review. The 40 Recommendations are exactly that – recommendations. The Recommendations are not binding on any member. However, compliance with the 40 Recommendations is encouraged by the process of peer review implemented through a program of mutual evaluations. Under the mutual evaluation program, each jurisdiction is periodically examined by a team of reviewers to assess each member's compliance with the 40 Recommendations. Jurisdictions are given a ranking of Fully Compliant (FC), Largely Compliant (LC), Partially Compliant (PC), or Non Compliant (NC) with respect to each Recommendation.

The United States has undergone three such evaluations, with the most recent one taking place earlier this year. The evaluation report was presented to the FATF Plenary in June 2006. While the overall evaluation of the United States was very positive and lauded

our efforts in terms of investigations, prosecutions, and seizures, the United States received four rankings of NC. Two of these four NC rankings were based on our laws and regulations relating to legal entities and beneficial ownership (Recommendations 33 and 34). The Report found that the United States is not compliant with respect to Recommendation 33 ("Transparency of Legal Persons and Arrangements") because:

> While the investigative powers are generally sound and widely used, there are no measures in place to ensure that there is adequate and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities.

As a result of these NC rankings and the PC ranking the U.S. received on core Recommendation 5 regarding customer due diligence (of which identification of beneficial owners is a significant part), the United States must provide a succinct update to the FATF Plenary in June 2008 describing the corrective actions it has or is taking.

Of course, company formation processes within the United States have traditionally been within the province of the individual states. As FATF itself recognized, it is an over-simplification to simply label the "United States" as non-compliant in this area. Rather it is the company formation mechanisms within fifty individual states that are currently deficient in this respect.

However, it is important to recognize that, as the *GAO Report* points out, some jurisdictions that have had reputations as "money laundering havens" have enacted measures to regulate firms that provide services such as company formation. The United Kingdom Crown Dependencies of Jersey and the Isle of Man began regulating company service providers in 2001 and 2000, respectively. In those jurisdictions, company service providers now must be licensed, and are required to conduct due diligence to verify the identity of their clients and to obtain company ownership information to form a new company. By

implementing these measures, Jersey and the Isle of Man have taken a major step toward ensuring that information concerning the beneficial ownership of new corporations will be obtained. In order to address privacy concerns, the ownership information is not maintained in the public record, but is kept at the registry in Jersey and with company service providers in the Isle of Man, and is available only to law enforcement.

In fact, many jurisdictions in the Caribbean, once labeled as "money laundering havens," have taken similar measures. For example, the Cayman Islands has enacted legislation to regulate company service providers. They are now governed by the Companies Management Law (2003 Revision) and its accompanying regulations, and supervised by the Fiduciary Services Division of Cayman Islands Monetary Authority (CIMA). A large range of service providers falls within the ambit of the law — law firms; asset managers; those providing registered office, company secretary, and alternate director facilities; administering offices; and trust service providers. Allowance is also made for additional corporate services to be included. A corporate service license is required for those providing basic services such as company formation, and the filing of statutory returns. Service providers controlling assets or acting as secretary, authorized custodian, or other more substantive functions require a companies-management license. Trust companies are, however, licensed under the Banks and Trust Companies Law (2003 Revision), while insurance and fund managers are licensed under the insurance and securities investment business laws.

Compliance with the Cayman money laundering requirements is effected through CIMA's supervisory process. CIMA's Fiduciary Supervisory Division is responsible for supervising trust companies and company management service providers, and applies the same high standards during the licensing and "Know Your Customer" process as is applied in other industry sectors. An on-site inspection program has been implemented that reflects the

Offshore Group of Banking Supervisors' *Trust and Company Service Providers Statement of Best Practice*. Company managers must submit audited financial statements to CIMA. In addition, company manager directors must submit a certificate of compliance with the AML requirements on an annual basis. The Money Laundering Regulations require that Cayman Islands Financial Service Providers (FSPs) implement procedures regarding customer identification, suspicious transaction reporting, employee training, and record keeping. Laws protect those who make reports, and tipping-off (*i.e.,* notifying a customer that a suspicious transaction has been reported) is penalized. Additionally, any bearer shares issued by a corporation must be immobilized and held by a custodian outside of the corporation. The steps taken by other jurisdictions to address the problems presented by shell corporations demonstrate that the problem is not insurmountable.

Conclusion

I would like to conclude by expressing the gratitude of the Department of Justice for the continuing support that this Subcommittee has demonstrated for anti-money laundering enforcement, especially in the area of correspondent banking. The Department believes that we must continue to strengthen our anti-money laundering laws, not only to fight drug trafficking but also to fight terrorism, white collar crime and all forms of criminal activity that generate or utilize illegal proceeds. The downside of globalization is that it affords perpetrators of crime new outlets and vehicles for these crimes, and thus poses new threats to confront. We in the Department of Justice look forward to working alongside our Treasury and Homeland Security colleagues, with this Subcommittee and with your colleagues in the Senate and the House to address the issues identified in this hearing.

I would welcome any questions you may have at this time.