Volume I: No. 2 April 2004

U.S. Immigration and Customs Enforcement

TRIPWIRE

"Integrity is the CORNERSTONE of our financial systems"

TRIPWIRE is published by the U.S. Department of Homeland Security, Bureau of Immigration and Customs Enforcement (ICE). It is distributed to the public free of charge to support ICE's law enforcement mission. Tripwire is not affiliated with any private, commercial, or non-governmental entity.

Inside TRIPWIRE

Following the Money	2
New IRS Team Provides Education to Combat Money Laundering	3
Project COLT: Telemarketing Fraud	3
Financial Tidbits	4
Cornerstone Launches Expansion of Partnerships	4
Calendar of Events	5

www.ice.gov

Toll-Free Tip Line:
1-866-DHS-2ICE

Around the World

Foreign Political Corruption Task Force

ICE IN CARIBBEAN ISLANDS, SOUTH AND NORTH AMERICA

On March 20, former Nicaraguan President Arnoldo Aleman was imprisoned after being convicted for his role in diverting nearly $100 million in public funds from his nation's bank accounts. ICE investigators, working with their Nicaraguan counterparts, discovered that Aleman had stashed at least $5.5 million in the United States, with real estate investments in Florida and hundreds of thousands of dollars in certificates of deposit at U.S. banks.

In a world of globalized financial markets, bribery, fraud, and embezzlement cannot go unchecked. Frequently, as in the Aleman case, corrupt foreign leaders will channel illicit funds to U.S. financial institutions for laundering or investment.

While there are numerous indicators that could signal a corruption case, "red flags" for investigators might include irregularities like the following:

- High-ranking government officials establishing offshore companies and bank accounts.
- Officials writing checks for non-existent goods and services to companies owned by a politician, his associates, or family members.
- Wire transfers to bank accounts in the United States or elsewhere.
- Government officials purchasing significant assets or investing in high-end real estate in the United States or other countries.
- Officials accumulating unexplained financial wealth, often inconsistent with information provided on public disclosure forms.
- Disregard of general accounting procedures for purchases of government equipment and use of government funds.
- Government checks issued to individuals with no justification listed on the books and cashed at exchange houses.

In recent years, the U.S. government has assisted governments in Central America, South America, and the Caribbean region to build cases against government officials and prominent citizens who accept bribes and embezzle funds. To this end, ICE has established a pilot program – the Foreign Political Corruption Task Force Unit (FPCTF) – to address these crimes. This Miami-based task force draws upon the combined resources of ICE, the U.S. Attorney's Office, and the Bureau of Alcohol, Tobacco, and Firearms to identify, investigate, and, where possible, help prosecute cases of public corruption and money laundering.

The FPCTF brings to bear all of our resources in the fight against foreign public corruption. ICE Special Agents offer critical assistance to foreign governments in sensitive embezzlement and bribery investigations. Furthermore, ICE attaches in U.S. embassies throughout the Caribbean and Latin American region have been tasked with providing lists of potentially corrupt officials to be denied visas to ensure they can't flee to the United States. The 2001 USA Patriot Act included several anti-money laundering provisions that will serve as a critical tool in this battle, allowing us to pursue civil forfeiture of proceeds and property related to foreign offenses.

In the past, numerous retired officials from Latin America and the Caribbean have purchased fashionable homes in the United States—living off the proceeds of bribes, fraud, and embezzlement. The FPCTF will ensure that these criminals face the full force of the law. The United States will not be a safe haven for corrupt foreign officials.

The Business Community and ICE's"Cornerstone" Program

Building Partnerships To Ensure Economic Security

One clear lesson our nation learned after September 11, 2001, was that we could not afford to take homeland security for granted. With the creation of the Department of Homeland Security (DHS), our government took a major step toward better addressing threats to our nation and our way of life.

But an effective homeland security effort also requires the cooperation of the private sector. After all, a terrorist attack of any kind would have major consequences for business—undermining confidence, shaking markets, and spreading ripples throughout the economy. We all remember the effects of shutting down the aviation system for three days in September 2001; more recently, the March 11 railway bombings in Spain illustrated how a terrorist strike could rattle consumer confidence around the globe. A terrorist attack that systematically targeted a particular economic sector—through cyberattacks or bioterror, for example—could have equally serious consequences.

Clearly, the business community has a real stake in our nation's security. That's why business leaders at every level—from large industry to independently owned businesses—should work in partnership with local, state, and federal governments to develop effective security strategies.

To this end, U.S. Immigration and Customs Enforcement (ICE), the investigative arm of DHS, has developed "Cornerstone," a comprehensive program to safeguard and strengthen our economic and financial systems. "Cornerstone" directs ICE's investigative and enforcement tools toward tracking the money and methods that terrorists and criminal networks use to fund their activities and shutting down vulnerabilities in our financial systems. ICE investigates and prosecutes a wide variety of economic crimes that affect virtually every sector, including money laundering, commercial fraud, intellectual property rights violations, and smuggling and trafficking.

"Cornerstone" also offers an exchange through which business and government can share information about potential economic and financial vulnerabilities. To facilitate that exchange, ICE will staff "Cornerstone" agents as full-time industry liaisons in each of the agency's 27 regional offices. These agents will serve as resources for business while helping to educate the public about the importance of economic security. By working together with the business community, ICE hopes to:

- Ensure that businesses are not vulnerable to exploitation by terrorists, criminal organizations, or money launderers;
- Help business owners avoid getting caught in a legal situation as a result of not knowing the law;
- Build two-way information-sharing partnerships through which "Cornerstone" can identify and shut down threats to homeland security in our financial system.

Homeland security isn't just a federal strategy or a government initiative—it's a shared mission for all Americans, including the business community. ICE and the Department of Homeland Security understand that success in this mission will require cooperation, coordination, and communication with the private sector. NFIB looks forward to collaborating with ICE in the "Cornerstone" partnership—because the security, stability, and integrity of our markets and financial systems are integral to continued growth and prosperity.

ICE Financial Investigations, Money Laundering Coordination Center Follows the Money

Following the Money

A key fact of law enforcement in the 21st century is that financial investigations will be critical in the fight against criminal and terrorist organizations. In the Department of Homeland Security, U.S. Immigration and Customs Enforcement (ICE) aims to be the investigative leader by applying a systems-based approach to attacking financial crimes.

ICE's financial investigators and analysts build on the legacy we inherited from the U.S. Customs Service, which was empowered under the Bank Secrecy Act and Money Laundering Control Acts to investigate and interdict the illegal movement of currency in and out of the United States. High-profile Customs investigations of the past, such as the Bank of Credit and Commerce International (BCCI) case, illustrated how our financial system could be corrupted and exploited to facilitate the laundering of criminal proceeds.

As a result, law enforcement agencies in the 1990s developed greater knowledge of the extent to which money laundering had compromised our financial system's integrity. To counter the threat, investigators moved to employ new techniques, such as infiltrating money-laundering networks with undercover agents, to identify targets and dismantle criminal organizations. In turn, the information and knowledge gathered in each investigation helped spur new leads, allowing investigators and agents to pursue criminal activity more vigorously.

ICE's Financial Investigations division builds on this legacy by seeking out creative and innovative avenues for investigating these crimes. One of our top

(continued on page 3)

New IRS Team Provides Education to Combat Money Laundering

The International Monetary Fund estimates that money laundering, the process of moving funds generated from illicit activities to disguise their ownership or origin, is approximately a 3 trillion dollar industry worldwide. People launder money to conceal their involvement in criminal activity such as terrorism, drug trafficking, or illegal tax avoidance.

The Taxpayer Education and Communication (TEC) Unit of the Small Business and Self-Employed Operation Division of Internal Revenue Service has assembled a team of Anti-Money Laundering (AML) Specialists. This new team will provide education on the registration, reporting, and record keeping provisions of the Bank Secrecy Act (BSA).

The BSA requirements may apply to you, your members and/or clients. A money services business includes any person conducting business as a currency dealer or exchanger; check cashier; issuer of traveler's checks or money orders; seller or redeemer of traveler's checks or money orders; or money transmitter. These businesses must register with the Department of the Treasury and file Suspicious Activity Reports and certain other reports with the Department of Treasury.

Other types of businesses with cash transactions over $10,000 must also report those transactions to the Department of the Treasury.

In addition, if you own a bank account, a brokerage account, a mutual fund account, an interest in a unit trust, or other type of financial account in a foreign country and the value of the accounts exceed $10,000, you may be required to report the account yearly to the Department of Treasury.

If you are a money services business, deal with suspicious or large cash transactions, have a foreign bank account, or would like more information about the Bank Secrecy Act or Internal Revenue Code section 6050I, please call the TEC AML Specialist in your area (not toll-free). AML Specialists may provide seminars free of charge, if the requestor meets certain requirements.

Alex Basden, (212) 719-6764 — ME, NH, VT, MA, CT, RI, NY, PA, NJ, DE, MD

Susan Vega, (954) 423-7777 —VA, NC, SC, GA, FL, AL, MS, TN, AR, Puerto Rico

Theresa McGill, (630) 493-5190 —WV, OH, KY, MI, IN, IL, MN, WI , IA, MO

F. Kim Buggs, (281) 721-8034 —ND, SD, NE, KS, OK, TX, LA

Ulla Scott, (213) 576-3865 —Los Angeles, So. CA, NM, AZ, NV, UT, CO

David Vicente, (510) 637-2199 — No. CA, WY, MT, ID, WA, OR, AK, HI

You can find additional information about money laundering at these web sites:

http://www.fincen.gov or
http://www.msb.gov.

Following the Money

(continued from page 2)

priorities has been to attack the alternative financial systems and secondary markets that have flourished to meet the demand for money laundering, such as the Black Market Peso Exchange (BMPE). The BMPE shows how legitimate systems can be exploited to facilitate the laundering of drug proceeds. To combat this type of exploitation, ICE developed a systems-based approach to financial investigations.

One of our critical tools in this approach is the Money Laundering Coordination Center (MLCC). The MLCC was created in 1996 to serve as the clearing-house and principal supporter of ICE's financial investigations, including those targeting domestic and international money laundering organizations and systems. The MLCC gathers information on laundering targets, money brokers, bank accounts and trade data to identify systems and patterns for exploitation by ICE field offices.

Another key tool in ICE's financial investigation is the Numerically Integrated Profiling System (NIPS), software developed in 1990 to analyze import and export trade data, financial information made available by the Bank Secrecy Act, and law enforcement databases. NIPS allows ICE investigators to integrate information in the drive to develop smarter, more aggressive approaches to combating financial crime. Today, our agents use NIPS to determine trends, anomalies, and suspicious activities in the arena of international commerce. In addition, NIPS is a valuable weapon against alternative systems of moving illicit funds out of the United States, such as networks that support illegal trade in commodities like gold.

These are just two examples of how ICE is integrating existing investigative assets into its new systems-based approach to fighting financial crime. We'll continue looking for fresh ways to address the ever-changing threats to the integrity and security of the U.S. and international economic systems.

Financial Tidbits

PHISHING

Phishing (pronounced "fishing") refers to an e-mail scam under which the sender poses as an established, legitimate enterprise in an attempt to fool the receiver into surrendering private information, which is subsequently used for identity theft. "Phishing" is also referred to as "brand spoofing" or "carding."

A typical phishing e-mail directs the receiver to visit a counterfeit web site, where he or she is asked to update personal information such as passwords and credit card, social security, and bank account numbers. The counterfeit web site is set up only to steal the user's information, which is then used to order goods and services or to obtain credit.

For example, in 2003, a number of e-mail users received notifications that appeared to come from the Federal Deposit Insurance Corp (FDIC). The e-mail claimed that the receiver's bank account was under investigation and would be suspended unless the receiver clicked on a provided link and updated his or her credit information. The link led to a phony website designed to look like an official bank site. (It is relatively easy to construct a web site to look like a legitimate organization's site). By spamming large groups of people, the "phisher" counts on the e-mail reaching a small percentage of people who actually have accounts with the financial institution. With the low costs associated with mass e-mailing, a small number of responses can make the enterprise profitable.

Suspicious e-mails and suspected scams should be reported to the Federal Trade Commission (FTC). The FTC Identity Theft website (www.ftc.gov/idtheft) has more information on minimizing the risk of damage from identity theft. In addition, Microsoft has made security software available to combat the threat of fraudulent "phishing" schemes.

ICE'S CORNERSTONE PREPARES TO EXPAND INDUSTRY PARTNERSHIPS

Industry Liaisons To Be Placed In ICE Regional Offices

A key link between ICE's Cornerstone program and the private financial sector will be our special financial investigations liaison agents serving in each of ICE's 27 Special Agent in Charge (SAC) offices. Beginning this spring, each SAC office will include a Senior Special Agent serving as a designated Cornerstone point of contact – working with industry to pinpoint vulnerabilities in the financial system, sharing new information on the program, and soliciting feedback from industry. In the near future, these Cornerstone liaisons will be contacting private sector representatives to expand longstanding partnerships with the financial and trade sectors. For more information on the Cornerstone liaison program, contact your local SAC office.

ICE and Project COLT: Fighting Telemarketing Fraud

On March 27, 2004, a Montreal man pled guilty to a number of fraud and conspiracy charges for his role in a telemarketing scheme that defrauded over 80 senior citizens in the U.S. of hundreds of thousands of dollars.

This telemarketing scheme began in early 2000, taking a common form for such scams. Callers contacted senior citizens and told them they had won large cash prizes as part of a Canadian lottery. The callers went on to explain that the prizes couldn't be released until the victims prepaid taxes, duties, and fees on the winnings. In this case, the victims sent checks ranging from $20,000 to $240,000 to a Canadian address, where the money was subsequently laundered and sent to banks in the Middle East.

Telemarketing schemes have emerged as a multi-billion dollar growth industry. Worse, the perpetrators prey on lonely or vulnerable seniors, in many cases defrauding them of their entire life savings. In some instances, they hit their victims with a second round of calls, posing as law enforcement officials who will help them to recover their losses, only to solicit further funds. Once the victims realize they have been defrauded, they are often too embarrassed or reluctant to report the fraud to the authorities, which leaves the perpetrators free to continue their schemes.

The good news is that ICE is working to fight telemarketing fraud. Project COLT is a joint law enforcement initiative to combat telemarketing fraud through aggressive investigation and prosecution. In Project COLT, ICE works in partnership with the Federal Bureau of Investigation (FBI), the U.S. Postal Service, and our allied law enforcement agencies in Canada to intercept funds, track suspicious wire transfers, uncover telemarketing fraud, and, when possible, to recover defrauded money and return it to the victim. We've had outstanding cooperation from wire transmitters, who don't want to see their legitimate businesses abused by fraudulent schemes. With Project COLT, ICE's investigators are working to shut these schemes down and to protect seniors from financial loss.

TRIPWIRE

The official newsletter of Cornerstone

Secretary of Homeland Security:
Tom Ridge

Assistant Secretary, ICE:
Michael Garcia

Director of Operations, ICE:
Michael Dougherty

Director, Office of Investigations, ICE:
John Clark

Deputy Assistant Director, Financial Investigations Division, Office of Investigations, ICE:
Marcy Forman

Editor, Financial Investigations Division, ICE:
Michael Kuhn

Associate Editor Financial Investigations Division:
David Denton

The Secretary of Homeland Security has determined that the publication of this newsletter is necessary in the transaction of business required by law of U.S. Immigration and Customs Enforcement (ICE).

ICE Web site: http://www.ice.gov

Address correspondence and news contributions to:

Tripwire
Financial Investigations Division
U.S. Immigration
and Customs Enforcement
1300 Pennsylvania Avenue, NW
Room 6.3C
Washington, DC 20229

Fax: 202-927-6476
Voice: 202-927-0840

E-mail: Tripwire@dhs.gov

Invitation for Tripwire Article Submissions

MANUSCRIPT SUBMISSION GUIDELINES

Tripwire covers a broad range of topics related to financial investigations and vulnerabilities in the financial and trade sectors. Tripwire strives to present clear thinking by knowledgeable observers on important issues, that can be read with ease and pleasure by both professionals and a general audience.

We publish pieces approximately 1,000 words long that make a single, provocative point or highlight an interesting financial investigation. Articles submitted for publication should be no more than 3,000 words and may be edited for space and style if selected. Tripwire does not offer any financial compensation for any articles are images submitted and all submissions become the property of Tripwire.

We welcome unsolicited article proposals. The way to submit material is through E-mail at Tripwire@dhs.gov. Accompanying images should be submitted with the article.

The best guide to what we are looking for, in terms of both substance and style, is what we have already published, so prospective authors should start by carefully examining current and recent issues of the magazine. All submissions should be accompanied by a brief note describing the author's current and past positions, recent publications, and relevant experience. We do not have fact checkers, and rely on authors to ensure the veracity of their statements. Although we try to avoid, using footnotes in print, authors should be able to provide, if asked, appropriate citations for any facts or quotations their pieces contain.

We accept submissions on a rolling basis. The following deadlines, however, are worth keeping in mind in order for a piece to be considered for a particular issue: for the December issue, November 14; for the March issue, February 17; for the June issue, May 17; for the September issue, August 16.

Any questions on these or related editorial issues should be directed to the Tripwire Editor at Tripwire@dhs.gov.

Calendar of Events

Future Cornerstone Conferences and Training

Cornerstone is planning and scheduling future conferences and training seminars. In addition, as part of its outreach program, Cornerstone will offer individualized training seminars to financial and industry sector businesses around the country. Cornerstone subject matter experts will conduct these conferences and seminars.

The next issue of Tripwire will feature a new name, look, style and improved format. Tripwire is currently being enhanced to include articles from other ICE investigative areas that impact the U.S. economy.