Hey Crystal,

Here are pictures from my vacation. Thanks to the team at the McAdams Group, I was able to actually use my vacation time without having to bring my laptop or blackberry.

Thank you for the peace of mind.

McAdams Group

Miami, FL, USA
Tel. +(1) 305-801-8910
Fax + (1) 305-259-1985
info@mcadams-group.com
www.mcadams-group.com
www.everydaycompliance.com
Service available in English, Spanish & Portuguese.

Statistical Analysis
KYC, CIP, CDD, and EDD
Lower False Positives
Internal Audit
System Validation
Operations, Policies and Procedures Manuals

“Committed & On-Board”.... So, You Can Sail Away!
ACAMS
Executive Director: Gregory J. Calpakis, CAMS
Editor/Communications Manager: Karla Monterrosa-Yancey, CAMS
Director of Operations for Latin America: Gonzalo Vila, CAMS
General Manager: Kathleen Richardson
Global Director of Conferences and Training: Eva Binder
Marketing Manager: Kourtney McCarty
Certification Manager: Giovanna Oquendo
Account Executives: Geoffrey Chunowitz, CAMS, David Kehr, Sonia Leon, Camila Levy and Jose Lewis
Corporate Sponsorship and Advertising: Andrea Winter and Ryan Lucia
Contributing Writer: Ambar C. Loria

ACAMS ADVISORY BOARD
Chairman: John J. Byrne, CAMS, Regulatory Relations Executive, Bank of America, USA
Vice Chairman: Richard A. Small, Enterprise Wide AML and Sanctions Risk Management, American Express, USA
Samar Baasiri, CAMS, Head of AML Unit, BankMed, Lebanon
L. Kim Estrada, CAMS, Chief Compliance Officer I-TradeFX, LLC, USA
Wissam Fattouh, Deputy Secretary General, Union of Arab Banks, Lebanon
Rainer G. Hoerning, CAMS, Senior Compliance Officer and Vice President of Credit Suisse, UK
Barry M. Koch, CAMS, Senior Vice President, Washington Mutual, USA
James Richards, CAMS, EVP and Corporate BSA Officer, Wells Fargo and Company, USA
Saska Rietbroek, CAMS, President, AML Services International, LLC, USA
Nancy Saur, CAMS, FICA, Regional Head of Compliance & Risk Management, ATC Group N.V., Cayman Islands
Daniel Soto, CAMS, Managing Director-AML/BSA, Wachovia, USA

ACAMS Today is designed to provide accurate and authoritative information concerning international money laundering controls and related subjects. In publishing this work, neither the authors nor the association are engaged in rendering legal or other professional services. The services of a competent professional should be sought if such assistance is required.

ACAMS Today is published six times a year for ACAMS members.

To join, contact: ACAMS
Brickell Bayview Center
80 Southwest 8th Street, Suite 2350
Miami, FL 33130
Tel. 1-866-459-CAMS (2267) or 1-305-373-0020
Fax 1-305-373-5229 or 1-305-373-7788
E-mail: info@acams.org
Website: www.ACAMS.org • www.ACAMS.org/espanol

To advertise, contact: Andrea Winter
Tel. 1-305-373-0020 ext. 3030
E-mail: awinter@acams.org

ON THE COVER
Money laundering on the high seas p. 22
The New Year is always a time to re-evaluate what we have accomplished in the past year and what we hope to accomplish as we start anew. One of the steps for a new beginning is making a New Year’s resolution list.

As I reflect on the events that have transpired and the turbulent economic times we face, I have come up with a list of resolutions to hopefully inspire each ACAMS member:

1. Enhance marketability by obtaining my CAMS
2. Increase knowledge base by becoming an avid reader
3. Participate in professional development and trainings
4. Develop my network within my profession
5. Learn something new this year

As with every list of resolutions be sure to follow through by evaluating your resolutions using SMART (Specific, Measurable, Achievable, Realistic, Time) or by simply making sure you:

• Write down your resolution
• Place it somewhere visible
• Hold yourself accountable
• Set a timeframe for accomplishing resolution
• Follow-up

In this first edition of ACAMS Today for 2009, we cover several topics. The featured story Money laundering on the high seas discusses the eminent threat of piracy in Somalia and what measures can be taken to abolish money laundering. The enemy within identifies how to recognize those within our own companies who are violating trust by committing the crime that we are all striving to prevent — money laundering.

Learn about the emerging currency black market in Venezuela and what we need to do to mitigate this risk for our institutions. Are free trade zones havens for terrorist financing and money laundering? Read about what best practices can be instituted to stay one-step ahead of the criminal.

Finally, if you’re interested in expanding your knowledge and earning continuing education credits, don’t forget to register for upcoming ACAMS Web seminars by filling out the registration form in the back of this issue.

As always, if you prefer to read us in Spanish, you can visit us at www.acams/espanol.org to download an electronic format of ACAMS Today “en español.”

And don’t forget to send your comments, ideas for articles and submissions directly to me at editor@ACAMS.org.

Karla Monterrosa-Yancey, CAMS
Editor/Communications Manager
ACAMS
Hossam M. Abd El-Rahman, CAMS
Dubai, United Arab Emirates

Hossam M. Abd El-Rahman, CAMS is a well-known consultant, trainer and speaker with more than 12 years of experience in the fields of public accounting, banking, fraud, forensics, financial crimes, compliance, anti-money laundering, internal control and business re-engineering.

Abd El-Rahman has worked for leading conventional and Islamic banks in the MENA region where he has assumed senior positions. He is currently compliance, AML and fraud head at Samba Financial Group - Dubai, UAE. Prior to that, he was compliance supervisor at Kuwait Finance House - Kuwait. In addition to 8+ years of extensive public accounting experience in “BIG FOUR” International CPA firms including PriceWaterhouseCoopers & Arthur Andersen.

Abd El-Rahman translated into Arabic the CAMS exam study guide, supplement and preparation seminar. He is among the pioneers in setting up the Arabic AML terms and definitions. In addition, he has written many articles and white papers in the areas of AML, fraud and financial crimes that were published in various international magazines.

Abd El-Rahman is the founder and moderator of Allied Compliance Consultants (ACC), a professional network of 255 members from all over the world including: compliance professionals, AML officers, auditors, risk managers and consultants. ACC is dedicated to raising the AML, compliance, fraud and financial crimes awareness. The network provides various services including: professional discussion forum, articles, breaking news, training, recruitment, consultancy and more.

Abd El-Rahman is CAMS, Certified Fraud Examiner, Certified Fraud Specialist, and Certified Anti-Money Laundering Professional. He received his bachelor’s degree in Commerce (an accounting major) in accordance with the American Accounting principles and Auditing standards from Cairo University.

Antone Victor Sabella
Amman, Jordan

Antone Victor Sabella is a manager of the Regulatory Compliance Department which he established in 2005 at Cairo Amman Bank. He is responsible for managing compliance risks for the entire bank through monitoring, implementing and developing policies, procedures, measures and processes which ensure the full compliance with applicable laws and regulations. He advises the top senior management on how to fully comply and implement laws and regulations.

Since the efforts, methods and regulations to combat Money Laundering and Terrorist Financing have been intensified in Jordan, Sabella recently has been entrusted to manage the AML\CFT Department as well. Sabella draws on his past experience and knowledge as an external auditor in Ernst & Young to implement, develop and update policies, procedures and measures to combat and detect money laundering and terrorist financing.

Sabella’s positive attitude, along with his uncompromising moral rectitude toward fighting money laundering and terrorist financing paved the way for the development and systematization of the AML\CFT Department. Sabella has represented the bank at many international conferences, initiatives and efforts pertaining to AML\CFT. He also is proactive in delivering and participating in AML\CFT training to bank staff.

Sabella holds a bachelor’s degree in Accounting and had been working for 5 years at both Arthur Andersen and Ernst &Young as a supervisor. Currently, Sabella holds a certified compliance officer and he is keen to expand his knowledge to different horizons in these fields.

Henry Yu
Hong Kong, Hong Kong

Henry Yu, Detective Senior Inspector, Fraud Investigations, Commercial Crime Bureau, Hong Kong Police Force, Hong Kong.

Inspector Yu has served in the Hong Kong Police for more than 10 years and currently works in the Commercial Crime Bureau of the Hong Kong Police as the lead investigator and officer in charge of commercial fraud and related anti-money laundering (AML) investigation. He has extensive experience in the investigation and prosecution of director fraud/assets misappropriation, boiler room fraud, investment fraud and related money laundering cases where cross jurisdiction fund tracing, restraint and confiscation of crime proceeds is involved.

Yu has a business degree and also holds various postgraduate qualifications including a Post Certificate in Laws and a Master in Corporate and Financial Laws with the University of Hong Kong. Yu also holds a Professional Certificate in Internal Audit and Control with the Chinese University of HK Professional College.

Yu is a professional member of the Association of Certified Anti-Money Laundering Specialists and a Certified Fraud Examiner.

Yu has extensive lecturing experience in AML and fraud investigation and has given seminars to police officers, universities and professional bodies. Most recently, Yu gave a lecture on business ethics, AML and fraud to members of the Hong Kong Securities Institution.
As you know, 2008 shaped up to be one of the most challenging economic years that the world has ever faced. Due to the precipitous fall of the stock market, slumping housing sales, lower consumer spending and rising unemployment, there is no question our global economies face tough times. These factors have caused many companies and organizations to make severe adjustments to prepare for an unpredictable new year.

For 2009 there are predictions anti-money laundering (AML) will play a vital role as potential mortgage fraud and other corruption is uncovered. The need to not take our efforts off of current money laundering methods and the exploitation of new methods is as important going forward as it was in the past. Suspicious transaction reports in many countries will need to be filed and some of the cases may lead to government investigations. Depending on the size, we could see some big cases coming out of this, along with big penalties.

Back to the basics for 2009 is an important reminder of how we as AML professionals can stay afloat during turbulent times. At its most basic, money laundering is close to impossible if all parties to the transaction are well-known. Knowledge is what the entire money laundering compliance program is built upon; therefore, the center piece of any AML program is Know Your Customer (KYC). A commitment to a strong KYC is what is required. This means up-to-date policies and procedures and effective training.

What’s more, strong internal controls are a must. When budgets and personnel are cut there is strong risk of these areas weakening. It is imperative that the key decision makers are kept informed of the status and need of these programs.

With all the focus on each country’s domestic economic problems it is easy to be sidetracked. Remember that money laundering is a global phenomenon. Even in a weakened economy money flows across borders. Simply maintaining your current skills and knowledge level is not enough. You should be actively engaged in continued professional development.

During times of plenty there is always pressure to cut corners. In times of famine that pressure will become even greater. No matter how you prepare for the future; going back to business basics is crucial now more than ever. One thing is certain in these unpredictable times — this is one learning experience we don’t want to repeat.

Wishing you all a happy and prosperous New Year!

Gregory J. Calpakis, CAMS
ACAMS Today: Describe your current position and responsibilities.

Mihaly Erdos: My name is Mihaly Erdos and I am Deputy Director General of the Hungarian Financial Supervisory Authority and the Hungarian Financial Supervisory Authority’s member on the Committee of European Banking Supervisors (CEBS), and Chair of the 3L3 Anti Money Laundering Task Force (AMLTF).

AT: How did you become involved in the AML/CFT field?

ME: I succeeded Andrea Enria, the former CEBS Secretary General, who was the previous Chair of the 3L3 Anti Money Laundering Task Force, in September 2008. Since I used to work with Committee of the European Insurance and Occupational Pensions Supervisors (CEIOPS), I gained experience working with other L3 committees and as such I was approached to manage the 3L3 committee.

AT: What is the main purpose of the AMLTF?

ME: The AMLTF is a joint committee of CEBS, and its sister committees CEIOPS and Committee of European Securities Regulator (CESR), the, collectively known as the 3 Level 3 Lamfalussy committees or “3L3” for short.

The AMLTF was set up in the second half of 2006, with a view to providing a supervisory contribution in anti-money laundering (AML) and counter Terrorism Finance (TF) issues, with a specific focus on the Third Anti-Money Laundering Directive.

We have over 30 members who come from the various EU Supervisory Authorities who are members of our parent committees CEBS, CESR and CEIOPS.

In particular, our mandate is focused on the developments of risk-based approaches to Customer Due Diligence (CDD) and the Know Your Customer principle (KYC) and their impact on the internal organization and control of intermediaries.

The AMLTF provides a forum for exchange of experiences and networking between supervisory authorities, to help identifying practical issues that supervisors face in their day to day work, and when possible find common practical answers.

AT: What is the AMLTF doing to assist countries in overcoming the challenges faced through the implementation of the Third EU Directive?

ME: It is conducting several stocktakes amongst its members of practical issues facing supervisors in the area of CDD/KYC; with the intention of producing a Compendium of EU supervisory practice in implementing the Third Money Laundering Directive (3MLD), including:

• A compendium of the legislative and regulatory framework, and supervisory responsibilities/authorities per EU member state; and
• An analysis of the responses to the AMLTF 2008 Member questionnaires on assessments of the answers to the questionnaires on customer identification and on cross-border customer due diligence; and
• An analysis of issues identified in AMLTF Members’ presentations on practical supervisory implementation on 3MLD

AT: You stated that AMLTF’s main mandate focuses on CDD and KYC, what advice do you have on how to appropriately implement a risk-based approach for CDD and KYC?

ME: At this stage, given the existing differing legal frameworks and the differences in supervisory practice amongst member states in the EU, the AMLTF recognizes that the risk-based approach for CDD and KYC may not be implemented in identical fashion in the EU.

Within the AMLTF, members share their differing approaches and practical supervisory experience; and in 2009 at the AMLTF’s plenary meetings, some members will be providing presentations on specific topics in relation to their supervisors’ risk-based approach of 3MLD implementation (e.g., approaches to Ultimate Beneficial Owners (UBO) and Politically Exposed Persons (PEPs) assessments), and we hope that such presentations and their subsequent discussion will assist supervisors in their application of a risk-based approach to CDD and KYC.

AT: What are the biggest challenges AML professionals will face in 2009?

ME: To make sure that financial crime continues to have a sufficiently high profile, given the considerable changes in the current financial market. This challenge could be described as two fold, as it remains to keep on top of developments in financial crime, and from the supervisory perspective our challenge is to make sure that mitigating the risk of financial crime continues to have a sufficiently high profile — given the increasing and competing demands on supervisors arising from the current financial market.

AT: As an AML expert what is the most important lesson you have learned?

ME: Under the Third MLD, to be able to supervise effectively such a diverse group of entities, be they money services businesses, offer finance leases, provide safety deposit boxes or be a large bank, such that you identify, assess, monitor and mitigate the risks of financial crime appropriately, especially for some of the smaller firms, where you may have minimal supervisory contact nor be in receipt of prudential reports.

Interviewed by Karla Monterrosa-Yancey, CAMS, editor/communications manager, ACAMS, Miami, FL USA, kmonterrosa@acams.org
Stolen Without A Gun

Authored by Walter Pavlo, Jr. & Neil Weinberg  •  Publisher Etika Books  •  Co. 2007, 285 Pages

Stolen Without a Gun details the life of an employee from his first day with the MCI in 1992 to the day he entered federal prison in 2001. The book recounts the mistakes the employee made and the temptations he succumbed to while working for MCI. His story provides a powerful and compelling description of the decision to engage in a form of corruption that not only invaded MCI but that is threatening to invade and corrupt the core values of other modern corporations. This form of corruption — money laundering — is described using a powerful storytelling genre. In the end, the book by Walter Pavlo, Jr. and Neil Weinberg, published by Etika books, provides a rich description of and insight into the psychological and social reasons why individuals may participate in money laundering schemes.

The story is centered around the 1998 merger of MCI and WorldCom. When MCI-WorldCom subsequently filed for Chapter 11 bankruptcy protection on July 21, 2002, the failure garnered a lot of headlines. There were interviews with Bernard Ebbers, the president of MCI-WorldCom, and many investigative reports about the problems leading to this failure. What is interesting about the reports is that all the attention focused primarily on the WorldCom side of the business. No one seemed interested in or questioned the MCI role in the company’s demise. In fact, when the firm emerged from Chapter 11 bankruptcy protection in 2003, it took back the MCI name, possibly to distance itself from the problems associated with WorldCom.

The story begins with the Pavlo family living the American dream. Walter Pavlo was married to Rhoda Voth and together they had two sons. They were homeowners and Walter was making enough money that Rhoda was able to be a stay at home mom for their two young sons. Two events set the stage for Walter’s downfall. The first was his initial hiring as a manager in MCI’s Financial Services Unit at a salary of $43,000 a year for a job that entailed collecting past due business accounts. These business accounts were not ordinary companies; they were 900 number businesses — purveyors of phone sex, astrology, racing results, for-profit evangelism, personals and sports scores. Walter soon learned that MCI had a major collection problem and that the Financial Services Unit was only allowed to write-off a fraction of the accounts that were uncollectible. The unit kept its accounts that were more than 90-days overdue to seven percent of accounts receivable and the bad debt write-offs under two percent. After three months, Walter was promoted to a higher managerial position by his supervisor William McGowan. Walter, who had become McGowan’s “first lieutenant,” was eager to fit in and move up the corporate ladder. The first hint that Walter was too eager was when he began smoking and drinking to get more one-on-one time with McGowan.

Second, early in his MCI career Walter met Harold Mann, an MCI client who operated two businesses — a 900-number and the “reseller business,” which entailed selling phone services to other businesses at a significant mark-up. Ultimately, Mann would turn out to be one of Walter’s biggest allies. Although Mann was only two years older than Walter, he had what Walter wanted — a mansion, unlimited money and a life where he could take an exotic trip on a whim.

Walter and Mann’s paths crossed several times, both socially and professionally, and Mann eventually came up with the solution to Walter’s growing delinquent account problem at MCI. Their initial encounter was early in Walter’s career with MCI when they met to try to resolve the issue of a 90+ day past due receivable of several million dollars from Mann’s company. Not only did Mann come up with a way to put the problem at bay, but he introduced Walter to the money laundering business. A Mann protégé, Mark Benveniste, developed a firm named Manatee that used a collection process for the delinquent accounts. Manatee would place the delinquent account holders on payment plans. The monies would be applied in four ways: Manatee would receive a fee, MCI would receive partial payment and both Mann and Walter would receive a substantial amount for their part in the plan. The amount that Walter often received was more than $100,000. The receipt of such substantial amounts presented Walter with a problem — where to deposit the monies since his salary at MCI had increased only to $62,000 per year. Once again, Mann came up with a solution to Walter’s dilemma by introducing him to setting up bank accounts in the Cayman Islands. Mann was now showing Walter how to launder his money.

Walter was making large amounts of money from his money laundering activities. At the same time the stress that he was encountering at MCI to keep the amounts of accounts that were written off annually, to a level that was significantly less than the actual amount that he knew would never by collected was taking its toll. Additionally, he was spending almost no time at home and his family life was suffering. As the money rolled in, problems began to mount — writing off the portions of the accounts that MCI would never recover since they were going into Benveniste, Mann, and Walter’s pockets while keeping the bad debt expense at the limit MCI decreed it should be. Walter had also recruited people at MCI to assist him in the accounting shenanigans and collection process. The first person Walter recruited was Sean Hennessy. After Walter’s money laundering and other schemes at MCI began to unravel, it would be the recruit Sean Hennessy who would prove to be essential to the case.

Stolen Without A Gun goes beyond the untold story of MCI’s role in the downfall of MCI-WorldCom. The book profiles Walter Pavlo, an employee who ignored his moral upbringing and entered the criminal world in an attempt to meet the expectations of others. It describes the culture that existed at MCI before Walter’s arrival and how the company’s management overlooked accounting gaps and unethical behavior. The money laundering activities described in this book tell part of the story of the illegal activities that were taking place at MCI and the dangers inherent in the environment that corporations operate in today. But what makes this book even more important are the honestly made disclosures by Walter Pavlo into his decision making processes that ultimately led him to a federal penitentiary.

Deborah Pavelka, CAMS, professor, Roosevelt University, Chicago, IL, USA, dpavelka@roosevelt.edu
Free trade zones: Havens for terrorist financing and money laundering?
**What is a free trade zone?**

By definition, a free trade zone (FTZ) is an area that is a part of a country or encompasses a whole country, that allows for free trade between other regions or countries. “Free trade zones are labor intensive manufacturing centers that involve the import of raw materials or components and the export of factory products.” Free trade zones produce products ranging from clothes to sneakers to electronics to cars. Within a free trade zone, merchandise can be “assembled, exhibited, cleaned, manipulated, manufactured, mixed, processed, relabeled, repackaged, repaired, salvaged, sampled, stored, tested, displayed and destroyed.” What is unique about these areas is that they allow trade restrictions such as tariffs and quotas to essentially be eliminated in the hopes of interesting trading parties and encouraging business investments within the area, in addition to encouraging the transfer of technologies and skills outside of the zone. Benefits to the public include encouraging and attracting international trade, making the process of international trade more efficient and easier for businesses and individuals, increasing employment opportunities for individuals around free trade zones, and encouraging and facilitating domestic trade. There has been a rapid growth of free trade zones over the past 40 years throughout the world. As of 2002, 43 million people worked in approximately 3,000 free trade zones worldwide, spanning approximately 116 countries.

**Foreign trade zones in the United States**

Foreign trade zones were first introduced in 1894 in the United States, but were not fully implemented until they were reintroduced successfully as part of the New Deal under President Franklin D. Roosevelt in 1934. The U.S. established the Foreign Trade Zone Act as a means of promoting economic growth, promoting employment within the United States and encouraging free trade between countries, as well as encouraging foreign investments. This act covered how and where zones are established, how these areas are administered and what activities can and cannot occur within these areas.

Under the umbrella of foreign trade zones within the United States there are approximately 260 general-purpose zones and 450 subzones. It should be noted that there are no United States foreign trade zones operating outside of the jurisdiction of the U.S., though there are three zones located in Puerto Rico. A general-purpose zone is normally located at a port or industrial park. The most common activity within these general-purpose zones is for the purpose of warehousing goods and the distribution of goods. Subzones are special-purpose zones usually located at manufacturing plants. Subzones are approved for a specific purpose for a specific company.

Overseeing foreign trade zones within the U.S. is the United States Foreign-Trade Zones Board (FTZB), which is comprised of members of the Department of the Treasury and the Department of Commerce (DOC). Federal agencies within the United States also play a role in the operations and daily activities of foreign trade zones. The Department of Homeland Security (DHS) has the authority of designating Customs and Border Protection (CBP) officials to perform zone-related work and act as an enforcement body for activities that occur within a zone, as well as prepare and implement rules and regulations maintained within foreign trade zones through the publication of the Foreign-Trade Zone Manual (FTZM), as well as enforce the rules and regulations within a zone. Though it is not law, the Foreign Trade Zone Manual provides guidance, recommendations and regulations of proper use within a foreign trade zone. Other United States government agencies, such as the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), Department of Agriculture (USDA), Environmental Protection Agency (EPA) and the Federal Communications Commission (FCC), are also involved in the daily activities of foreign trade zones within the U.S. Most of these agencies have rules and regulations that apply directly to the activities within these foreign trade zones.

In an effort to combat terrorism, Customs and Border Protection has created the Customs-Trade Partnership Against Terrorism (C-TPAT), which addresses the issue of securing supply chains of importers, carriers, brokers, for-wards, ports and terminals, and foreign manufacturers. The security enhancements put in place by C-TPAT participants allow the Department of Homeland Security to devote more resources to high-risk shipments. It should be noted that foreign trade zone sites and facilities remain within the jurisdiction of local, state or federal governments. In 2005, as stated in its annual report to the United States Congress, the National Association of Foreign-Trade Zones stated that foreign trade zones in the U.S. provided jobs for approximately 340,000 Americans at approximately 2,500 firms, exporting US$23 billion in goods and importing $US410 billion in goods. For a listing of Foreign Trade Zones located within the United States and Puerto Rico please refer to the U.S. Import Administration Foreign-Trade Zones Board website (http://ia.ita.doc.gov/ftzpage/letters/ftzlist.html).

1Free trade zones can also be under the name of free zones, freeport zones, (port) free trade zones, foreign trade zones, duty-free trade zones, commercial-free trade zones, export processing zones, logistic zones, trade-development zones, industrial zones/parks/areas, hi-tech industry parks, hi-tech and neo-tech industrial development zones, investment zones, bonded zones, special economic zones, economic development zones, economic and technological development zones, resource economic development zones and border economic cooperation zones (from Caribbean Financial Action Task Force’s interpretive note, 2002).
2Export Processing Zone Online Web site
3United States Foreign-Trade Zones Board
4International Confederation of Free Trade Unions Web site
5Secure Seas, Open Ports; Homeland Security; June 21, 2004
6NAFTZ Web site
Each day, terrorists and money launderers find new ways to manipulate our banking systems and nonfinancial systems, in addition to unusual methods that require certain action.

Possible free trade zone vulnerabilities

There are several possible vulnerabilities associated with the area of free trade zones. These include:

- Possible lack of regulations or lack of enforcement of regulations within free trade zones;
- Use of cash or nonfinancial instruments, which are usually high risk, as the primary forms of payment that occur within these zones;
- Lack of means to implement, enforce or create regulations needed within free trade zones;
- Difficulties in determining the primary owner of the goods or the point of origin of the shipments due to the transference of many shipments into and out of multiple free trade zones around the world;
- Due to the beneficial tax incentives offered within these areas, and the decrease or lack of tax revenue gathered by customs officials, there is little incentive to enforce or implement regulations and oversee trade;
- The lack of automation and an accurate method of recording shipments and items manufactured or received within many free trade zones, causing the loss of a paper trail that can accurately verify the true owner of the goods;
- Possible zone manipulation to evade the laws of the country because often times the regulations are lax in these zones.8 Dubai poses particular concern in regard to free trade zones in that it is strategically located in the Persian Gulf. Records show that nearly a third of all counterfeit drugs confiscated in Europe last year came from the United Arab Emirates (UAE).9

Possible best practices and recommendations for free trade zones

Several areas need to be targeted within free trade zones to ensure these regions are used for legitimate business purposes:

1. A tracking system is necessary for imports and exports within free trade zones across the world to allow for countries to interface with each other, compare import and export information, and to keep a record of the types of products within these areas, in addition to a record of the businesses and individuals using these zones.
2. Information sharing is needed in regard to free trade zone trends, concerns, security issues and threats, which are crucial elements in the fight against terrorism.
3. Continued training, enhanced training or the beginning of training for some countries’ customs officials, financial intelligence units, employees at points of entry and exit, law enforcement officials, tax authorities and banking systems in regard to free trade zones would aid in possible problems faced in these zones and to ensure their legitimate use.
4. A special focus on emerging nations and developing countries should be applied. These countries are more apt to create free trade zones to capitalize on the positive benefits of these areas for their economies, so particular attention needs to be focused on these nations.
5. Lastly, a legislative body that encompasses nations from across the world to monitor and govern these areas should be implemented with a unit that focuses on the issues of money laundering and terrorist financing.

Conclusion

Though not a novel concept, free trade zones have forged a new way for potential terrorist financing and money laundering to occur within these areas. Various best practices and recommendations, as mentioned, could increase the security, regulations and enforcement within these areas that currently do not have the measures in place to monitor or detect illegal activities. Each day, terrorists and money launderers find new ways to manipulate our banking systems and nonfinancial systems, in addition to unusual methods that require certain action. The subject of free trade zones is a unique area that needs to be addressed in relation to anti-money laundering and combating the financing of terrorism.

For further information on Free Trade Zones around the world, please refer to the World Economic Processing Zones Association website (http://www.wepza.org), the World Federation of Free Zones website (http://www.free-zones.org), as well as the World Free Zone Convention website (www.freezones.org).

Heather A. Brown, CAMS, Washington, D.C., USA, HABrown35@aol.com

---

72007 National Money Laundering Strategy
8Counterfeit Drugs’ Path Eased by Free Trade Zones; New York Times; December 17, 2007
Let Regulatory DataCorp™ (RDC™) help.

Is she a client? A vendor? A contractor? A key employee? Is she a _legal_, _reputational_ or _financial risk to your firm_? Your job is to know before it’s too late. Our job is to help.

We are Regulatory DataCorp (RDC), the most trusted source for enhanced due diligence among the world’s leading financial institutions. RDC was founded in 2002 by 20 global financial services industry leaders. Today more than 6,600 users rely on RDC to ensure compliance with KYC, AML, FCPA and other regulations.

Why? The most comprehensive risk-related database ever assembled:
- Five million risk-relevant events
- 4,000 new records added daily
- 15,000 global sources

And the most responsive, flexible risk-related database ever assembled:
- 42 risk categories: monitor only risks relevant to your institution
- Pick up criminal or terrorist activity by group or individual
- Ongoing monitoring
- Delivery options that suit your needs and budget

_Know who you’re doing business with™_ Let RDC help.
Assessing a prospective target’s anti-money laundering (AML) compliance program is essential to today’s deals. To remain competitive in the current market, financial institutions are inevitably involved in mergers, acquisitions or the assessment of potential targets. Traditionally, the required due diligence for such activities focused on credit quality, financial statement analysis and legal risks. However, the USA PATRIOT Act introduced a new element: consideration of the effectiveness of the target’s AML compliance program.

Section 327 of the USA PATRIOT Act requires the federal banking supervisory agencies (Federal Reserve Bank, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation and Office of Thrift Supervision) to consider the effectiveness of a financial institution’s AML program before approving a merger or acquisition under the auspices of the Bank Holding Company Act or the Federal Deposit Insurance Act. If the reviewing agency determines that the target institution lacks a satisfactory AML program, regulators may delay approval — based on the institution taking corrective action — or even reject the application outright.

Needed: Specialized knowledge

In considering a transaction, the acquirer’s executive management or the board of directors should bring its AML compliance officer (AMLCO) into discussions as early
as possible, prior to the commencement of due diligence. The AMLCO's knowledge and insights about the prospective target's risk profile — perhaps new, or not previously considered information may prove beneficial. Unfortunately, many institutions often overlook the potential contribution of the AMLCO during the initial stages of the mergers and acquisitions (M&A) process, even though their perspective could offer a valuable addition to the target entity’s regulatory history.

Once a decision is made to pursue a target and a data room is established, the AMLCO should assess the capabilities of the team that will address AML compliance and their capacity to handle the additional volume of work presented by the due diligence process. Often, consulting firms are engaged to either perform the AML due diligence or to augment the AMLCO’s due diligence team. Whatever the case, it is imperative that the individuals performing the AML due diligence are appropriately skilled, experienced and, if possible, have the designation of certified anti-money laundering specialist (CAMS).

The initial stage in the due diligence process is used to obtain and assemble an inventory of documents that are made available in the data room for review by the acquiring institution. These include policies and procedures, minutes of board meetings, internal audit and regulatory examination reports and employee training programs. A sample list is provided in Table 1.

In addition, the AML due diligence team should have the opportunity to interview the target institution’s AMLCO and department heads to determine, among other things, their risk appetite, existing client base and future growth opportunities. This will give the AML due diligence team the opportunity to foresee any potential risks and to develop an action plan to manage these risks once they become part of the acquiring institution’s portfolio.

Reporting and documenting the results of the M&A due diligence review is important for the acquirer, in part, to use as potential leverage in deal pricing. The greater the identified residual risk (inherent risk less mitigating controls), the more the deal price should be adjusted downward. In some cases, high impact issues are identified that may cause a transaction to unravel — or drive an adjustment in the deal price. For example, AML due diligence might expose either the fact that the target institution accepts customers typically considered high-risk for money laundering (e.g., shell companies) or the fact that the target institution has weak “know your customer” (KYC) documentation, meaning a significant re-documentation effort would be necessary to bring this information in line with the acquiring institution’s standards. Certainly, all issues identified during due diligence should be reported, analyzed and considered.

**Compliance issues**

Once the results of the due diligence have been reported, the proposed deal must receive regulatory approval. Prior to signing off on any transaction, the supervising regulatory agency will review the acquiring institution’s due diligence around the target’s AML compliance program. The regulators will ask to see the scope, methodology and overall results of the AML due diligence review. In some cases, acquiring banks (with regulatory approval pending) have been criticized by the relevant regulatory agency for not performing sufficient AML due diligence. An acquirer that has demonstrated a weak due diligence effort can be penalized, as regulators start to question the management’s ability — and may severely scrutinize due diligence efforts related to future prospective M&A.

Evaluating the target company’s AML compliance program helps gauge the strength of the AML-related policies, procedures and surrounding internal controls designed to assist in the detection of money laundering and terrorist financing. When a transaction is finalized, the risks (e.g., operational, regulatory, compliance, reputational) of the acquired institution are transferred to the dominant institution.

A comprehensive AML due diligence review may benefit the acquiring institution in the form of cost savings resulting from re-pricing of the deal, and avoidance of possible future regulatory sanctions and potential damage to reputation. Thorough due diligence is vital to pre-merger activities. Today, for risk management and regulatory compliance reasons, the target’s AML compliance program must be integral to those efforts.

Vasilios Chrisos, CAMS, Ernst & Young, senior manager, New York, NY, USA, vasilios.chrisos@ey.com

Rick Kryzynski, Ernst & Young, senior manager, Charlotte, NC, USA, rick.kryzynski@ey.com

---

**Table 1**

Documents to review in AML-related due diligence on potential merger partners or acquisition targets

- Current compliance manual
- Current BSA/AML compliance policy manual
- Current AML-related operating procedures
- Summary of specific products and services offered by the institution and an approximate volume or level of transactions
- Most recent regulatory examination and internal audit reports related to the institution’s AML compliance program
- Information related to previously received or pending regulatory enforcement actions
- Compliance and operational organizational charts
- Minutes from the board of director’s meetings, compliance committee meetings and audit committee meetings
- Copies of AML-related reports regularly presented to senior management
- Copies of AML training materials used during the past year
- The institution’s AML risk assessment of products, services, customers and geographic locations
- List of accounts identified as high-risk and a description of enhanced due diligence measures performed
- Copies of filed suspicious activity reports (SARs)
- Documentation of any positive matches related to USA PATRIOT Act, Section 314(a) & 314(b) requests
- List of blocked or rejected transactions with individuals or entities on Office of Foreign Assets Control’s (OFAC) SDN list
- Copy of the annual report submitted to OFAC
- Inventory of technology systems within the AML compliance function, and description of source and purpose (e.g., vendor purchased, activity monitoring)
- Service level agreements with vendors specifically focusing on AML delegation and responsibilities

---

**AML CHALLENGES**
Risk and compliance experts often compare their work obligations to those of a competitive swimmer. Compliance professionals stand on the edge of a pool, looking down the lanes that define the regulations and obligations of our field. However, the situational reality is that while we work within the lanes, the pool’s waters flow beneath and over the lane lines. The water does not respect these boundaries. In these times of turbulent waters and continuous change, the overlap of regulatory requirements and the complexity of financial crimes require that we swim outside the lane lines and face our challenges with a structured holistic approach. Having well defined operational processes and workflows enables the compliance professional to successfully address challenges.

Anti-money laundering, Fact ACT and mortgage fraud

AML, Fact ACT compliance and mortgage fraud dominate the financial crimes sector and may contribute to future completion of a large percentage of Suspicious Activity Reports (SARs). These three financial crime areas intersect and need to be recognized, mitigated and resolved. Prior to identifying the commonalities in these subject areas it is important to begin with the end in mind. The goal is to construct a workflow that becomes a part of a comprehensive case management system that enables the analyst to:

- Have a single view of the alert and/or investigation
- Automated data collection from disparate transaction systems, customer systems and relevant investigation activity
- Pre-configured alert engine interfaces for alert enrichment
- Ability to link multiple alerts to investigations for processing leading to resolution
- Triage, prioritize and assign urgency to Red Flags, Events, Alerts and Exceptions

In The SAR Activity Review Trends Tips and Issues, issue 14 published October 2008 by Financial Crimes Enforcement Network (FinCEN), the SAR report cited SAR cases related to the health and insurance industries, mortgage fraud, AML and Identity Theft (Fact Act). Cases cited were:

- BSA Records Show Money Received through Mortgage-related Ponzi Scheme Supported Million Dollar Gambling Habit
- SARs Lead to Recovery of Funds Derived from Medical Fraud
- SAR Leads to Structuring Conviction for Mortgage Broker
- BSA documents Lead to Repatriation and Seizure of over $9 Million Generated by Illegal Pharmacy

Additionally, the FinCEN report featured an industry forum section that was written by John Byrne who is an AML Executive for Bank of America and chair of ACAMS board of directors. In his comments, Byrne discussed the new obligations the financial industry faces with the impending regulatory requirements of the Fact ACT. Byrne wrote “The financial industry now has the obligation to establish policies and procedures in a program designed to formally address identity theft. While most institutions were already reporting activities that were determined to evidence identity theft, the Fact Act final rules demand both a response to red flags and a process to update the program when there are changes in identity theft risk. The rules reference sources of red flags as actual incidents of identity theft,
In a recently published article, Mr. Dan Soto and Mr. David Caruso (ABA bank compliance Sept./Oct. 2008) wrote “Institutions must find ways to apply what they learn from analysis of transactions, including creating prioritization processes to insure alerts representing greater risk are resolved first, and consideration should be given to incorporating the results of alert analysis into the enterprise BSA/AML risk assessment.”

While responsibilities may vary from one financial institution to the next, the specialist role can no longer be contained in the compliance silo. However, the complexity of financial crimes, audit, fraud deduction, AML and compliance can’t be handled using a jack of all trades mindset.

The skills needed for detecting suspicious financial activity are completely different from those needed to combat money laundering, check and deposit fraud. One specialty may call for a seasoned former law enforcement officer while another may require a CPA with a background in forensic accounting. The follow-up investigation also must be handled by the appropriate specialist. The level of investigator experience, domain expertise and alert urgency must all be taken into consideration.

From a holistic view what is needed is an organizational culture that encourages cooperation, communication and coordination. Every financial institution employee must recognize the role they play in the overall risk-mitigation culture. The financial institution should consider deployment of technology tools that empowers employees to not only complete their risk mitigation and compliance work with a degree of competency but to maximize the utilization of their time and subject-matter expertise by automating processes and reusing information to increase efficiency and productivity while simultaneously applying/updating best practices within the boundaries of regulations and service level agreements.

**Meeting the challenges**

In conclusion, financial institutions are challenged with fighting fraud and financial crimes in an environment of enhanced regulatory scrutiny. The expansion of risk associated with Fact ACT compliance, mortgage fraud, global sanctions issues and AML/terrorist activity in an environment of international financial instability presents never ending change for organizational employees tasked with mitigating these risk issues.

Financial Institutions need to determine how they will effectively manage the challenges resulting from change. A major consideration is the use of technology solutions and human assets in a manner that involves an automated work flow process to address:

- Managing high volumes of alerts from disparate alerting engines
- Reducing the high cost and risk of manual processing
- Creating an auditable trail of tasks performed to increase efficiency of investigations and look back projects
- The frequent changes associated with regulatory requirements, market fluctuation, challenges associated with financial institution mergers, work force reduction and consolidation.

Swimming outside the ropes can be a risky path to take while navigating the distance from one end of the pool to the other. In these times of constant change, the risk officer that can adapt to lane changes and water turbulence will not only survive but succeed. The same can also be said for financial institutions. Institutions that rely solely on past practices, processes and work flows that may have provided stability in past business environments may not be able to adapt to changing conditions.

In comparison, agile financial institutions that embrace change and deploy game changing technology tools will find that present and future challenges can be met by establishing new business rules, shifting the operational paradigm and empowering their employees.

Robert A. Goldfinger, CAMS, CFS (retired) Cmdr. CID, director of fraud/AML Market PEGASYSTEMS INC., Cambridge, MA, USA, rob.goldfinger@pega.com

Charles Thiel, CIA CFE CFS, vice president fraud/AML markets, PEGASYSTEMS INC., Cambridge, MA, USA, Charles.thiel@pega.com
The Federal Deposit Insurance Corporation (FDIC), states that insider fraud has accounted for over one half of all bank fraud and embezzlement cases closed by the FBI during the past several years. FDIC also states that insiders are in a position of trust and can abuse that trust for their own personal benefit. Insider abuses include failure to disclose their interests that borrow from the institution or otherwise have business dealings with the institution; diverting assets and income for their own use; misuse of position by approving questionable transactions for relatives, friends and/or business associates; abuse of expense accounts; acceptance of bribes and gratuities; and other questionable dealings related to their positions at the institution. Insider abuse undermines confidence in institutions and often leads to failure.

Fraud is pervasive in America. The 2008 Report to the Nation issued by the Association of Certified Fraud Examiners (ACFE) established that U.S. organizations face occupational fraud and abuse. It affects organizations of all types, sizes, locations, and industries. The ACFE study was composed of a sample that included 40% privately owned companies and 18% public companies. According to the report, organizations lose an estimated seven percent of annual revenues to fraud. This calculates to a staggering estimate of losses around $994 billion among organizations based on the projected U.S. Gross Domestic
Product for 2008, despite emphasis on anti-fraud controls and recent legislation to combat fraud.¹

FBI investigations proved that financial institutions could fall victim. Its 2005 Financial Institutions Fraud reported that out of the 1,497 subjects convicted during that year, 220 were bank employees and 92 were bank officers, which accounts for 21% or the total.²

**Background of embezzlement and white-collar crime**

Embezzlement occurs when someone is so trusted with property fraudulently converts it — that is, keeps it for his or her own or the use of others.

Edwin Sutherland — authority in criminological history — defined white-collar crime as a crime committed by a person of respectability and high social status in the course of his occupation. Today that concept has been reevaluated to include crimes of middleclass and corporate employees who use the marketplace for their criminal activity.³ A prime example would be a banker who embezzles money.

The characteristics of a skilled criminal, such as the professional thief, include highly developed, career behavior patterns characterized by nonviolence that targets loosely organized corporations rather than individuals.

**Former bank vice-president’s journey to justice and death**

In February 2008 a former bank vice president was indicted for embezzling $559,040 and laundering stolen funds.⁴

The initial charges against Steven Francis Sueppel included one count of embezzlement of bank funds and six counts of money laundering for which he pleaded not guilty. He was released on a $250,000 bail bond because he did not have a prior criminal record and was not considered a flight risk.

Sueppel realized that if he were found guilty of embezzlement, he could face up to 30 years in prison, a $1 million fine and five years of supervised release. In addition, for each count of money laundering, he would be sentenced to 20 years in prison, fined up to $500,000 or double the amount allegedly stolen, plus three years of supervised release.

Authorities believe that Sueppel’s bleak future drove him to kill his wife and their four adopted children and later he killed himself by crashing the family minivan. According to the Iowa City Press-Citizen, autopsies March 23, revealed that Sueppel’s wife, Sheryl, died of blunt force trauma and their four children — Ethan, 10, Seth, 7, Mira, 5, and Eleanor, 3 — died of blunt force trauma or asphyxiation. Police said they found evidence Sueppel tried both.⁵

**Fraudsters within financial institutions**

When an employee drastically changes his or her behavior, co-workers and management should closely scrutinize this individual.

Common red flags of fraud:

- Living beyond the employee’s means.
- Memberships to country clubs, driving expensive cars, wearing brand-name clothes, especially when not justified by a high compensation package or an inheritance, for instance.
- Working unusual hours and being reluctant to take sick leave or vacation. Forcing the suspected employee to take vacation or time off and having another employee take over the position, in many cases, has uncovered instances of fraud.
- Earning management and peers’ trust by being charming and mindful. Attitudes of friendliness and generosity are appealing to everyone. It can be characterized as charisma.
- Bragging about assets such as properties, investments and leisure activities. A fraudster’s ego is a conduit that leads to self-confidence and assurance that his or her actions will go undetected. Investigators have successfully enticed these criminals when interviewing them to eventually obtain a confession. For example, a bank teller supervisor embezzled more than a $1,000,000 by making 1,050 transactions of $10,000 each. These transactions were covered up by creating false debit and credit transactions purporting to reflect cash shipments to a branch of the Federal Reserve. When confronted by FBI investigators, this supervisor confessed that the stolen money was used for living expenses, vacations and tuition for her children.

Non-existent internal controls or lack of monitoring existing internal controls is the easiest way to encourage fraud. Financial institutions can prevent and deter fraud by implementing effective internal controls, training employees and making them aware that there will be prosecution if security or trust is breached. Also, proper segregation of duties is paramount. The likelihood of wrongdoing increases when employees are in a position that allows them both to commit fraud and to conceal it.

A thorough hiring process that includes extensive background checks, verification of professional credentials, and references serves as a useful deterrent to fraud. Many fraudsters have gone from institution to institution committing crimes. Courts records prove that repeat criminals exist. Institutions should conduct follow-up background checks at least every two years; otherwise, financial institutions should implement an alternate means of determining whether an employee has been convicted of an offense.

**FDIC Insider Transactions Warning Signs**

The FDIC has an extensive list of warning signs. Some of them are:

1. Insider lending personal funds to customers or borrowing from customers.
2. Insider involvement in silent trusts or partnerships and/or shell corporations.
3. Insider appears to receive special favors from institution customers or shows unusual favoritism toward certain institution customers.
4. Insider purchases assets from the institution, directly or indirectly, and there is no evidence of independent appraisal of the assets.
5. Insider has apparent reciprocal lending arrangements with insiders of other institutions and his/her institution has correspondent relationships with those institutions.
6. Insider is involved in a business that arranges its financing through the institution.
7. Insider “perks” include use of expensive institution owned automobiles, boats, airplanes, housing, etc., where

¹ACFE – Report to the Nation 2008
³Siegell, Larry -Criminology, Theories, Patterns, and Typologies – Eighth Ed. Thomson
⁵http://www.westbranchtimes.com/article.php?id=2834
⁶http://www.fdic.gov/regulations/safety/manual/section9-1.html#part1
⁷http://definitions.uslegal.com
When an employee drastically changes his or her behavior, co-workers and management should closely scrutinize this individual.

the institution's earnings do not appear to support such extravagance.

8. Insider heavily indebted and debt service appears to require most, if not all, of the insider’s salary.

9. Insider financial statements show large or unusual fluctuations. Net worth cannot be reconciled from disclosed sources of income.

10. Insider is financing large purchases (home, auto, etc.) through private, nonbanking sources that may have a business relationship with the institution.

11. Insider financial statement reflects heavy concentration of high-risk investments and speculative ventures.

12. Insider sells personal assets to third party and the institution provides financing without benefit of an independent appraisal.

13. Insiders or their interests frequently appear on transaction suspense item listings or on computer generated past due loan lists, but do not appear on the “updated” version presented to the board of directors or to examiners.

14. Insider “unofficially” guarantees loans and/or loan participations.

15. Insider is responsible for clearing up audit exceptions on loan balance confirmations.

The FDIC suggested action is to review all insider transactions to see if they comply with policy and applicable state and federal regulations. Follow up on any exceptions. Any nonconforming transactions should be discussed with the institution’s board of directors. Apparent fraudulent activities should be referred to the proper authorities.

**Link between fraud and money laundering**

Usually fraud culminates in money laundering since the individual has to make his or her ill-gotten proceeds seem legitimate, or “clean.”

Fraud in the legal sense is defined as an intentional misrepresentation of material existing fact made by one person to another with knowledge of its falsity and for the purpose of inducing the other person to act, and upon which the other person relies with resulting injury or damage. Fraud may also be made by an omission or purposeful failure to state material facts, which nondisclosure makes other statements misleading. The false statement or omission must be material — meaning that it was significant to the decision to be made.

Another part of this link is mail fraud. Mail fraud and wire fraud are closely connected to money laundering. Usually fraudsters are concurrently convicted of mail fraud, money laundering and wire fraud. U.S. law states that mail fraud is committed when the United States Postal Service is used in carrying out a scheme to defraud. In order to be proven guilty of mail fraud, it must be shown that the person knowingly and willfully devised a scheme to defraud, or obtained money or property by means of false pretenses, representations or promises and that such act were carried out by means of use of the U.S. Postal Service. Obtaining a payment in response to a fraudulent offer or making a fraudulent offer through the mail is sufficient to claim an offense of mail fraud. To be convicted of mail fraud, it must be proven that the defendant (fraudster) used the mail or private carrier to facilitate a scheme that attempts to defraud others.

The wire fraud statute prohibits the transmittal of any information by wire, radio, or television in interstate or foreign commerce with the intent to defraud. The Federal statute prohibiting bank fraud makes it a crime to knowingly execute or attempt to execute a scheme to defraud a financial institution or to obtain funds by false pretenses under the control or custody of a financial institution.

**International case**

Beyond America’s borders, fraudsters wreak havoc on foreign institutions. In March 2005, Israeli police announced that they detained customers and staff of Bank Hapoalim Branch No. 353 and of the Bank Hapoalim Trust Company for questioning. The detentions mark the next stage of an undercover investigation pursued by the police over a period of about a year, during which evidence was accumulated apparently indicating that offences have been committed against the Prohibition on Money Laundering Law by some of the customers, staff and managers of the branch and the Trust Company.

Regarding this case, The New York Times reported that in one of the largest money-laundering inquiries in Israel in recent years, authoritiesthere froze $376 million in assets at Bank Hapoalim, the country’s largest bank, and questioned clients as far away as Russland and France. Israeli police detained nearly two-dozen low-level employees at one Hapoalim branch in Tel Aviv.

**Conclusion**

Fraud does happen. Fraud is linked to money laundering and financial institutions victimized by inside fraudsters end up having launderers on their payroll. Circumventing weak controls is easily achieved. Employees can exploit weaknesses, thus taking a toll on a financial institution’s earnings and ultimately undermining their reputation. It is imperative to have strong internal controls in place, train employees by providing bank employees with the tools they need to prevent and detect fraud. The CPA Journal Online suggests a good approach. It states that education and training are needed to supplement corporate communications and create awareness at all levels of the organization. The board, senior leadership, and financial personnel may need more extensive training in the inner workings of the programs and ethical issues, as well as a broader and deeper perspective on how and where fraud occurs. Routinely monitoring of controls is a must. Do not allow lax controls to nurture a potential fraudster in your institution.

**Consuelo Herrera, CAMS, CFE accountant at Forensic Technology Inc., Largo, Florida, USA, Consuelo.herrera@contactft.com**
Pirates have become a newsworthy subject these days. While the title of this article may sound like a possible sequel to the movie, *Pirates of the Caribbean*, its subject-matter consists of something more sinister—the increasingly dangerous and growing threat of piracy and maritime terrorism off the coast of Somalia. The pirates of Somalia are not Johnny Depp types sailing around with fake swords and dreadlocks. Instead, they are a brazen and ruthless lot; the sheer scale of their criminal activities has turned East African waters into the most dangerous in the world. The pirates use sophisticated equipment, speedboats and weapons to hijack ships often demanding huge ransoms from which they have reportedly made millions of dollars. Such huge sums of illicit funds inevitably have to be laundered, which raises the question of whether a plausible effort to fight money laundering in Somalia is even possible.

**Piracy and ransom demands**

On November 17, 2008, the New York Times reported that a Saudi-owned supertanker carrying more than $100 million worth of crude oil had been seized by pirates off the coast of Kenya. The 1,080-foot ship has become the largest vessel seized to date. In three days, the pirates had demanded a $25 million ransom payable in 10 days. In September 2008, the pirates had seized a Ukrainian tanker. Due to the vast area of the affected waters, it is impossible to effectively prevent piracy. Most ships are manned by a small and, often unarmed staff, leaving the tankers even more vulnerable to the pirates. The New York Times explains the problem:

“The piracy industry started about 10 to 15 years ago, Somali officials said, as a response to illegal fishing. Somalia’s central government imploded in 1991, casting the country into chaos. With no patrols along the shoreline, Somalia’s tuna-rich waters were soon plundered by commercial fishing fleets from around the world. Somali fishermen armed themselves and turned into vigilantes by confronting illegal fishing boats and demanding that they pay a tax.”

For their troubles the pirates acquire millions of dollars which they use to live the high life in Somalia. The question is why is it difficult to trace this money and prevent its laundering?

**Somalia’s failed government = No money trail**

Somalia’s central government collapsed in 1991 and this left the country wallowing in a sea of lawlessness. The country has no formal banking system and therefore no regulation of financial transactions. Against this background, it is often impossible to trace the ransom money derived from piracy. It has been said that piracy will not be resolved until political stability has been established in Somalia. Such stability would inevitably be accompanied by economic development which would discourage the population from turning to piracy for a living. Stability would also put in place the institutions necessary to curb crime and money laundering. There are other countries in that region of Africa that have stable governments and are actively involved in preventing money laundering in their countries.

**Anti-money laundering efforts in eastern and southern Africa**

Somalia’s neighbor, Kenya, is part of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) whose 14-country membership is dedicated to fighting money laundering in the region. Consequent to the Somali pirates’ latest escapade, Kenya’s foreign minister, Moses Wetangula, announced Kenya’s willingness to convene a conference to discuss ways of fighting piracy. Such a conference would be opportune particularly in light of recent security reports that the gaps in Kenya’s anti-money laundering make the country vulnerable to money laundering activities by, inter alia, the pirates.

The Somali pirates greatly rely on the hawala system of money transmission; therefore, there is a need for countries such as Kenya, Tanzania, Zambia and other members of ESAAMLG to monitor the use of hawala in order to trace money derived from piracy. In its 2004-2005 *Money Laundering and Terrorist Financing Typologies Report*, the Financial Action Task Force described an alternative money transfer system, like hawala, as a “financial service that accepts cash, cheques and other monetary instruments or other stores of value in one location and pays a corresponding sum in cash or other form to a beneficiary in another location by means of a communication, message or transfer or through a clearing network to which money/value transfer system belongs.” Such a system makes it possible for vast sums of money to be transmitted globally with little or no documentation at all. According to writers, Patrick Mayoyo and Lukas Barasa: “Investigators say this system of money transfer (hawala) not only abets piracy but also hampers investigations by countries tracking proceeds from drug-trafficking, arms-smuggling and terrorism activities” and piracy. Such difficulties could be overcome through a rigorous and effective anti-money laundering regime in the region.

**Money remittances**

There is no doubt that money remittances are a major aspect of Somali life;
remittances are a source of income for the majority of Somali people. However, Somalia’s money remittances have been known to be vulnerable to money laundering and terrorism financing. On September 23, 2001, the United States issued Executive Order 13224 which, among other things, authorized aggressive actions against the bankers of international terrorism. In particular, the order shut down Somalia’s largest money remittance company, Al Barakaat, on the grounds that the company raised “money for terror, invest it for profit, launder the proceeds of crime, and distribute terrorist money around the world to purchase the tools of global terrorism”. The 9/11 Commission went to great lengths to distinguish money remittances from hawala: “The key difference is in how the money or value moves between the office obtaining the money from the customer and the office paying the money out to the ultimate beneficiary. In transferring value between the sending and receiving offices, a money transmitter uses the formal financial system typically relying on wire transfers or a correspondent banking relationship. A hawala …does not use a negotiable instrument or other commonly recognized method for the exchange of money”. The report also notes that “Usama Bin Ladin and al Qaeda made significant use of hawalas to move money in the Middle East” prior to 9/11. Due to the blatant lack of formal institutions in Somalia, it is easier for money to be transmitted through the more informal hawala system; hawala is not inherently criminal but it provides for a conducive environment for criminal activity. Consequently, criminals, such as pirates, take advantage of the minimal identification requirements under hawala for easier transmission of funds and utilize the hawala system as a way to launder their funds or, possibly, finance terrorism.

Conclusion

The dangers of piracy and hawala are not lost on ESAAMLG member countries that recognize their own vulnerability to money laundering, especially in view of the fact that they are largely cash-based economies. These countries are making efforts to establish comprehensive AML laws and financial intelligence units that are equipped to investigate and trace money derived from illegal activities such as piracy. With such efforts in mind, it is hoped that an environment exists to continue fighting piracy and, consequently, money laundering and terrorism financing in East Africa. A successful battle against Somali pirates means the country must strengthen its own government and regulatory institutions.

Milimo Moyo, Zambian lawyer, New York, NY, USA, milimomoyo@gmail.com

The views in this article do not represent those of any organization.

www.ACAMS.org
Italy: Seeing the threat behind the corruption
In the context of anti-money laundering (AML), the Italian scenario is influenced by a series of typically Italian characteristics which distinguishes the country apart from other advanced European economies. Italy is a member of the EU and part of G8 and can appear to outsiders to be a country that is full of contradictions where decisions often appear difficult to decode.

A strong element in Italy is the existence of ‘family capitalism’ — small- and middle-sized family-owned companies which are subject to rapid transformations. As the real drivers of the Italian economy, they are deeply rooted locally and share close relations with foreign relatives in Latin America, Eastern Europe and the Mediterranean.

High levels of corruption also play a large factor in the Italian scenario. Corruption also is coupled with the presence of sophisticated organized crime groups that emerged as a cause and effect of an enormous gap between the poor regions of the south and the prosperous northern and central Italy. The economic disparity has continued to exist regardless of decades of public funding in the south to reduce these inequalities.

A subculture of illegality

Italy is well-known for its extremely high fiscal evasion rate, and its proportion of cash payments is one of the highest in Europe. The widespread diffusion of corruption, which originates from an existing interrelation between political and business milieus, has never been countervailed — but rather further promoted — by the Italian governments, which succeeded one after another following the Second World War. The interests and the balance of powers of the financial and the business worlds have often not just been mediated but actually managed by politicians. Finance and business are susceptible to sudden changes and even reflect the whims of political interests. The borders between licit and illicit have become “more flexible” than in other West-European countries. Progressively, corruption has pervaded all levels of Italian society with particular concentration in the South — a situation favored by the presence of criminal organizations and the above mentioned existence of the socio-economic gap among the south, the center and northern Italy.

The Clean Hands inquiry

The investigation of corruption escalated in the early 1990s. The famous national inquiry known as Clean Hands, that was launched to investigate a series of major scandals, revealed the existence of a corruption system, based on agreements which ensured a constant flow of bribes to political parties from companies providing services to the public administration. The inquiry led to confessions and convictions of major representatives of the Italian entrepreneurial and political world, and resulted in the largest political crisis since the Second World War. In the investigation’s wake, two major Italian political parties — the Italian Socialist Party (PSI) and the Christian Democratic Party (DC) — collapsed after it emerged that large sectors of business and politics survived through illicit activities. The corruption involved not just politicians and entrepreneurs, but magistrates and high-ranking military officers.

Corruption today

The Clean Hands inquiry weakened corruption, which became less visible, but it did not defeat the corruptive system. To the contrary, according to Achille Serra, former High Commissioner against corruption in Italy, the corruption system was damaged by the judicial inquiries of the 1990s. However soon after, Italy adopted an “evolution of the species” approach and more efficient, sophisticated and less visible corruption techniques were invented — de facto the corruption level increased.

Over the last fifteen years, the Italian government has ratified a series of international conventions against corruption but failed to adopt special legislation and the necessary reforms to contain illegality in an efficient way.

The corruption perception index published by Transparency International in June 2008 evaluated the abuse of public office for private gain. Italy’s ranking this year worsened by fourteen positions compared to 2007’s index, reaching 55, after countries such as South Korea and Costa Rica. Out of the first fifteen members of the EU (before the enlargement of the EU to nine eastern European countries, which started in 2004) Italy is positioned in second to last place in Europe.

The response of the Italian government to this situation seems contrary to Transparency International’s indicators on 25 June 2008, through a decree, the Italian government abolished the agency named High Commissioner against Corruption, which had become fully operative in September 2007.

In the confines of corruption via fiscal evasion, the statistics of public and private businesses show impressive numbers. In January 2007 it was estimated that fiscal evasion equaled approximately 19% of the GDP.

Corruption and fiscal evasion are strictly related. These two elements, combined with a high level of cash payment provide a fertile environment for money laundering.

Italy is well-known for its extremely high fiscal evasion rate, and its proportion of cash payments is one of the highest in Europe.

Organized crime

The most significant and worrying element characterizing money laundering in Italy is the pervasive presence of organized crime groups. Unlike any other developed European country, the local economies of some of the southern regions and in particular those of Campania, Calabria and Sicily are nearly entirely controlled by criminal organizations such as the mafia, the “ndrangheta” and the “camorra.” They tend to rely on the alliance of corrupt local politicians, who want to keep their positions and are interested in maintaining the support of criminal organizations, which are largely funded by an unlawful use of the public money.

In these regions, the control of the organized crime economy is the biggest risk factor. This affects not just the south, but the central and northern Italy, as a good
The Italian legislative AML framework is the result of a twenty-year engagement of the Italian authorities in the fight against organized crime.

In 1993, the Bank of Italy issued a Decalogo, a document containing operational instructions aimed at identifying suspicious operations, in order to strengthen the control over the use of intermediaries for money laundering purposes. The document was updated in 2001, in consideration of the development of new money laundering techniques in the areas most at risk of money laundering.

In 1997, Italy assigned the primary responsibility for matters related to anti-money laundering to the AML Department of the Italian Foreign Exchange Office (Ufficio Italiano Cambi – UIC) which acted in conjunction with the Financial Police and the Bureau of Anti-Mafia (DIA). In 2000, in line with the European directives, a national FIU was created within the UIC.

The Italian legislative framework became increasingly sophisticated and far reaching the point that Italy sometimes anticipated the principal indications of international organizations.

In 1991, one month before the adoption of the 1st European AML directive, Italy passed an AML law under which banks were obliged to identify their customer and record any transaction exceeding ITL 20 million (equaling today’s 10,000 Euros), increased to 12,500 in 2002, which is lower than the thresholds set in the first and the second European AML directives (15,000 Euros). In addition, investment firms and management companies were also subject to the AML regime (thus anticipating the 2nd AML directive).

In 1991, the Bank of Italy issued a Decalogo, a document containing operational instructions aimed at identifying suspicious operations, in order to strengthen the control over the use of intermediaries for money laundering purposes. The document was updated in 2001, in consideration of the development of new money laundering techniques in the areas most at risk of money laundering.

In 1997, Italy assigned the primary responsibility for matters related to anti-money laundering to the AML Department of the Italian Foreign Exchange Office (Ufficio Italiano Cambi – UIC) which acted in conjunction with the Financial Police and the Bureau of Anti-Mafia (DIA). In 2000, in line with the European directives, a national FIU was created within the UIC.

The Italian legislative framework was then progressively updated to mirror international standards and the European AML directives. In 2002 Italy implemented the December 2001 Second European AML directive, which extended the risk of recycling from financial institutions to professional and commercial operators.

In 2005, Financial Action Task Force’s (FATF’s) inspectors determined that Italy’s AML framework is extensive and mature, and that the country highly complied with most of FATF’s forty plus nine recommendation. The law enforcement efforts against money laundering led to convictions in almost 600 cases every year, one of the highest rates of successful prosecutions in Europe and more than and over 130 million euro worth of criminal proceeds were confiscated in 2004.

However, the FATF also assessed that it was necessary to clarify and reorder relevant laws, to implement a more detailed risk-based Customer Due Diligence (CDD) requirements and other new provisions of the revised FATF standard and of the Second European Directive on Money Laundering in particular with reference to non financial businesses and professions.

In addition, Italy was asked to consolidate the AML legal framework in one single text to reduce its complexity and increase its efficiency.

The Third European Directive

On 21 November 2007, Italy implemented the Third European AML directive (2005/60 EC) regarding the prevention of the use of the financial system for the purpose of money laundering and terrorist financing which EU member states were required to implement by December 2007.

The new AML law brought several changes to the Italian legislative AML framework of which the most significant are the following:

- The UIC ceased to exist on January 1, 2008 and its functions were transferred on the Bank of Italy where a new Financial Information Unit (FIU) was constituted.
- The modification of the existing law, which improved the coordination between the authorities and the AML law.
- The national legislative framework on the fight against terrorism made the obligation to signal suspicious operations more explicit.
- The introductions of so called “risk-based approach” to assess levels of money laundering and financing of terrorism.
- Obligations were extended in the customer identification and CDD and the obligation to identify the beneficial owners was introduced.
- Obligations to apply enhanced due diligence to Politically Exposed Persons (national PEPs excluded) were introduced.
- The adoption of a broader definition of money laundering than the one of the Italian criminal code (articles 648 and 684).
- To combat high cash transactions rates, the maximum sum for cash payment has been set at 5,000 Euro. However, on 25 June 2008 the new Italian government increased the threshold to 12,500 euro (law nr. 112).
- Stricter rules regarding money transfers...
were introduced: it has been limited to 2.000 euro without documentation and to 5.000 Euro if documentation to attest the operation is presented.

What are the effects of the implementation of the European AML directives?
The Italian AML framework was improved significantly thanks to the implementation of the Second and Third European AML directives. However, some experts stressed that a closer coordination with other specific legislations would be required and that adjustments would be needed on the enforcement side.

The obligation to adopt a risk-based approach and to abstain from conducting certain operations autonomously and not just upon request of the authorities should discourage fiscal offenses and, in particular, fiscal evasion which is a significant problem in Italy.

The extension of control and suspicious transactions reporting (STRs) obligations to professionals and other financial and non financial intermediaries should further speed up this process.

The data shows an increasing trend in the number of STRs filed. In 2007 the UIC received 12.503 STRs, 21% more than in 2006, the majority of which appeared to be related to fiscal evasion, followed by frauds, “layering” operations of organized crime groups as well as illegal waste dismantling. Nevertheless, the number of STRs is relatively still low.

Although the situation seems to be promising and financial institutions increasingly give attention to AML, there persists a noticeable gap in the number of STRs, both across the categories of those reporting and the geographic areas. In particular, it has emerged that the numbers of STRs filed by non-financial operators and professionals is extremely low (only 1.4%). This shows a difficulty by these subjects to adopt the new legislation.

The impression is that professionals such as notaries, lawyers and accountants continue to feel close to the interests of their clients and are not always willing to strictly adhere to the norms of compliance with AML regulations.

The inspections of money services businesses by Italian authorities have nearly doubled in 2007 compared to 2006. An operation conducted by the Italian authorities known as “Easy money” uncovered more than 400 unauthorized money services businesses, as well as traces of persons listed on UN blacklists.

The Italian AML framework was improved significantly thanks to the implementation of the Second and Third European AML directives.

What are the difficulties of compliance with the European AML directives?
Unlike the Anglo-Saxon countries, the praxis of costumer verification and knowledge has not been adopted by the Italian financial and business worlds.

Historically, Italian financial institutions have always made use of in-house techniques to verify their customers. This verification, however, has been limited to evaluating the risks of financial insolencies. Customer verification activities were conducted by the “Centrale dei Rischi” of the Bank of Italy in the form of monitoring the customers’ financial situation on a national level. It also was handled by a series of service providers, controlled by banks, that evaluated the possibilities of insolvency through a “black list” of “bad” creditors.

While these techniques were efficient to identify and monitor potential risks of financial insolencies, they are less appropriate for adequate compliance with the strict Know Your Costumer requirements of the current AML legislation. To comply with the current AML legislation, these hindrances must be overcome:

• Lack of customary conducting CDD activities both on national and international level by the Italian bankers and financiers.
• Wrong and/or exaggerated perception of confidentiality level between customer and managers of financial institutions who fear to invade the privacy of their clients and to lose the fiduciary relationship with them.
• Collusion between banks and clients at limits of legality in regions of the South of Italy and in some provinces of Central and Northern Italy. (Even more this collusion is spread between professionals and their clients, which explains the low number of STRs, as mentioned earlier).
• Lack of transparency in the public administration, especially in Southern Italy; many public bodies do not collaborate sufficiently in the supply of information required for tackling problems related to corruption and money laundering, either for lack of efficiency or, in some cases, for reasons of collusion with the “grey zone” of the local entrepreneurial world.
• In some cases, the strict legal framework in relation to privacy does not enable independent parties to obtain a sufficient level of knowledge on individuals most at risk (politically exposed persons and others). For example, criminal records and information on civil or criminal litigation is not public (unless it has been published by the press).

Italy, with a history of corruption and fraud, has made strides to combat money laundering and other forms of corruption; however, it still has a long way to go. Recently an immunity bill has been introduced in the Italian legislation to protect those holding the highest positions of public office from prosecution, a controversial proposal, considering that the Prime Minister was facing trial on corruption, which was suspended in October 2008 as a result of the immunity bill.

Nicoletta Grilli, managing director, Corporate Risk Watch Srl, Milan, Italy, n.grilli@corporateriskwatch.com
Historically, many Latin American countries have been susceptible to economic and political forces on their path to globalization. Several countries maintain well-diversified economies supported by increased financial independence and fiscal discipline. However, certain countries remain exposed to increased fluctuations in the global markets because of credit demands, political instability, and a reliance on commodities. Citizens in the region remain cautious about a country’s ability to control inflation, which results in the reduced purchasing power of local currencies, and concerns of social unrest.

As a result, many citizens of Latin American countries often seek to protect their wealth from local economic, political and social factors by converting it to the more stable banking systems in Europe and the United States (U.S.). To avoid a flight of capital, certain Latin American governments restrict the outflow of funds from their financial systems by imposing numerous barriers on currency exchange policies. One such country is Venezuela.

**Currency exchange in Venezuela**

Venezuela maintains a complex currency exchange system. Recently, certain events undertaken by the Venezuelan government have increased the usual pattern to convert local currency, the Bolívar Fuerte (Bs.F), to the stronger Euro and USD. Venezuela lacks a free market for currency exchange and transactions conducted outside legal channels could lead to criminal sanctions by the local authorities. For instance, engaging in black market currency exchange activity is a felony. Currently, according to Venezuelan law, only three legal ways exist to conduct currency exchange: bonds denominated in USD purchased with Bs.F, the CADIVI system, and the *permuta*.

1. **Bonds denominated in USD and purchased with Bs.F**

   Periodically, the Venezuelan government issues bonds denominated in USD. Individuals and corporations can purchase the USD denominated bonds with Bs.F at a fixed rate established by the government from registered Venezuelan broker-dealers. Subsequent to the initial sale by the government, the bonds can only be transacted in USD in the global markets.

2. **CADIVI**

   Comisión de Administración de Divisas or CADIVI is a government entity managed by the Venezuelan Finance Ministry with authority to regulate and impose restrictions on foreign currency exchange rates and the procedures used to obtain foreign currencies. CADIVI has the authority to sell USD to individuals and corporations for limited use purposes that include, among others, the purchase of products or imports for certain industries, personal trips up to $5,000 per year, medical reasons, and graduate studies conducted abroad.

   USD sold by CADIVI have a preferential exchange rate of 2.15 Bs.F for $1 USD. The CADIVI maintain tight control of the outflow of USD from Venezuela’s Central Bank. As such, the certification process to exchange Bs.F to USD is strict and requires an exhausting amount of documentary support, including licenses, permits, invoices and receipts. As a result, it takes several months to complete the CADIVI process to obtain USD.

3. **Permuta**

   The most common legal channel established to convert Bs.F into USD is by engaging in a “bond swap” or *permuta*, whereby bonds denominated in one currency are exchanged for bonds denominated in another currency. After the exchange is completed, the purchaser obtains USD from the sale of the bond.

   Unlike the CADIVI preferential rate, the exchange rate for the *permuta* fluctuates because it is subject to supply and demand market factors. This can increase the exchange rate exponentially, sometimes as much as two times the preferential rate.

   Venezuelan corporations are not required to obtain a government issued license to conduct *permuta* transactions. Legally, the *permuta* requires an offshore company to conduct the bond swap and a third party to provide the bonds in different currencies. However, broker-dealers are essential because they provide the bonds for the exchange. Typically, most
individuals and corporations do not possess the bonds to proceed with the transaction. As such, the *permuta* process is formally conducted through Casas de Bolsa and Sociedades de Corretaje, which are commonly known as broker-dealers. Casas de Bolsa and Sociedades de Corretaje are similar in nature, but have different authorities. A Casa de Bolsa is permitted to broker securities on the Caracas Stock Exchange and underwrite securities. A Sociedad de Corretaje is limited to securities brokerage.

To conduct the *permuta*, an individual or corporation must be a registered client of the broker-dealer. According to local bank laws, the broker-dealer is required to maintain a client profile and Know Your Customer documentation of its client. However, broker-dealers are not permitted to accept direct deposits. If the client lacks sufficient funds in the account to fund a *permuta* transaction, then a deposit must be made at a local bank where the broker-dealer maintains an account. Finally, the broker-dealers’ role in the *permuta* transaction is limited to the purchase and sale of the Bs.F denominated bond.

The following describes a *permuta* transaction:

**Purchase of bond**

The broker-dealer (Corp. A) purchases a Bs.F denominated bond, normally a fixed income security issued by the government, on behalf of its registered client (Client A). As a result, Client A holds a Bs.F bond.

**Sale of Bs.F Denominated bond**

Next, an offshore company (Corp. B), which acts as the exchanger in the sale, enters the transaction to perform the *permuta* with Client A. In addition, a second offshore company (Corp. C), representing its client (Client C) that wants to sell a USD denominated bond, is used to complete the transaction.

**Bond Swap**

Corp. B receives a Bs.F bond from the client A and simultaneously transfers the Bs.F bond to Corp. C. In return, Corp. B transfers a USD bond from Corp. C to Client A.

Upon completion of the swap by Corp. B, each client obtained a bond denominated in their desired currency: Client A has a USD bond and Corp. C has a Bs.F bond.

**Sale of USD denominated bond**

In the final step, Corp. C purchases the USD bond from the Client A at a pre-negotiated price established by both parties. As a result, Corp. C wire transfers the USD to the client’s U.S. bank account and Corp. C retains the USD bond for future transactions. At this point, with USD in hand, Client A will most likely take advantage of various bank deposit and investment products in the U.S. financial system.

**Offshore company and the Permuta**

The offshore company is a critical element in the *permuta* transaction because it can buy and sell bonds denominated in any currency, including USD and Bs.F. It may be affiliated or owned by the broker-dealer, but the two are intentionally structured to be difficult to link together. Moreover, the broker-dealer usually owns the second offshore company in the transaction. This form of ownership benefits the broker-dealers’ client because it eliminates the transparency of the currency exchange performed by the offshore company. Conducting transactions in this manner represents attempts to protect the confidentiality of clients, their assets, accounts held abroad and provide tax related benefits. On the other hand, the broker-dealer benefits from this structure because it selects the offshore company and may assign profits derived from the *permuta* transactions to the company located in the most favorable tax jurisdiction.

From the perspective of the U.S. financial institution, the offshore company is most likely established in a high-risk offshore financial center with strict secrecy laws. Common offshore locations include Antigua and Barbuda, Bahamas, Barbados, British Virgin Islands, Cayman Islands and Netherlands Antilles. As such, verifying the true ownership of the offshore company is near impossible, which creates an inherent risk with the transaction because the true source of the funds is unknown and the ability to trace the funds back to the true owner extremely difficult. Historically, funds associated with offshore companies have been linked to the proceeds of criminal activities including organized crime, drug trafficking, political corruption and tax evasion.

**Black Market**

The Venezuelan government has authorized the *permuta* for currency exchange transactions within a parallel market. However, as with any government with a fixed exchange rate, a black market for currency exchange activity is available that circumvents the legal methods and compliance controls. The black market for currency exchange is a faster and less complex process. The exchange can be executed without a broker-dealer; the separate transactions may take place simultaneously in different countries and in

The Venezuelan government has authorized the *permuta* for currency exchange transactions within a parallel market.
Transactions with offshore companies and domestic shell companies must be continuously monitored and scrutinized

Secondary currency exchange in the U.S.

A client with funds in a U.S. bank account may continue to perpetuate the more favorable currency exchange rate for his/her own self benefit. A market in the U.S. exists for Venezuelan nationals that seek USD and those that may not have access or the desire to participate in the permuta. As a result, upon receipt of a large wire transfer from an offshore company that participated in the permuta, the client will disperse funds in smaller denominations via check or wire transfer that benefit unrelated individuals and companies. This method increases the likelihood that the client may be acting as an unlicensed money transmitter and falling under the purview of U.S. Money Services Business registration laws.

U.S. shell companies

An agent in the U.S. registers numerous privately held shell companies with similar names as offshore companies. Upon formation, the companies establish bank accounts in the U.S. financial system. The shell companies may engage in a legitimate business purpose. However, for purposes of the offshore currency exchange, it acts as an additional layer to complete the permuta. U.S. financial institutions may have reservations and risk-based policies on transactions involving offshore companies. As a result, the use of the U.S. shell company is an effective method in an attempt to increase the transparency between the transactions in the permuta process to satisfy the U.S. financial institutions. Here, the offshore company wire transfers the USD to the similarly named U.S. shell company. Subsequently, the shell company distributes the funds to the individuals and corporations.

U.S. financial institutions should proceed with caution on U.S. shell companies. The companies are vulnerable to abuse and can be exposed to domestic and international illicit activity. The centralized formation by the registered agent significantly reduces the transparency of true ownership. Moreover, numerous companies can be formed for strategic periods that shadow or are a result of certain economic events, which may raise the appearance of impropriety.

Documenting the Permuta

The U.S. financial institution should request from its customer or U.S. broker-dealer the purchase and sale agreements of the permuta. Preferably, the agreements shall identify the parties, bond type and issuer, code, exchange rate, the USD value and any additional information required to properly identify the transaction. This does not extinguish the inherent risk in the transaction with the offshore company. Rather, the agreements attempt to support and confirm permuta activity in the customers account.

Conclusion

In Venezuela, the permuta is the most common and effective legal method for individuals and corporations to exchange BsF to USD. However, the process to convert the currency relies on shell and offshore companies that seek to eliminate any transparency in the currency exchange between Venezuela and the U.S. As a result, an inherent risk exists in the transaction because the true source of funds is unknown and funds associated with these companies are susceptible to illicit activity. U.S. financial institutions must remain cautious when their customers are found to be engaged in the permuta process. A risk-based approach should be undertaken that classifies the customers as higher-risk, their accounts subjected to enhanced due diligence, and continuous transaction monitoring.

Juan L. Santos, CAMS, Miami, FL, USA. juansantos@gmail.com

Brian J. Stoeckert, CAMS, president, Stoeckert Consulting Inc., Los Angeles, CA, USA. brian@stoeckertconsulting.com

Monitoring the exchange

For Customer Identification Purposes, the U.S. financial institution should effectively utilize a risk-based approach to manage customer accounts engaged in transactions that appear to be permuta activity. As a result, those customers should be classified as higher-risk, subjected to enhanced due diligence, and continuous transaction monitoring.

Transactions with offshore companies and domestic shell companies must be continuously monitored and scrutinized. Wire transfer analysis should be undertaken to determine certain transaction patterns, reference information on each wire transfer, locations of the originators, dates, deconstructed amounts when aggregated equal one large sum, spikes in volume inconsistent with prior account history, and activity concurrent or subsequent to publicized economic events. Certain offshore companies may pose a significant risk for various reasons to the U.S. financial institution. In response, it may consider blocking transactions involving those companies.

If a U.S. financial institution discovers suspicious activity in the currency exchange transactions, then it is required to file a Suspicious Activity Report (SAR) with FinCEN. In the SAR narrative, concise details should be provided on the originators, offshore companies, offshore banks, wire reference information, domestic shell companies, registered agents, and any information that would identify the overall picture of the transaction.
In a financial institution where hundreds of thousands of transactions are processed every day, how do you detect the few that may represent suspicious behavior that should be monitored and investigated?

The traditional method used by a large number of financial institutions but only applied to a limited number of accounts is the Know Your Customer (KYC) approach of comparing actual transaction activity to a customer’s anticipated behavior. This approach has two serious drawbacks. The first is its dependence on determining customers’ true anticipated activity, while the second is resolving the first drawback for a significant number — if not all — customers of the institution.

Completing the Customer Identification Program (CIP) during account opening is an ideal time to complete a questionnaire about the products a customer will use and to anticipate transaction levels. In an ideal setting this would work; however, this approach only captures the necessary information for customers opening a new account. Anyone planning to conduct transactions for money laundering purposes is unlikely to provide accurate information. The problem is compounded when “regular” customers think the CIP information requests are intrusive and do not provide accurate responses or abandon opening the new account with your institution altogether.

In both situations, the institution may be left with erroneous information that is must use to determine unusual out-of-pattern behavior.

Even if the institution were operating in an ideal environment, the huge challenge remains to collect accurate transaction activity for all customers. This would be realistically impractical, probably impossible, for any institution with more than 10,000–20,000 customers. How about 50,000 customers, 200,000, or over one million?

Given the significant value to an institution of monitoring out-of-pattern behavior what can an institution’s Bank Secrecy Act (BSA) officer do to comprehensively monitor all customers’ transactions?

The answer is statistical analysis of transaction patterns.

This method allows monitoring each customer’s behavior over a period of time and compares how their current transaction behavior compares to their past behavior. Accomplishing this comes from the statistical methodology of Standard Deviation (sigma $\sigma$) where one looks at a recent set of transactions over a period of time and compares this to the transactions of a base period.

This mathematical technique eliminates one of the disadvantages of the KYC approach discussed above and is more accurate in identifying out-of-pattern transaction activity. It provides alerts in a clear and simple way as part of the regular Money Laundering Routines (Scenarios) run everyday by the institution’s BSA team. Statistical analysis does not require any questionnaires to be completed or interviews to be conducted while allowing all customers to be included at the very start of the AML monitoring program!

In simple terms, Standard Deviation is a measure of a data point’s (financial transaction $ value) variance from the average transaction amount of all transactions over a specified period of time. One may also include the $\sigma$ based on the number of transactions.

The standard bell shaped distribution curve is used here to represent each customer’s transaction profile and calculate the standard deviation (sigma $\sigma$) value. Using this value, the BSA officer can decide how sensitive they want to be in creating...
alerts by selecting a \( \sigma \) for the routine e.g., 2 \( \sigma \) will generate alerts on about 32% of transactions while a 3 \( \sigma \) will generate alerts on about 1% of transactions. Therefore, a 3 \( \sigma \) transaction is much more likely to represent an out-of-pattern transaction.

Transactions
The calculation of averages and the \( \sigma \) is done automatically for all customers and accounts, so the BSA officer now has a powerful and sophisticated tool that is designed easily into a money laundering routine(s) that can be applied to:
- ALL customers,
- A group of customers defined by a common characteristic, e.g., all customers with a high dynamic risk rating \( >25 \),
- Specific customers identified by CIF or TIN.

For each routine, a different \( \sigma \) can be applied to allow for different sensitivities to the data. Given the risk of false positives generated from any new routine, the routines can be run against a test database (this allows for alerts to be deleted) so that the parameters can be fine tuned until the BSA officer is satisfied that the Alerts are valid. Then the routine can be moved into the Production Database.

For example, most customers have typical monthly income and expenses (salary and expenses such as car payment, mortgage payment, and credit card payment, utilities, etc.). The difference amongst these customers is the magnitude of their transactions.

The \( \sigma \) for each customer is calculated automatically and is unique to that customer or entity.

For the routine illustrated above if a deposit transaction is at least \$5,000 and 3 \( \sigma \) from the average transaction plus the transaction is at least \$2,000 more than the average transaction then an alert will be generated.

An alert is also generated if a withdrawal transaction is at least \$10,000 and 3 \( \sigma \) or more from the average transaction and \$4,000 more than the average withdrawal transaction.

Consider two customers:
The first customer has an average transaction amount of \$1,200 with a \( \sigma \) of \$600. The most significant transactions are two \$2,500 salary deposits per month and a mortgage payment of \$1,800. At 3 \( \sigma \) the threshold transaction amount for triggering an alert for this customer is \$3,000.

However, the routine specifies that a deposit transaction has to be at least \$2,000 more than the average transaction then the amount for triggering an alert is increased to \$3,200. Further, the final condition for triggering an alert is the \$5,000 minimum. So for this customer, any transaction below \$5,000 would not trigger an alert.

The second customer has a much higher salary, \$15,000 per month, two \$7,500 deposits and relatively greater expenses. This customer has an average transaction amount of \$3,600 per month with a \( \sigma \) of \$2,500. At \( 3 \sigma \) the threshold transaction amount for triggering an alert for this customer is \$11,100.

The \( \sigma \) threshold used to generate alerts requiring investigation mainly depends on the financial institution's size, transactions per day and the number of staff available to investigate these transactions. Based on the normal distribution represented by the curve above a bank with 100,000 transactions per day can expect to have 250 transactions greater than 3 \( \sigma \) or only seven transactions at 4 \( \sigma \).

Conclusion
BSA compliance efforts have been hampered in the effort to conduct meaningful KYC transaction analyses because of the dual challenges of determining valid anticipated data for each customer and including all customers.

For the purposes of identifying out-of-pattern customer transactions, the standard deviation (\( \sigma \)) calculation is a powerful and flexible tool because it eliminates two major limitations that are inherent in the traditional KYC approach. This SD method enables the BSA officer to measure and compare truly out-of-pattern behavior against actual past behavior for all customers and all accounts. This method also has the added benefit of adjusting to the most recent transaction history to build a more relevant profile of typical behavior.

The threshold for how out-of-pattern activity should be alerted is determined by the BSA officer and easily adjusted as necessary in the test database to assure that only valid alerts will be generated when the SD routine is moved into the Production Database.

Robert Cooper, principal software engineer, Focus Technology Group, West Peabody, MA, rob.cooper@FocusTechnologyGroup.com

Stephen O. Friend, CAMS, AMLP, vice president of sales, Focus Technology Group, West Peabody, MA, USA, stephen.friend@FocusTechnologyGroup.com

www.ACAMS.org
Recognizing suspicious activity — Red flags for casinos and card clubs

Financial Crimes Enforcement Network (FinCEN)
US Department of the Treasury
Guidance FIN-2008-G007
Issued: August 1, 2008

This guidance is intended to assist casinos and card clubs with reporting suspected money laundering, terrorist financing and related financial crimes. This guidance contains examples of circumstances or “red flags” - based on actual reports, the observations of examiners and the experience of law enforcement - that may indicate the presence of money laundering, terrorist financing and related financial crimes.

Casinos that are subject to the federal Bank Secrecy Act (BSA) have an obligation to implement anti-money laundering programs that include procedures for detecting and reporting suspicious transactions. Casinos are required to implement risk-based anti-money laundering programs that assist with the identification and reporting of suspicious transactions, including employee training and written procedures for recognizing and addressing indicia of suspicious activity and vulnerabilities that may arise in the provision of particular products and services.

Recognizing suspicious customer activity

Casino employees who monitor customer gaming activity or conduct transactions with customers are in a unique position to recognize transactions and activities that appear to have no legitimate purpose, are not usual for a specific player or type of players, or are not consistent with wagering transactions. Many casinos routinely obtain a great deal of information about their customers through deposit, credit, check cashing, player rating and slot club accounts. These accounts generally require casinos to obtain basic identification information about the accountholders and to inquire into the kinds of wagering activities in which the customer is likely to engage.
Attempts to evade BSA reporting or recordkeeping requirements

Be alert to customers who try to keep their transactions just below the reporting or recordkeeping thresholds, such as:

- Two or more customers each purchase chips with currency in amounts between $3,000 and $10,000, engage in minimal gaming, combine the chips (totaling in excess of $10,000), and one of them redeems the chips for a casino check.
- A customer seeks to cash out chips, tickets or tokens in excess of $10,000, but when asked for identification for completing a CTRC, reduces the amount of chips or tokens to be cashed out to less than $10,000.
- A customer pays off a large credit debt, such as markers or bad checks, of more than $20,000 over a short period of time (e.g., less than one week), through a series of currency transactions, none of which exceeds $10,000 in a gaming day.
- A customer receives a race book or sports pool payout in excess of $10,000 and requests currency of less than $10,000 and the balance paid in chips. The customer then goes to the cage and redeems the remaining chips for currency in an amount that is less than the CTRC reporting threshold.
- A customer, who is a big winner, enlists another individual (who is not a partner of the customer in the gaming activity), to cash out a portion of the chips or tokens won to avoid the filing of a CTRC, IRS Form W-2G or other tax forms.
- A customer attempts to influence, bribe, corrupt, or conspire with an employee not to file CTRCs.

Using a cage solely for its banking-Like financial services

Be alert to customer activity involving unusual banking-like transactions at the cage, such as:

- A customer wires funds derived from non-gaming proceeds, to or through a bank and/or a non-bank financial institution(s) located in a country that is not his/her residence or place of business.
- A customer appears to use a casino account primarily as a temporary repository for funds by making frequent deposits into the account and, within a short period of time (e.g., one to two days), requests money transfers of all but a token amount to domestic or foreign-based bank accounts.

Minimal gaming activities without reasonable explanations

Be alert to customers conducting large transactions on the floor with little or no related gaming activity and without reasonable explanation, such as:

- A customer purchases a large amount of chips with currency at a table, engages in minimal gaming, and then redeems the chips for a casino check.
- A customer draws casino markers (e.g., between $5,000 and $10,000) which he/she uses to purchase chips, engages in minimal or no gaming activity, and then pays off the markers in currency and subsequently redeems the chips for a casino check.
- A customer makes a large deposit using numerous small denomination bills (e.g., $5s, $10s and $20s); and withdraws it in chips at a table game, engages in minimal gaming, and exchanges remaining chips at a cage for large denomination bills (e.g., $100), a casino check or a money transfer.
- While reviewing computerized player rating records, an employee determines that a customer frequently purchases chips with currency between $5,000 and $10,000, engages in minimal gaming, and walks away with the chips.
- A customer using a slot club account card inserts $2,990 of paper money (or an amount just below established thresholds) into a slot machine or video lottery terminal (e.g., contemporaneously inserting $5s, $10s and $20s), accumulating credits with minimal or no gaming activity, presses the “cash out” button to obtain a ticket. The customer goes to three other machines and conducts the same activity for $2,990 at each machine. Then the customer redeems the tickets for large denomination bills or casino checks with different cashiers at different times in a gaming day.
- A customer transfers funds to a casino for deposit into a front money account in excess of $5,000; and withdraws it in chips at a table game, engages in minimal or no gaming activity, and exchanges remaining chips at a cage for a casino check.

Unusual transaction characteristics or activities

Be alert to transactions with any unusual characteristics, such as:

- A pair of bettors frequently cover between them both sides of an even bet, such as:
  - Betting both “red and black” or “odd and even” on roulette;
  - Betting both with and against the bank in baccarat/mini-baccarat; or
  - Betting the “pass line” or “come line” and the “don’t pass line” or “don’t come line” in craps; and, the aggregate amount of both bettors’ total wagering is in excess of $5,000.
- A customer routinely bets both sides of the same line for sporting events (i.e., betting both teams to win) and thus the amount of overall loss to the customer is minimal (known as hedging).
- A customer requests the issuance of casino checks, each less than $3,000, which are made payable to third parties or checks without a specified payee.
- A customer furnishes a legitimate type of identification document, in connection with the completion of a CTRC, or the opening of a deposit, credit or check cashing account, which:
  - Does not match the customer’s appearance (e.g., different age, height, eye color, sex); or
  - Is false or altered (e.g., address changed, photograph substituted).
- A customer presents information for the completion of CTRCs for different gaming days that contains conflicting identification information, such as:
  - Different address or different spelling or numerical address;
  - Different state driver’s license number; or
  - Different social security number.
- A customer makes large deposits or pays off large markers with multiple instruments (e.g., cashier’s checks, money orders, traveler’s checks, or foreign drafts) in amounts of less than $3,000.
- A customer withdraws a large amount of funds (e.g., $30,000 or more) from a deposit account and requests that multiple casino checks be issued each of which is less than $10,000.
- A customer arranges large money transfers out of the country which are paid for by multiple cashier’s checks from different financial institutions in amounts under $10,000.

Criminal activities

Be alert to a customer conducting illegal activity, such as:

- A customer conducts transactions that the casino believes to be the result of some illegal activity or from an illegal source (e.g., narcotics trafficking).
- A customer or a group of individuals forge signatures or use counterfeit business or personal checks to obtain currency, chips or tokens.

Questions or comments regarding the contents of this Guidance should be addressed to the FinCEN Regulatory Helpline at 800-949-2732.

Garry Clement, CAMS, managing director, IPSA International, Toronto, Canada, garrypaisntl@xplornet.com
Anti-money laundering (AML) measures stemming from the Bank Secrecy Act (BSA) and the U.S. Patriot Act were created to ensure that society is protected against criminal and terrorist activity. The rationale why different financial sectors fall under mandatory AML regulation is clear when one considers how these entities are excellent vehicles to launder money. In observing this rationale, why have hedge funds been essentially excluded from this category? Is there a need for mandatory AML compliance in hedge funds? There appears to be many schools of thought on this. With a new administration taking over the White House and scrutiny in all areas of compliance, the debate might soon come to an end. What does this potential change mean for AML professionals with a limited understanding of hedge funds, as well as for hedge fund compliance professionals with limited exposure to mandatory AML compliance? This and other questions can be put into perspective by analyzing the current market and related AML and hedge fund issues.

History and future direction of proposed legislation

In September of 2002, Financial Crimes Enforcement Network (FinCEN) put forth proposed amendments to the BSA that would require many types of hedge funds to fall under mandatory AML regulatory compliance. The several different aspects of this proposed legislation appear to be moot for the time being as review of these amendments were repealed through FinCEN in October of 2008. Does this mean that this issue is going to be ignored,
or should we expect a complete revamp? Perhaps the current administration is too inundated with resource allocation in financial oversight as a result of a crumbling economy. Or have matters been put on hold because hedge funds are composed of large investors that appear to pose little imminent threat of terrorism? Only time will tell, but it stands to reason that President-elect Barrack Obama will create mandatory hedge fund compliance regulation based on his 2007 support of the Stop Tax Haven Abuse Act that he co-sponsored with Senators Carl Levin and Norm Coleman.

Government oversight

Before the government starts overseeing hedge funds, it needs to find the appropriate regulatory body that has the available resources and expertise to take the lead on AML compliance. FinCEN could hire and train existing personnel, but such an undertaking could prove to be too much for them to take on themselves. Hedge funds are similar in many ways to the types of institutions that FinCEN now oversees, but at the same time there are many aspects of hedge funds that are quite different and unique. Clearly, the regulatory agency designated as the main oversight body must be carefully handpicked with the necessary resources and skills to take on this new specialized area. In addition to the oversight body, the legislative branch must be flexible and be prepared to adopt amendments and make additions to any new legislation that conforms to this embryonic and evolving area of regulation.

Merging of two disciplines

There are essentially no existing mandatory AML regulations for hedge funds, as most of the current compliance work in this field is undertaken primarily through due diligence measures. As a result, many self-administrated hedge funds and third-party hedge fund administrators that perform compliance work appear to have little practical experience in dealing with a full-scale AML investigation that stems from a regulatory action, such as a cease and desist order. Similarly, many AML professionals have limited exposure to the mechanics of hedge funds that is needed to apply and implement an AML engagement. When new legislation forces these two worlds to collide, they are going to have to educate one another and transfer knowledge in a joint effort to achieve regulatory mandated goals. For example, if malfeasance is suspected at a hedge fund, the hedge fund might be ordered to perform an investigation that is analogous to a look-back. The seasoned AML professional will have the expertise to analyze and migrate relevant data, set risk parameters, write SARs, perform testing, coordinate and meet regulatory deadlines. Such expertise however is only half of the equation that cannot be fully implemented without sharing knowledge with internal and external hedge fund professionals that deal with derivatives and other complex financial transactions that are unique to hedge funds.

The marriage of AML and hedge funds has a particular importance in the area of Know Your Customer (KYC) where the structure and composition of hedge funds typically have many layers and different types of investors that are not found in other financial institutions. Again, the AML professional knows how to attack the overall KYC issues and systemically write policies and procedures, investigate, monitor and report, but because of the aforementioned unique makeup of hedge funds, AML professionals will most likely need the assistance of a hedge fund professional to successfully accomplish this task.

Ultimately, after an undefined period of time, this symbiotic relationship could result in the production of single well-rounded professionals with expertise in both disciplines. However, until that time, professional consulting firms and staffing needs will most probably need to draw from and supply the requisite mix of AML and hedge fund professionals.

Industry perspectives

Hedge fund compliance firms stand in a position to make a difference in both the hedge fund and AML compliance sector if new legislation is passed. These firms are the true pulse of the overall compliance of hedge funds, and the successful hedge fund compliance professional knows the genesis of AML and will track it into any new legislation. CEO, William G. Mulligan Jr. of HedgeOp Compliance, which addresses all facets of hedge fund compliance issues including the current demand for AML engagements. Mr. Mulligan stated that current AML compliance issues focus on the due diligence of Know Your Investor (KYI) to ensure that all investors in a fund have been thoroughly researched. Mr. Mulligan believes that there could be a “synergy” with AML professionals to the extent that new legislation require testing of policies and procedures. He said, “AML professionals could perform the testing of policies and procedures developed by hedge fund compliance firms.”

Technology solution experts who form the backbone for any hedge fund or AML undertaking should not be overlooked. Prashant Muddu is a principal at Naveara Consulting, a firm that offers specialized development and implementation of customized business intelligence. Realizing the need to address KYC issues within the context of hedge funds, Mr. Muddu stated that “when dealing with hedge funds, it is the responsibility of fund managers to ensure that known risk groups or individuals are identified” and he further states that there is a need to maintain and upkeep this information that can be accomplished through various tools that “are available for performance identity verification.” Clearly the highly skilled work performed by Mr. Muddu is already in effect for hedge funds practicing due diligence, but new legislation could make these and other functions mandatory.

Conclusion

No one holds the crystal ball that is going to show us what AML mandates will ultimately be levied upon hedge funds. But the issue, while still in its infancy, is thought provoking and warrants airtight. Although hedge funds are essentially free from AML regulation now, a new specialized niche might be created that will ultimately be levied upon hedge funds worlds if new legislation is passed.

Aaron Kahler, CAMS, managing director, Kahler Forensic Solutions, akahler@kahlerforensicsolutions.com

Christopher Ernst, CAMS, CFE, J.D, managing director, Kahler Forensic Solutions, cernst@kahlerforensicsolutions.com
The dismal and downward spiral of the American economy pushed Illinois Senator Barack Obama into the presidency. Rising jobless claims and the media’s fascination with the word recession also aided the President-elect. Now that he has won the presidency those same economic difficulties loom as his greatest challenge.

The economy has always been a measuring stick for the success or failure of an American president. Bad economic tidings contributed greatly to tarnishing the legacy of President’s Martin Van Buren, Herbert Hoover and Jimmy Carter. Conversely, Calvin Coolidge, Ronald Reagan and Bill Clinton, presided over periods dubbed, “The greatest economic expansion in American history.” Based on the proposed economic policies of the incoming forty-fourth president, the Obama administration appears to have the potential of presiding over the greatest economic crime expansion in American history.
Inherent problems

This article is not designed to hash out every aspect of President-elect Obama’s economic plan, but there are several factors at play, which do not require an economist for interpretation. First, when one party controls the presidency, House of Representatives, and the Senate, in this case the Democrats, a foundation exists for the unfettered willful blindness of economic ignorance in exchange for voter appeasement. Second, and more importantly, America is financially strapped. When you combine the deficit, bailout, and proposed Obama tax philosophy, the only realistic road to solvency is one paved with a massive across-the-board tax hike.

Undoubtedly, the Obama plan would lift up the most downtrodden among us. Nothing wrong with that, in fact, it is a noble endeavor. But unlike the previous administrations of Reagan and Clinton, it will come at a costly expense to the rest of the nation. Obama’s economic team and Congress seem to be stumbling into a convoluted version of President Lyndon Johnson’s Great Society of the 1960s, where social ills could be solved through targeted tax and spending policies.

Economic insurgency

So just what does all this dinner table socialism mean for the anti-money laundering (AML) community? Seeing an upswing in economic crime during tough economic times is hardly unusual. When the public struggles to make ends meet, the temptation to scheme and earn an extra buck - or avoid taxes - becomes a by-product of government-induced frustration. That same frustration drives even the most honest and financially conservative in our ranks to consider options contrary to their own beliefs.

Beyond that, there is a more deep-rooted sentiment growing of not only taxation without representation, but rather taxation with bad representation. An economic insurgency may very well take hold, leading to an all too energetic desire to avoid taxes. Nowhere might this manifest itself more than in the backbone of America, the small business, which is not only the centerpiece of the Obama tax plan, but also the target of certain unexplained health care initiatives.

Many Americans who own small businesses are smart enough to figure out ways to keep their receipts below any government imposed taxation thresholds — especially if those receipts are slightly above the imposed threshold limit to begin with.

The 1099ing of America

In a bulletin dated May 19, 2008, U.S. Customs and Immigration Enforcement (ICE) warned that their analysis of suspicious activity reports revealed a rise in payroll schemes, many involving illegal aliens. These schemes generally center on payroll tax evasion by paying workers off the books, or issuing them 1099s as if they were sub-contractors. To a small business owner, where the profit margin may be precarious, the practice is the most enticing of lures.

Interestingly, during the campaign, Obama, and his opponent, Senator John McCain, said nary a word about illegal immigration, an issue that may very well become the next great divide.

Payroll schemes are an area where a depository institution can play a significant role. Red flags abound for certain businesses such as construction, landscaping and staffing agencies. A small business account with minimal or no tax payments of any kind on at least a quarterly basis is suspicious. So is a large weekly or semi-monthly cash withdrawal in lieu of paychecks. Look for situations where the payroll check activity seemingly, “drops dead,” replaced by the cash withdrawal. Cash withdrawals on a daily basis — sometimes through ATM machines — is another sign that day laborers are being paid off the books and on the spot.

The split paycheck, check and cash, is another maneuver by employers to minimize tax liability. The split allows someone to be on the books for tax purposes, but not for the amount of hours they’re actually working. It gives the appearance of part-time employment. The intent of course is to decrease the potential of government scrutiny. The red flag associated with this activity is a weekly combination deposit of a small payroll check and cash, where the amount of the check is hardly a weeks pay, even at minimum wage.

The Internal Revenue Service (IRS) has certain criteria under which an employer can issue a 1099, but many employers don’t care or intentionally ignore them. By issuing a 1099, an employer avoids payment of what would be their liability for the payroll tax. They also avoid workers compensation and unemployment insurance payments. It additionally creates a situation where the employee must pay his own payroll and income taxes. An employee is also required to submit these taxes via estimated quarterly remittances, which extends to state taxes too.

Transient workers generally vanish before a nickel of tax is paid. The employer, in many cases, will then feign ignorance of whom they were employing — or attempt to tap dance around the IRS criteria. The loss of state and federal tax revenue has become staggering.

Depository institutions must also beware of employers that, “social engineer,” branch personnel into providing check cashing and wire services to their employees who are not customers. Just because the funds are coming from an employer’s account is not a license to ignore Customer Identification Program (CIP) or Office of Foreign Assets Control (OFAC) procedures. Some of these employers charge a kickback to their own workers for arranging this. They also use their own employees as straw men, coercing or cajoling them into wiring their own wealth overseas under the worker’s name.

The economy has always been a measuring stick for the success or failure of an American president
In what may eventually end up as the ultimate bit of irony, President-elect Obama, cosponsored a bill that was introduced in the Senate this past September, titled, “The Employee Misclassification Prevention Act.” Among other things, the act prohibits employers from misclassifying employees as sub-contractors. If the bill is to eventually become law, President-elect Obama will have to sign his own cosponsored bill into law as president.

The effect of this legislation on tax evasion remains to be seen, but by the time enforcement catches up, the current workforce may shift even further toward illegal workers and cash payments. This can be further aided and abetted by unscrupulous individuals establishing shell companies whose sole function is to supply a never-ending pipeline of illegal workers under the guise of a sub-contractor. The shell company allows an employer to disburse one check to the shell, who then issues paychecks to the workers. The employer is now effectively off the hook, since they do not have to argue sub-contractor status for individuals. Throw in the willfully blind and/or complicit Money Services Business (MSB) that cashes the worker’s checks, President Obama may be in the throes of his re-election bid before any headway is made.

Cash is king
Pocketing sales tax receipts is another area that will most likely see a spike. It’s a general consensus that people who operate a cash-intensive business skim, but added financial pressure, combined with a newly developed economic belligerence, may see them brazenly increase their appetite for skimming, depriving the government of income and sales tax revenue.

Structuring will also increase as business owner’s hide and horde cash, only to surface it out of necessity or for luxury items. Expect international outgoing wires to see a jump in volume as people try to shift their wealth, some of it untaxed, out of America. Custodial accounts, long a staple of financial shenanigans, will continue to be a source to disguise funds.

An economy in hard times also brings out the worst in people, those peddling everything from phony investment scams to saving your home from foreclosure. In many cases, the victims are the uneducated or the elderly. Questioning elderly people withdrawing large sums of cash is a responsibility as opposed to an invasion of privacy. Suspicious activity is not for money laundering alone, as the preponderance of cases in Part III — Suspicious Activity Information — of the suspicious activity report (SAR) form reflects.

Credit fix
Intentional over-lining is prevalent enough at any time, but faced with desperation and the inability to obtain credit, don’t be surprised if people take it upon themselves to extend their own credit limits. Intentional over-lining occurs when a borrower, usually a credit card user, knowingly sends a bad check to payoff or substantially reduce a large credit card balance, then immediately uses the card before the check is returned. This happens because the payment must be immediately credited creating available funds on the line.

A tip-off that this may be about to occur is excessive inquiries by the borrower, sometimes several times a day, to verify that payment was received. In some cases the borrower can double his or her line of credit in the blink of an eye. If it's an honest mistake, the funds to correct it should be on hand and tendered immediately. If not, it's bank fraud.

Behind the curve
The challenge for the AML professional at a depository institution will never be greater. Poring through deposit and withdrawal records is as time-consuming and laborious as it gets, but in case after case, analyzing those records and their patterns is the key ingredient to unearth- ing economic crime. In some cases it won't help. Discovering someone skimming is extremely difficult from an AML standpoint. AML on a cash-intensive small business is all about too much cash coming in, and how it’s going out, not determining if the business is under-performing.

Finally, one of the major problems in fighting money laundering and economic crime at the depository level is something that can be referred to as the cost center syndrome. The criminal, and the rise in criminal problems, will always be ahead of the staffing curve in the AML area. Getting management to increase staff is difficult enough, but with a sputtering economy the reluctance will even be greater. It may well take the demands of regulators to spur those in charge of your financial institution into action.

The American economy is the quintessential conundrum in American presidential politics. The cyclical nature of an economy and the complex nature of America’s economy in many cases will leave a president at its mercy — despite what they enact. With the campaign rhetoric gone, don’t be surprised to see the Obama philosophy morph into a polar opposite shift. He’s already talking about a massive public works program reminiscent to those of the 1930’s instituted by President Franklin Roosevelt in response to the Great Depression.

The aforementioned Calvin Coolidge, the thirtieth President of the United States, once said, “Collecting more taxes than absolutely necessary is legalized robbery.” Perhaps, President-elect Obama will think of that when he looks at Coolidge’s portrait some sleepless night in the White House.

Charles Falciglia, CAMS, Suffern, New York, USA, redstate05@yahoo.com
During this free interactive web seminar, our panel of experts will:

- Explain expectations for program evolution, development and enforcement
- Update you on what to expect from the enforcement actions and how to mitigate the risk to your organization as you move forward
- Address your questions during our live Q&A session

REGISTER TODAY FOR THIS FREE WEB SEMINAR!

www.ACAMS.org/RedFlags
Masterclass initiative

In a developing anti-money laundering (AML) environment the role and responsibilities of those dealing with it are continuously changing. Changing roles and responsibilities imply a need for enhanced competencies. To support AML specialists in acquiring these competencies education must change accordingly. The ACAM/UMBS Masterclass Anti-Money Laundering is an initiative to realize this.

Competencies in the changing world of AML

AML has become a major issue in the corporate world, particularly in the financial services industry. The main reasons for that is the significantly enhanced general awareness that money laundering is a severe threat to our economic system and the – obviously related – expansion of AML laws and regulations.

Over the past decade the role of those dealing with AML has changed and has become much more senior. Their working environment is now more demanding and AML activities are more integrated in commercial processes. AML has become an area where many professional disciplines meet under the umbrella of the basic business principle of profitability.

The knowledge and skills needed for the implementation and maintenance of AML concepts, policies, and programs have developed rapidly. Nowadays the competence to turn concepts into action is key. It requires the ability to deal effectively with internal politics, strategic planning, and external stakeholders. As a result communication skills are needed more than ever.

AML specialists are rapidly evolving toward the level of other well-established professionals, such as certified public accountants and lawyers.

Enhanced AML education

To prepare AML specialists for the changing environment their education must be adapted continuously. AML education must aim to develop an attitude that enables AML specialists to face the future challenges in a conceptual and flexible, yet pragmatic way. An exam preparation program that combines an academic approach with existing AML education is one option. This concept is not new and has a proven track record in Europe regarding the education of Chartered Accountants and Chartered Controllers.

Since money laundering knows no boundaries, combating it effectively can only be done when the professional standards, working methods, and the level of knowledge are comparable worldwide. On a global scale, ACAMS, the professional body for AML specialists, is by far the leading body for AML standards and well-developed educational programs. However, in order to keep this certification relevant, constant evaluation and adjustment of the current approach — including educational programs and promotion channels is needed.

In cooperation, ACAMS and the Universiteit Maastricht Business School (UMBS) are organizing a Masterclass Anti-Money Laundering. This is one of the initiatives to respond to the evolution of AML education needs and to establish new channels for promoting ACAMS as the leading international professional body of AML specialists. This Masterclass, organized for the first time in March 2008, prepares participants for their CAMS certification exam in an academic environment.

The applied methodology is a combination of self-study, lectures, cases and discussions among the participants. All lecturers have proven track records in turning AML concepts into operational environments in their specific professional discipline. All lectures have proven track records in turning AML concepts into operational environments in their specific professional discipline. The Masterclass is an international oriented and comprehensive program. It is offered in a six-day seminar and is followed by the official CAMS exam organized by ACAMS. The main topics discussed are:

- The (macro economic) framework of money laundering;
- The view of the prosecutor, the judge, and the attorney;
- The view of the regulator;
- Anti-money laundering policies, programs, and procedures;
- The anti-money laundering (internal) control environment;
- The concept and implementation of risk based approaches;
- IT support;
- Special investigations from a forensic investigator point of view;
- Financial Investigation Units (FIU);
- The next generation money laundering.

The participants of the first Masterclass heralded the course and its wide scope and the quality and experience of the lecturers. More than 85% of the participants passed the exam with an average score of 90%.

The second course is scheduled for March 2009. Detailed information on the Masterclass Anti-Money Laundering is available on www.ombs.nl/aml. Any further questions can be directed to Drs. Ingrid Voncken at i.voncken@umbs.nl.

Prof.dr. Eddy Vaassen RA is professor of Accounting Information Systems at the Universiteit Maastricht and the Universiteit van Amsterdam

Jos de Wit RA, CAMS is Non Executive Director and Chairman of the Audit Committee of Euro Clear Netherlands and senior expert for AML projects of the Council of Europe

Drs. Pat Hermse RA is Executive Director of Van Lanschot Bankiers (Luxembourg) SA
moneylaundering.com makes everyday a bank holiday.

Leveraging the internet to get your essential AML news and training has never been easier and more efficient.

Find out more at moneylaundering.com/mlp
New York Chapter

The ACAMS New York Chapter recently provided another stellar workshop entitled, “Insurance as a New Asset Class: AML Best Practices.” The keynote speaker was Brian Loutrel, VP & Chief Privacy Officer of New York Life Insurance and Annuity Corp. Additionally a panel of regulators was on hand and included an Agent from the IRS Criminal Investigation division currently assigned to the OCDEFT task force, and an IRS CI analyst assigned to the BSA/FinCEN unit. Mr. Loutrel explained the products covered by regulation, high risk products and how to design an AML program specifically for the insurance industry.

Although the next workshop’s details have not been finalized, rest assured, we will continue to provide the members with presenters that are at the top of their respective industries and topics that are timely and informative.

The New York Chapter Board would like to extend our warmest holiday wishes to all our Chapter members, all ACAMS’ members and the employees of ACAMS. The board members would like to bid you all a happy holiday season in some of their native dialects:

- **Nollaig Shona Dhuit**
  Gaelic – Happy Christmas

- **Καλά Χριστούγενα**
  Greek – Merry Christmas

- **Chag Sameach**
  Hebrew – Joyous Festival

- **Maligayang Pasko**
  Tagalog – Merry Christmas

- **Buon Natale**
  Italian – Happy Christmas

Kevin Sullivan, CAMS, NY Chapter Co-Chair

Chicago Chapter

On September 11, 2008, the ACAMS Chicago Chapter held its inaugural meeting, marking a continued drive toward the national expansion of ACAMS activities to meet the needs of its members and the markets in which they serve. According to Chapter Co-Chair Jack Oskvarek, “We chose to launch the Chicago Chapter on this date in order to pay respect to those who were lost on that tragic day.”

Recently, the Chicago Chapter held its first AML workshop, entitled “Managing AML Risk and SAR Review,” on December 4, 2008. The event was sponsored by BDO Consulting, a division of BDO Seidman, LLP, a consultancy with offices in downtown Chicago. The workshop featured both a guest speaker, David D. Barth Special Agent with the US Treasury’s IRS – Criminal Investigation Division, and round table discussion with guest panelists Frank Vecchione, Manager, BDO Consulting, and Michael Florence, Senior Manager, Crowe Horwath LLP.

Special Agent Barth provided a comprehensive “behind the scenes” overview of Suspicious Activity Reports (SARs) through discussion of the history, life cycle, effectiveness and impact of SAR filings. Highlights included: in-depth analysis of current SAR data; discussion of SAR preparation and trends from the perspective of IRS; tips on improving SAR content in order to maximize their value to law enforcement; and coverage of case studies of both recent and ongoing investigations resulting from SAR filings.

Workshop panelists Frank Vecchione and Michael Florence facilitated discussions regarding AML Risk Management, AML program controls, program effectiveness, and residual risk analysis. Presenters reviewed essential elements of the AML risk assessment process, as well as current challenges and issues faced by financial institutions and AML Compliance professionals in developing and maintaining a sustainable AML risk strategy. In addition, the speakers shared general recommendations based upon industry observations, experiences and trends.

AML practitioners from various financial services institutions throughout the Chicagoland area attended the workshop, and new Chapter members were welcomed. The Chicago Chapter hopes to continue to provide a forum for the professional development of its members, as well as networking opportunities and will host similar events throughout the coming year. Members who attend learning events may receive continuing education credit toward ACAMS certification membership.

For questions or further information regarding membership within the ACAMS Chicago Chapter, please contact Chapter Membership Director Terri Downey at teri.downey@rsni.com or Co-Membership Director Steve Schneider at steve.schneider@sungard.com.
## Conferences and Seminars

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Title of Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 09, 2009</td>
<td>On-line, United States</td>
<td>Web Seminar - Adopting Best Practices for AML Compliance in a Tight Economy</td>
</tr>
<tr>
<td>January 13, 2009</td>
<td>On-line, United States</td>
<td>Seminario por Internet - El lavado de dinero a través de las nuevas tecnologías: Internet, telefonía celular y medios electrónicos—Las zonas de peligro</td>
</tr>
<tr>
<td>January 21, 2009</td>
<td>On-line, United States</td>
<td>Web Seminar - Adopting Due Diligence Strategies to Mitigate the Risks of Informal Value Transfer Systems</td>
</tr>
<tr>
<td>January 23, 2009</td>
<td>Caracas, Venezuela</td>
<td>Seminario intensivo para profesionales ALD en el marco de la nueva realidad mundial</td>
</tr>
<tr>
<td>January 25, 2009</td>
<td>Dubai, United Arab Emirates</td>
<td>2nd Annual ACAMS Anti-Money Laundering &amp; Counter-Terrorism Financing Conference Middle East-North Africa</td>
</tr>
<tr>
<td>January 28, 2009</td>
<td>On-line, United States</td>
<td>Web Seminar - Lexis-Nexis Red Flags</td>
</tr>
<tr>
<td>January 29, 2009</td>
<td>On-line, United States</td>
<td>Web Seminar - Insurance: Adopting Best Practices for Information Sharing under Section 314(b) of the USA Patriot Act</td>
</tr>
<tr>
<td>February 06, 2009</td>
<td>On-line, United States</td>
<td>Web Seminar - Overcoming FACT Compliance Challenges: Implementing and Maintaining an Effective Identity Theft Program</td>
</tr>
<tr>
<td>February 06, 2009</td>
<td>Mexico City, Mexico</td>
<td>Seminario intensivo para profesionales ALD en el marco de la nueva realidad mundial</td>
</tr>
<tr>
<td>February 10, 2009</td>
<td>On-line, United States</td>
<td>Seminario por Internet - Mercado de valores bajo la lupa: Lo último en riesgos y obligaciones que enfrenta el sector bursátil, recientes casos</td>
</tr>
<tr>
<td>February 12, 2009</td>
<td>Chicago, IL, United States</td>
<td>AML Full day Seminar - The Essential U.S. Laws, Rules and Regulations that AML Specialists Must Know</td>
</tr>
<tr>
<td>February 12, 2009</td>
<td>Chicago, IL, United States</td>
<td>AML Full day Seminar - Enhanced Techniques and Solutions to Take Your AML Program to the Next Level</td>
</tr>
<tr>
<td>February 18, 2009</td>
<td>New York, NY, United States</td>
<td>AML Full day Seminar - Essential U.S. Laws, Rules and Regulations that AML Specialists Must Know</td>
</tr>
<tr>
<td>February 18, 2009</td>
<td>New York, NY, United States</td>
<td>AML Full day Seminar - Enhanced Techniques and Solutions to Take Your AML Program to the Next Level</td>
</tr>
<tr>
<td>February 18, 2009</td>
<td>New York, NY, United States</td>
<td>Seminar - The Essentials of an Effective AML Compliance Structure for Money Services Businesses</td>
</tr>
<tr>
<td>February 18, 2009</td>
<td>On-line, United States</td>
<td>Web Seminar - Weighing the Risks and Rewards of Remote Deposit Capture</td>
</tr>
<tr>
<td>February 20, 2009</td>
<td>Bogota, Colombia</td>
<td>Seminario intensivo para profesionales ALD en el marco de la nueva realidad mundial</td>
</tr>
<tr>
<td>February 26, 2009</td>
<td>Charlotte, NC, United States</td>
<td>Essential U.S. Laws, Rules and Regulations that AML Specialists Must Know</td>
</tr>
<tr>
<td>February 26, 2009</td>
<td>Charlotte, NC, United States</td>
<td>Enhanced Techniques and Solutions to Take Your AML Program to the Next Level</td>
</tr>
<tr>
<td>February 26, 2009</td>
<td>Charlotte, NC, United States</td>
<td>The Essentials of an Effective AML Compliance Structure for Money Services Businesses</td>
</tr>
<tr>
<td>February 26, 2009</td>
<td>On-line, United States</td>
<td>Web Seminar - MSBs: Perfecting Your Suspicious Activity Reporting Program</td>
</tr>
</tbody>
</table>

## CAMS Preparation Seminars

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Title of Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>February 26, 2009</td>
<td>New York, NY, United States</td>
<td>CAMS Examination Preparation Seminar</td>
</tr>
</tbody>
</table>
Web seminars

English

January 9, 2009
Adopting Best Practices for AML Compliance in a Tight Economy

Banks’ anti-money laundering units have always been considered expensive cost centers. How are AML departments affected while dreadful headlines about unexpected mergers, massive lay-offs and budget cuts make the world economy shake? How can you continue dreadful headlines about unexpected mergers, massive lay-offs and expensive cost centers. How are AML departments affected while adopting best practices for AML compliance in a tight economy? What strategies exist to achieve greater efficiency and maximize your resources?

Attend this web seminar and hear useful tips on how to maximize your AML efforts on a tight budget.

January 21, 2009
Adopting Due Diligence Strategies to Mitigate the Risks of Informal Value Transfer Systems

Hundreds of billions of dollars are funneled annually through informal value transfer systems (IVTS). These systems, which include havala, hundi and the black market peso exchange, are an alternative or underground method to remit money and in some regions of the world, like the middle east, they are integrated into the formal financial system. However, although it is used as a legitimate means of moving funds, especially in rural areas, it is often exploited by drug traffickers and terrorists to circumvent formal transaction monitoring. If these suspicious transactions infiltrate your institution, even via correspondent accounts, they can result in millions of dollars in lost revenue. In this seminar, expert speakers will assess the geographic risks of commonly used IVTS, dissect recent issued financial action task force typologies and explain what level of due diligence is necessary to thwart these ill destined transactions.

January 29, 2009
Insurance: Adopting Best Practices for Information Sharing under Section 314(b) of the USA Patriot Act

Information sharing is a valuable asset in investigating suspicious activity seen in the financial industry, including the insurance sector. Section 314(b) of the USA Patriot Act stipulates that financial institutions are permitted -- upon filing a certification form to the Treasury Department -- to share information with other financial institutions regarding suspected money laundering and terrorist financing. However, in the newly regulated insurance industry, compliance officers often time lose sight of this provision’s function and place too much emphasis on the certification reports. In this session, gain guidance on how to properly handle information sharing requests and how to improve your internal processes to ensure valuable information is acquired to strengthen your suspicious activity monitoring.

February 6, 2009
Overcoming FACT Compliance Challenges: Implementing and Maintaining an Effective Identity Theft Program

Due to confusion in the industry over the scope of the FACT Act rules, the U.S. Federal Trade Commission extended the original November 1, 2008 deadline to comply with the ID theft prevention policies until May 1, 2009. The FACT Act requires that financial institutions implement programs to detect and prevent identity theft. Bankers and former regulators affirm that their implementation can be as difficult and expensive as AML rules and the cost of failing to comply could be even higher. How do you solve the implementation challenges? How do these rules overlap with AML/CFT? Can your existing suspicious transaction monitoring systems work to catch identity theft? What are the regulatory expectations? Walk away with practical answers to these questions and ensure that your organization implements and maintains an effective program against ID theft before the implementation deadline.

February 18, 2009
Weighing the Risks and Rewards of Remote Deposit Capture

Remote deposit capture (RDC), a system that allows merchants to deposit checks directly into their bank accounts with a scanned digital image of the check, affords banks speed and convenience. However, it also introduces new avenues for fraud and money laundering. Know Your Customer is the first line of defense to protect your organization from potential abuse through this new service. This session will examine what steps banks should take to familiarize themselves with their clients’ overall management of information security, how to treat higher-and-lower risk customers and how to meet the regulatory expectations associated with this popular new technology.

February 26, 2009
MSBs: Perfecting Your Suspicious Activity Reporting Program

A properly completed SAR narrative always address the 5 Ws - who, why, where, when and what. A narrative could be deemed inadequate if it does not accurately and completely explain the nature and circumstances of the suspicious activity. During this informative session, learn some key differences between suspicious and unusual activity. We will also examine the lessons learned from the Sigue Corp. case on filling out SAR forms. In this seminar, get your pressing concerns addressed so that your organization’s SARs are an effective tool in combating money laundering.

Español

13 de enero de 2009
El lavado de dinero a través de las nuevas tecnologías: Internet, telefonía celular y medios electrónicos—Las zonas de peligro

La proliferación de sistemas electrónicos de pago y otros nuevos productos para pagar se traduce en enorme desafíos y riesgos anti-lavado para los oficiales de cumplimiento, reguladores y agentes de la ley. Por ejemplo, el M-payment es el pago a través de sistemas de teléfonos celulares, las tarjetas virtuales son las tarjetas tipo cajero automático o de retiro de dinero vinculadas a los mundos virtuales. La facilidad con la que pueden ser utilizados, la universalidad y el anonimato de estos nuevos sistemas sumados a la escasa regulación, los convierten en atractivos instrumentos para los criminales. Aprenda en este webcast las últimas novedades, cuáles son las áreas de más peligro y cómo minimizar el riesgo.
REGISTRATION FORM

Name: ____________________________

Title: ____________________________

Company: ____________________________

Address: ____________________________

City/State/Zip/Country: ____________________________

Telephone: ( ) ____________________________ Fax: ( ) ____________________________

Email: ____________________________

ACAMS Membership Number: ____________________________

---

**English**

- Adopting Best Practices for AML Compliance in a Tight Economy, January 9, 2009
- Insurance: Adopting Best Practices for Information Sharing under Section 314(b) of the USA Patriot Act, January 29, 2009
- Overcoming FACT Compliance Challenges: Implementing and Maintaining an Effective Identity Theft Program, February 6, 2009
- Weighing the Risks and Rewards of Remote Deposit Capture, February 18, 2009
- MSBs: Perfecting Your Suspicious Activity Reporting Program, February 26, 2009

---

**Español**

- 13 de enero de 2009
  El lavado de dinero a través de las nuevas tecnologías: Internet, telefonía celular y medios electrónicos—Las zonas de peligro

- 10 de febrero de 2009
  Mercado de valores bajo la lupa: Lo último en riesgos y obligaciones que enfrenta el sector bursátil, recientes casos

---

**Save More, When You Buy More!**

<table>
<thead>
<tr>
<th># of seminars</th>
<th>ACAMS Member</th>
<th>Non-Member</th>
<th>ACAMS Member</th>
<th>Non-Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$245</td>
<td>$345</td>
<td>$860</td>
<td>$1,212</td>
</tr>
<tr>
<td>2</td>
<td>$464 Save $26</td>
<td>$654 Save $36</td>
<td>$1,029 Save $196</td>
<td>$1,449 Save $276</td>
</tr>
<tr>
<td>3</td>
<td>$675 Save $60</td>
<td>$951 Save $84</td>
<td>$1,176 Save $294</td>
<td>$1,656 Save $414</td>
</tr>
</tbody>
</table>

Total Amount: $ ____________________________

---

**Credit Card**

- Visa ☐
- Mastercard ☐
- American Express ☐
- Discover ☐
- Diner's Club ☐

Cardholder Name: ____________________________

Account Number: ____________________________

Expiration Date: ____________________________ Verification Code ____________________________

(Found on the back of your credit card)

Signature: ____________________________

---

**Check**

(make check payable to ACAMS)

Please send to:

ACAMS
Brickell Bayview Center
80 Southwest 8th Street, Suite 2350
Miami, FL 33130

**Bill my institution,**

Purchase Order # ____________________________
Walk away with the practical knowledge you need to decrease costs while preserving your organization’s effectiveness:

- Hear what AML departments worldwide are doing to mitigate the impact of a weakened economy.
- Understand how the relationship between fraud and money laundering is changing the compliance landscape.
- Take home best practices to identify and eliminate inefficiencies in your AML program.
- Discover new solutions to mitigating regulatory risk.

Take away at least three practical tips or your money back!

Come early and enhance your training with pre-conference workshops!

Register by January 19 and Save $200!

Register Today!

Online: www.moneylaunderingconference.com

Phone: 800.232.3652 (in USA) or +1.305.530.0500 (outside USA)