INTELLENET NEWSLETTER

DECEMBER 2009

Table of Contents **Page**

Carino's Corner

James P. Carino, Jr., CPP, VSM
Executive Director

Each year as the end of the Holiday Season approaches we all reflect back on those events which have had an impact. Some will look back on 2009 with reservations and perhaps wish that things could have been different, while others will view 2009 as another successful year. Certainly the economy had a negative impact on the bottom line of many.

Fortunately for Intellenet, CY 2009 falls into the Good Year category as most of our short term goals were met. Through the dedicated effort of several, new initiatives were developed which led to billable time in onetime projects as well as repeat business. As the year is ending, Intellenet appears close to serving as the investigative arm for two additional entities with prospects for working relationships with others looking promising.

Our efforts to expand worldwide coverage through selective recruitment has had excellent results with adequacy of coverage throughout the US long established, several new international members were added, further strengthening our overall geographical coverage. With a formalized Recruitment Plan in place, 2010 should further enhance our capability for total global response.

The current year also saw expanded exhibiting at conferences designed to promulgate the Intellenet name, promote business and create billable opportunities for our members. Year 2010 will see further commitment in this area.

In sum, through business developed initiatives by our members, through a carefully crafted recruitment drive and through expanded exhibiting, this past year has seen fruitful execution of an economic recovery plan for our members. A goal in 2010 is for all to reap the benefit of these efforts.

My thanks to our terrific family of members for all the support, dedication and commitment and my best wishes to all for a joyous holiday season and health/success for 2010.

Intellenet Officers and Board of Directors

OFFICERS

Executive Director	James P. Carino, Jr
Assistant Director	Fred Bornhofen
Treasurer	Art Fredheim
Secretary	Nancy Poss-Hatchl

AT LARGE BOARD MEMBERS

Gerald Adams	Bruce Hulme
Gary Brown	Don Johnson
Tom Cseh	Jerry Levy
Joanne Dougherty	Reggie Montgomery
Peter Psarouthakis	Bert Falbaum
Kevin Ripa	Mary Clark Fischer
Stan Schwartz	Ruth Hoffman
Jeffrey Williams	Geoffrey Hughes
Robert Dudash	

NON-VOTING BOARD MEMBERS

Bill Blake, Editor, Intellenet Newsletter
Dennis Crowley, Special Advisor

EXECUTIVE SECRETARY

Peggy Centronze

LEGAL COUNSEL

James J. West, Esq.

ETHICS OFFICER

Fred Bornhofen

HISTORIAN

Vacant

LISTMASTER

Gary Brown

LEGISLATIVE LIAISON CHAIR

Bruce Hulme

"Man," said Fred stretching out his hands, "did I catch a fish the other day! It was enormous. It was t-h-i-s long. Why, I never saw such a fish!"

"That I believe," replied Al.

Lovestruck Hank told his girl that if she didn't marry him, he'd get a rope and hang himself right in front of her home.

"Oh, please don't do that," she pleaded. "You know my pa doesn't want you hanging around here."

Know Your Fellow Member

Herbert Simon, CPP
R.J. Montgomery Associates
Allendale, New Jersey

Herbert Simon CPP is Vice President for R.J. Montgomery Associates. During the early 1980's, Herbert's career began working for Wells Fargo Guard and Investigation Services, coordinating the Morris Plains, New Jersey office's physical security. After several years managing minimum wage employees, Herbert fortunately escaped the Industry and became the Corporate Manager of Safety and Security at Emerson Radio Corp. (North Bergen, New Jersey). Emerson, at the time an $800M company, had five North American facilities, for which all physical/electronic security, loss prevention programs/investigations were Herbert's responsibility. Additional safety responsibilities: OSHA, EPA, Worker/Community Right-to-Know and all national safety training. While at Emerson, a need for a Private Investigator arose and Kevin P. Carey (Intellenet) was the first to help Herbert solve a difficult case.

Emerson faltered and Herbert found employment at Gemini Industries (Clifton, New Jersey) and continued learning and conducting corporate (white/blue collar, cargo theft, fraud, etc.), safety and all investigations. Followed a brief 'stint' with

a company coordinating and conducting pre-employment background investigations (3,000+ in 16 months), 1996, Herbert joined R.J. Montgomery Associates, a full-service investigation firm and obtained his New Jersey's Private Detective license, 1999.

Thirteen years and thousands of cases later, the network Herbert has created is substantial and powerful, very effectively serving Fortune companies, Attorneys and domestic Clients. A former Northern New Jersey ASIS International Chapter Chair, Herbert earned his Certified Protection Professional (CPP) and has served as Law Enforcement Liaison (conducting a Valor Awards Ceremony since 1991) and Placement Chair (Herbert has a talent for and is always willing to help reconstruct his peers' résumés) for many years.

As anyone who has ever spoken with Herbert knows, he is 'Beyond Buckeye' and passionate exceeding reason regarding Ohio State Football (just ask to see his 'ink'). A twenty-five year NASCAR fanatic, Herbert makes the pilgrimage to Dover's Monster Mile, every September. With wife, Lisa, an Aruban time-share keeps the sanity . . . while raising a beautiful teenage daughter, challenges. Now living in down-State, New York (Orange County), Herbert and family extend Holiday and New Year's greetings!

New Members

Andy Hanson, Intelligence Technologies, Bakersfield, CA
Armando Castaneda----El Paso, Texas;
Jerry Cole, Coconut Creek, Florida, with 45 years of experience in the field of fingerprint identification with the U.S. Secret Service has been added to the Supplemental Support Section
Chris Finley, Finley Consulting and Investigations, Inc., Pittsburgh, Pennsylvania

Members in the News

Lynn Levy, Baltimore, Maryland received the Top 100 Minority Business Enterprise Award on November 15, 2009 at the University of Maryland.
On December 4, 2009, **Cynthia Hetherington,** Haskell, New Jersey, held a one-day seminar in Philadelphia entitled *Strategic Analytical Multi-Platformed Research Training.*
Alan Lipkin and **Al Ristuccia**, Los Angeles, California exhibited for Intellenet at the Los Angeles Paralegals Conference on October 17, 2009.

Jim Carino, Gladwyne, Pennsylvania, **Bill Blake**, Littleton, Colorado, and **Gary Brown**, Beaverton, Oregon, exhibited for Intellenet at the National Association of Paralegals Conference in Portland, Oregon on October 29-30, 2009.

Richard Horowitz, New York, New York, was a recent speaker at the Human Rights and Terrorism Conference on October 8-9, 2009 in Malaya and at the 5th Annual AML/Compliance and Financial Crime Conference October 15-16, 2009, in the Cayman Islands.

Geoff Hughes, Royal Tunbridge Wells, UK gave a presentation to bankers, accountants, attorneys and fund managers at a seminar in Bahrain on October 12, 2009.

Mayer Nudell, N. Hollywood, California, was a presenter recently at the University of Texas, San Antonio, Texas, speaking on Threat Assessment and Crisis Management Planning.

Etiquette in the Middle East

As expectations regarding good manners differ from person to person and vary according to each situation, no treatise on the rules of etiquette or any list of faux pas can be complete. As the perception of behaviors and actions vary, intercultural competence is essential. However, a lack of knowledge about the customs and expectations of people of the Middle East can make even the best-intentioned person seem rude, foolish, or worse.

Points of Etiquette

Although the Middle East is a large expanse of geography with a variety of customs, noting the following points of etiquette can be useful when dealing with people around the world who have been raised according to the traditions of the Middle East or, in some cases, Muslim societies elsewhere.

● Conducting business effectively in a souk or bazaar requires an understanding of how to haggle like the locals. This is an art requiring participants to be appropriately aggressive, keen to how much should be offered at a given point in a transaction, etc.

● The modesty of one's personal attire is of great concern to many in the Middle East, although the parameters of this modesty vary. In Saudi Arabia, for example, many families expect all female members to wear a niqab (a variety of head scarf) or burqa while even men and women visiting from other cultures should wear very non-revealing clothes to avoid harsh confrontation. In another example, males and females in shorts, skimpy t-shirts or other "immodest" clothes might find themselves roughly evicted from a variety of places, especially holy sites (be they tended by Muslims, Jews or Christians). Get specific guidelines from locals when possible.

● Regarding head attire specifically, the etiquette at many Muslim holy sites requires that a headscarf or some other modest head covering be worn. For women this might be a hijab and for men it might be a taqiyah (cap), turban, or keffiyeh. A yarmulke or other head covering is expected for men in synagogues and other places where Jews pray. Orthodox Christian sites might require the removal of hats by men but will expect women to cover their hair with a kerchief or veil.

● Among Muslims, the left hand is reserved for bodily hygiene and considered unclean. Thus, the right hand should be used for eating. Shaking hands or handing over an item with one's left hand is an insult.

● Public display of affection between people of the opposite gender, including between married people, are frowned upon everywhere more conservative values hold sway. Public displays of affection include activities as minor as hand-holding.

● In many cases, people of the same gender holding hands while walking is considered an ordinary display of friendship without romantic connotations.

● In a related point, many people in the Middle East claim a more modest area of personal space than that which is usual elsewhere. Accordingly, it can seem rude for an individual to step away when another individual is stepping closer.

● In regard to vocal emphasis, volume and body language, people in the Middle East may communicate in ways which other people (such as English and Germans) reserve for when they are angry or upset. This should be kept in mind when analyzing the mood of a situation.

● Special respect is paid to older people in many circumstances. This can include standing when older people enter a room, always greeting older people before others present (even if they are better known to you), standing when speaking to one's elders and serving older people first at a meal table.

● Many people throughout the Middle East, especially Arabs, take great pride in shows of hospitality, never failing to at least serve coffee and a snack such as figs but preferring to present guests with a lavish choice of expensive delicacies in abundance. To refuse such hospitality can cause offense.

● In some areas in the Middle East, it is common for people to take their food from a common plate in the center of the table. Rather than employing forks or spoons, people may scoop up hummus and other foodstuff with pita bread.

● In many Middle Eastern countries, grouping the thumb and fingers together, and shaking it up and down, fingers pointing upwards, indicates "wait".

● In Iran, the "thumbs up" gesture is considered an offensive insult.

● Displaying the sole of one's foot or touching somebody with one's shoe is often considered rude. In some circumstances, shoes should be removed before entering a living room.

● Many in the Middle East do not separate professional and personal life. Doing business revolves much more around personal relationships, family ties, trust and honor. There is a tendency to prioritize personal matters above all else. It is therefore crucial that business relationships are built on mutual friendship and trust.

● Responding to an anger or seriousness with light laughter or a smile is common. This must not be seen as an indication that the other person is not taking you or the situation seriously.

- A common custom in Iranian culture is 'tarof' (taarof) which can be translated as "offering"; it is common for a person to not accept an offering (food, beverages, etc) the first or possibly second time, instead taking up the offer the third, this traditionally implies dignity, self-respect and respect for the host.

- Positioning yourself so your back is not facing another person is also a common Iranian custom.

_____

Extracted from Wikipedia, the free encyclopedia.

National Archives of the United States and Federal Records Centers

The National Archives and Record Administration (NARA) is the recordkeeping agency for all U.S. government agencies. The National Archives was established in 1934 by President Franklin Roosevelt but its major holdings date back to 1775. They capture the sweep of the past: slave ship manifests and the Emancipation Proclamation; captured German records and the Japanese surrender documents from World War II; journals of polar expeditions and photographs of Dust Bowl farmers; Indian treaties making transitory promises; and a richly bound document bearing the bold signature "Bonaparte"—the Louisiana Purchase Treaty that doubled the territory of the young republic.

NARA keeps only those Federal records that are judged to have continuing value—about 2 to 5 percent of those generated in a given year. By now, they add up to a formidable number, diverse in form as well as in content. There are approximately 9 billion pages of textual records; 7.2 million maps, charts, and architectural drawings; more than 20 million still photographs; billions of machine-readable data sets; and more than 365,000 reels of films and 110,000 videotapes.

Archives locations in 14 cities, from coast-to-coast, protect and provide public access to millions of records. In addition to assisting Federal agencies and the public with research and reference services, NARA delivers educational programs and public workshops to help Americans learn how to use archived records. Further, 17 Federal Records Centers (FRC) provide Federal agencies superior records storage, access, and disposition services through a national network of facilities.

The National Personnel Records Center in St. Louis manages the records of millions of military veterans of the 20th century as well as former civilian Federal employees.

Record Restrictions

Some of the images in which you are interested may be restricted by donor agreement. To purchase a copy of these materials, you must obtain permission from the donor.

Some of the images in which you are interested may be copyrighted. It is the user's responsibility to identify the copyright owner and to obtain all necessary clearances before making, commercial, broadcast, or other use of this material.

The copyright law of the United States (Title 17, United States Code) governs the making of photocopies or other reproductions of copyrighted material. Under certain conditions specified in the law, libraries and archives are authorized to furnish a photocopy or other reproduction. One of these specific conditions is that the photocopy or reproduction is not to be "used for any purpose other than private study, scholarship or research." If a user makes a request for, or later uses a photocopy or reproduction for purposes in excess of "fair use," that user may be liable for copyright infringement.

Federal Records Center Locations

Each Federal Record Center (FRC) provides services based on geographical and federal agency criteria. Some records have restricted access, for example, prior approval of the originating agency must be obtained before gaining access to records. Telephonic contact is recommended prior to visiting any FRC.

Southeast Region
4712 Southpark Boulevard
Ellenwood, GA 30294
404-736-2820
Records of Federal Agencies located in Alabama, Florida, Georgia, Kentucky, Mississippi, North Carolina, South Carolina, and Tennessee.

Northeast Region
380 Trapelo Road

Waltham, MA 02452-6399
781-663-0130
Temporary records of Federal Agencies located in Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island and Vermont. Access to all records is controlled by the agency of origin. Records stay at the FRC until they are either destroyed through recycling or accepted by The National Archives and Records Administration as permanent records.

Federal Records Center
7358 South Pulaski Road
Chicago, IL 60629-5898
773-948-9000
Inactive records created or received by Federal agencies in Illinois, Minnesota, and Wisconsin, and Federal courts in Illinois, Indiana, Michigan, Minnesota, Ohio, and Wisconsin. Handles bankruptcy records for all courts in Illinois, Indiana, Michigan, Minnesota, and Wisconsin. Bankruptcy records for Ohio are handled by FRC, Dayton, Ohio.

Great Lakes Region (2 Locations)
3150 Springboro Road
Dayton, OH 45439-1883
937-425-0600

8801 Kingsridge Drive
Dayton, OH 45458
937-425-0601
The Kingsridge Drive facility and the Springboro Road Facility house Federal Agency records from Ohio, Indiana, Michigan and IRS and Defense Finance facilities nationwide.

Rocky Mountain Region
Denver Federal Center
Building 48
Post Office Box 25307
Denver, CO 80225
303-407-5700
Retired records temporarily transferred from Federal agencies located in Colorado, Utah, Montana, the Dakotas, Wyoming, and New Mexico. Records are maintained until they are either destroyed through recycling or accepted by NARA as permanent records. Access to all records is controlled by the agency of origin.

Southwest Region
1400 John Burgess Drive
Forth Worth, TX 76140
817-551-2000
Inactive records created or received by Federal agencies in Arkansas, Louisiana, Oklahoma, and Texas. Records are maintained until they are either destroyed through recycling or accepted by NARA as permanent records. Access to all records is controlled by the agency of origin.

National Archives
200 Space Center Drive
Lee's Summit, MO 64064-1182
Records from Federal agencies and courts in New Jersey, New York, Puerto Rico, the U.S. Virgin Islands; most records created by Department of Veterans Affairs Regional offices nationwide; and active Official Personnel Files (OPFs) from the IRS.

Na**tional Archives**
17501 W. 98th, Suite 47-48
Lenexa, KS 66219
913-563-7691
Stores and services records from Federal agencies in Iowa, Kansas, Missouri and Nebraska. Federal agencies include Department of Veterans Affairs and the Internal Revenue Service. Records are available for agency retrieval as needed.

Mid Atlantic Region
14700 Townsend Road
Philadelphia PA 19154-1096
215-305-2000
The National Archives - Mid Atlantic Regional Program serves the geographic areas of Pennsylvania, Delaware, West Virginia, Maryland and Virginia.

Northeast Region
Silvio O. Conte National Records Center
10 Conte Drive
Pittsfield, MA 01201-8230
413-236-3600
Microfilm reproduction of basic documentation of nation-wide records for the study of history, economics, public administration, political, genealogy and other subjects.

Pacific Region (2 Locations)
23123 Cajalco Road
Perris, CA 92570
951-956-2000
Open to the public by appointment only. Temporary storage of records from Federal agencies in Arizona, southern California and Clark County, Nevada.

Pacific Region

1000 Commodore Drive
San Bruno, CA 94066-2350
650-238-3500
Storage for inactive records created or received by Federal agencies in northern California and Nevada (except Clark County) and for selected agencies in Hawaii and the Pacific Ocean area. Access to all records is controlled by the agency of origin.

Pacific Alaska Region (2 Locations)
6125 Sand Point Way NE
Seattle, WA 98115-7999
206-336-5115
Records from Federal agencies and courts in Idaho, Oregon, and Washington.

Pacific Alaska Region
654 West Third Avenue
Anchorage, AK 99501-2145
907-261-7820
Records retired from Federal agencies and courts in Alaska.

National Personnel Records Center
Civilian Personnel Records
111 Winnebago Street
St. Louis, MO 63118-4126
314-801-9250
OPFs and Employee Medical Folders (EMF) of separated Federal civilian employee; medical records of military family members treated at Army, Air Force, and Coast Guard Medical facilities. Access to all stored records is controlled by the authority of the creating agency. OPFs and EMFs are strictly regulated by the Office of Personnel Management (OPM).

National Personnel Records Center
Military Personnel Records
9700 Page Avenue
St. Louis, MO 63132-5100
314-801-0800
Records of military personnel, health, and medical records of discharged and deceased veterans of all services during the 20th century (records prior to WWI are in Washington, DC); and medical treatment records of retirees from all services, as well as records for dependent and other persons treated at naval medical facilities.

Washington National Records Center
4205 Suitland Road
Suitland, MD 20746-8001
301-778-1550
Serves Federal agencies in Washington, Maryland, Virginia, and West Virginia (U.S. Courts excepted).

Carrier Evidence

John B. Minor, CCE, CSA, CSE
Atwater Enterprises
Odessa, Texas

Digital evidence has become pervasive in most investigations whether civil or criminal. Cell phones, are rapidly becoming more common digital evidence producers than computers for two reasons, First, a cell phone is often a more personal and intimate digital device than a computer. A cell phone may be used more often than a regular desktop or notebook computer for an individual's voice, video and text communications. Secondly, the volume of devices, over 850 million computers are used to communicate via the Internet whereas over 3.2 billion cell phones are used to communicate via the telecommunications infrastructure and a high percentage via the Internet. Cell phone evidence can so quickly make or break a case that investigators are often hard-pressed to find any evidence related to cell phone usage. Although forensic examination of a cell phone can frequently assist an investigation it is often the records maintained by cell phone carriers that, properly examined and interpreted, can become the true blockbuster.

A Five Step procedure should be followed by an Investigator or litigation team when the decision to pursue cell phone carrier records is made. If followed carefully, and with the support of a communications expert, an investigator can gain access to what may be explosive answers in the case inquiry.

First, determine the evidence target or decide what may be important to learn from the evidence. Much more than location tracking information and call history is usually available. Use the services of an expert to determine which evidence categories best suit your case.

Second, determine the cell phone carrier to whom the cell phone number is subscribed through.

Third, contact the cell phone carrier legal compliance department for verification.

Fourth, author a records preservation request and forward to the legal compliance department of the cell phone carrier. Use the services of a communications expert to achieve the best results in a preservation request. Hidden gotcha's such as the fact that preservation of user data maintained by a cell phone carrier is usually held from prior to the date of the preservation request but not for any dates after the request is submitted can affect the outcome of your case.

Fifth, immediate pursue a subpoena or court order depending upon what evidence you are seeking. The basic rule of thumb is that billing records may be obtained with a subpoena. Anything beyond billing records including user date maintained by the carrier, cell sit/sector associated with calls and other logging will require a court order.

	AT&T	Verizon	TMobile	Sprint	Nextel
Cell site/ Sector	30 days	1 year	30 days	45 days	18 months
SMS (Text Msg)	No storage	3-5 days	No storage	7-14 days	7-14 days
Saved SMS	No storage	No storage	No storage	Subscri ber	Subscri ber
IP History	No storage	30 days*	No storage	7-14 days	7-14 days
Email	No storage	No storage	30 days	7-14 days	7-14 days
CDR's	5-7 years	1 year	2 years**	18 months	18 months

* If computer sent the message 5-10 days
** Prepaid accounts—longer retention for monthly accounts

A communications expert should be engaged at the earliest stages of a case and should not only be able to provide guidance in the evidence determination and preservation request stages but should also be able to adequately support a court order request and provide the technical language necessary and the testimonial support for the court order request. Once the call detail records or CDR's have been obtained, the work really begins. A careful analysis of what is produced by the cell phone carrier may lead to immediate evidence conclusion but often requires additional communication with the legal compliance department of the carrier. Location tracking, social network analysis, and activity timelines are commonly useful analysis products of cell phone CDR's.

New Federal Regulation Makes Identity Theft Prevention Your Corporate Responsibility

Carrie Kerskie, CITRMS
Marcone Investigations
Naples, Florida

Lately it seems you can't read a paper or turn on the television without hearing about identity theft. One company is trying to sell you "identity theft protection" and another company has been breached and thousands of customers had their information compromised. One thing you probably haven't heard about is the new federal regulation that requires businesses to implement an identity theft prevention program. This new regulation is the FACTA (Fair and Accurate Credit Transaction Act) Red Flag Rules.

You are probably thinking to yourself, "It must not affect me because I would have heard about it from my trade association, or my attorney, or my accountant." Unfortunately the rules were written in such a way there has been much confusion regarding what types of businesses must comply. I too was confused and contacted Pavneet Singh, an attorney with the Federal Trade Commission, for clarification. What I discovered was the regulation will affect the majority of businesses, large and small, from various industries including government and non-profit entities.

The Facts about the Red Flag Rules
The FACTA Red Flag rules apply to the following businesses:

1. Users of consumer reports.
2. Credit and Debit card issuers.
3. Businesses that offer products or services in advance of payment.

Users of consumer reports are required to verify the consumer report is in fact relating to the consumer for which it was requested. This applies to landlords and employers. If you conduct pre-employment background checks on your employees it is your responsibility to verify the person applying is the person on the consumer report. If you observe an address discrepancy you must put forth reasonable effort to verify the validity of the address. In addition, you may be required to report the address discrepancy to the consumer reporting agency.

Credit and debit card issuers must implement policies and procedures regarding change of address notifications and request for replacement or additional cards received within a short period of time of an address change notification. This was implemented to help reduce identity theft where the criminal changes the mailing address on your credit card to prevent you from receiving statements and observing their purchases.

Businesses that offer products or services in advance of payment have the most amount of work to do to be in compliance with the regulation. These businesses are required to implement a written Identity Theft Prevention Program ("Program") to detect, prevent and mitigate identity theft risks associated with consumer accounts and the financial security of the business. The "Program" is flexible to reflect the size and scope of your business and the nature of your operations. The deadline for compliance was originally November 1, 2008. There have been a few extensions for compliance and, as of this writing; the current deadline for compliance is November 1, 2009.

The Identity Theft Prevention Program

The basic elements of your Identity Theft Prevention Program must include the following;

- Identify the "red flags" specific to your business.
- Detect "red flags" that have been incorporated into your Program.
- Respond appropriately to any "red flags" that are detected.
- Ensure the Program is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the business.
- Oversight of service provider agreements.

Risk Assessment

In order to identify the "red flags" specific to your business you must conduct a risk assessment. The risk assessment should identify the following;

- Risk factors
  - Types of consumer accounts offered or maintained.
  - Methods provided to open consumer accounts.
  - Methods provided to access consumer accounts.
  - Previous experience with identity theft.
- Sources of Red Flags
  - Previous incidents with identity theft.
  - Methods of identity theft identified that reflect changes in identity theft.
  - Applicable supervisory guidance.
- Categories of Red Flags
  - Alerts, notifications, or other warnings received from consumer reporting agencies or service providers such as fraud detection services.
  - Presentation of suspicious documents
  - Presentation of suspicious personal identifying information, such as a suspicious address change
  - The unusual use of, or other suspicious activity related to an account
  - Notice from customers, victims of Identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with consumer accounts.

Recently in the news breaches have occurred by employees throwing away documents with customer information in unsecured dumpsters, businesses having an unsecured computer network, or retired company laptops being sold or donated without removing customer files. The Federal Trade Commission has released guidelines to be used as just that, guidelines. Unfortunately many businesses and consultants are using these guidelines as a checklist. This will not ensure you have identified all of the "red flags" pertinent to your business. To reduce your liability you must diligently identify all "red flags" pertaining to the size and scope of your business and the nature of your operations.

Detecting

Detecting "red flags" can be handled by obtaining identifying information about your customer, verifying the identity of your customer, authenticating the customer's identity, monitoring transactions in consumer accounts, and verifying the validity of change of address requests for customers

Mitigating

Once you have identified your "red flags" you need to provide an appropriate response to any breach detected. This could be a letter you mail to your customers notifying them of the breach or closing an existing account that may have been breached. Another way to mitigate identity theft is by not collecting on a consumer account or selling a consumer account to a debt collector if it is believed the consumer was a victim of identity theft. Finally, the breach may warrant notifying law enforcement.

Periodic Updates

Once your "Program" has been completed and implemented you are required to periodically update the "Program" to incorporate any experiences your business may have had with identity theft, any changes in the methods of identity theft, or any changes to detect, prevent and mitigate identity theft. In addition, if your business has had any changes in the types of accounts offered or maintained or changes in the business arrangements of your business these need to be incorporated into your "Program". This would include mergers and acquisitions, alliances, joint ventures, and service provider agreements.

This information should be reported, at least annually, to reflect compliance with the "Program". The report should contain information regarding the effectiveness of the policies and procedures of your business regarding prevention of identity theft, service provider agreements, and significant incidents involving identity theft and management's response, and recommendation for material changes to the "Program". These can be done by a conducting compliance audits to ensure your employees are following the "Program".

Oversight of the "Program" is to be the responsibility of a board member, a board committee member or senior level employee. This designated individual is responsible for the implementation of the "Program", reviewing reports prepared by staff regarding compliance with the "Program", and approving material changes to the "Program".

Consequences for Not Complying

There are many consequences for not complying with the Red Flag Rules. The Federal Trade Commission is responsible for regulating the Rules and will issue financial penalties for non-compliance. In addition, your business could be faced with civil liability and possibly criminal charges for negligent business practices.

More importantly, you are at risk of having your company's reputation damaged and loss of business from lack of consumer confidence, or customer churn. Could your business survive the negative publicity? Or what if you open a consumer account for a new customer and soon realize they provided you with false information. Who will pay for the products or services given to this customer? You cannot collect from the real person whose identity was stolen to open the account with you.

Sources of Identity Theft

There are many ways identity theft occurs. A few of them are: technology, employees and dumpster diving.

Technology

As mentioned before unsecured networks are a major source of identity theft. If a criminal can tap into your unsecured network he now has access to all of your company files. This is the equivalent of leaving the office doors and filing cabinets unlocked when you leave at the end of the day. There are also computer viruses that can be downloaded by email or surfing the internet. If your company computers do not have antivirus, antispyware and firewall protection you run the risk of a breach.

Employees

Unfortunately we are in an economy that breeds fraud. With high fuel and food expenses and the risk of foreclosure your employees may be tempted to earn extra money by selling your customer account information. When people are faced with desperate times they will do desperate things. Employees will also "bend" the rules now and again not realizing the potential consequences. This is why employers are required to train relevant staff on their written identity theft prevention program. A study by the Ponemon Institute revealed that in 2008 88% of data security breaches were the result of insider negligence. The study also revealed the average cost to mitigate a data breach was $202 per compromised record.

Dumpster Diving

I remember a few years back watching the local news reporters reporting from inside of a garbage dumpster with stacks and stacks of financial account statements. Criminals still today use trash as a source of information. This is why it is important for your company to utilize shredders. These can be purchased at a store or you can hire a company to shred your documents. You are required to shred any paper that contains customer account information including phone messages and sticky notes that is not secured.

Benefit of Complying

By complying with the Red Flag Rules, even if you are not required to, you will gain consumer confidence by protecting their personal information. You will also have a disaster plan in place in the event of a breach. In addition, you will reduce your risk of a breach of information, reduce your financial risk of civil liability and financial penalties, and reduce your risk of opening a fraudulent account. Basically you are protecting your bottom line.

Opportunities for Private Investigators

Many of the requirements for compliance are services offered by Private Investigators. A few of these are: conducting a risk assessment to locate red flags for identity theft, compliance audits to verify employees are following the "program", assisting with verification of client and employee identities and compliance audits in preparation for the annual report. Public speaking on the requirements of the regulation and how to comply for local bar associations or other trade organizations to gain exposure to new clients.

In summary, the FACTA Red Flag rules apply to users of consumer reports, credit and debit card issuers and businesses that offer products or services in advance of payment. They also provide new opportunities for Private Investigators.

The deadline for compliance is November 1, 2009.

For more information please visit the Federal Trade Commission's website at www.ftc.gov.

Carrie Kerskie is a Licensed Private Investigator and Certified Identity Theft Risk Management Specialist with Marcone Investigations, Inc. located in Naples, Florida.

"Yes I Can!"

Bill Blake
Blake and Associates, Inc.
Littleton, Colorado

In this period of business slowdown, it is imperative to be innovative to maintain your revenue flow. The "Yes I Can" concept is a money-maker that is frequently ignored, resulting in a loss of income. This concept will allow the investigator or security consultant to remain a viable business resource.

A request for services can be handled in a number of ways—with some you make money and with others you make money for others. You may not personally have the required skills to respond to a request but you have assets if you desire to use them.

For example: I receive a request for an electronic countermeasures search of a client's office. I can handle this in one of two ways. I can identify the appropriate resource, provide a name to the client, and tell him to contact the individual directly. At least two adverse actions can come out of this way of doing business.

One, you are not availing yourself of the opportunity to make money through managing the request. Two, there is a good possibility that any such requests for services will go to the person who responded to previous requests.

Second, you can adopt the "Yes I Can" approach, manage the client's request and get paid a fee for your management and quality control actions. You identify the proper resource and subcontract the tasks to them as your representative. With the resource available to you through your Intellenet membership, there are virtually no requirements that you cannot perform when you adopt the right approach.

FIFA WORLD CUP 2010 AND CRIME IN SOUTH AFRICA

Peter Grant, CFE, CII
C Risk International (Pty) Ltd
Lyttelton, South Africa

Republic of South Africa (RSA)
Population: 46.9 Million
Area: 1,219,912 sq km
GDP: US$255Billion

INTRODUCTION

The FIFA Soccer World Cup tournament will be played between 11 June and 11 July 2010 at ten stadiums in nine cities across The Republic of South Africa (RSA). For more information go to;

http://www.sa2010.gov.za/

South Africa is often referred to as one of the most crime ridden countries of the world and from time to time Johannesburg is given the title of "murder capital of the world". An exaggeration if comparison is made with Ciudad Juarez in Mexico.

This said, crime is a problem in South Africa and it is a problem that residents have to live with and adapt to. The prevalence of crime as reported in the media will most certainly come as a culture shock to foreign visitors.

There is a large population of illegal immigrants in RSA, which the authorities have difficulty in dealing with, due to the restraints of the Constitution, confusion over the definition of refugee status and interference by self professed "human rights" and charitable organisations.

As a result there are literally colonies of Chinese, Vietnamese, Zimbabweans, Angolans, Mozambicans and Nigerians in various parts of the country and particularly in the Cape Town area there are Somalis and various Farsi and Pushtu speaking Islamic enclaves. The majority of these people cannot find gainful employment and take to a life of crime. From time to time the black South Africans, who are very xenophobic, get fed up with being preyed upon and a public affray takes place aimed at foreigners.

An offshoot of the above is organised crime insomuch as the organisers are either illegal immigrants or they were not properly vetted before entering the country. There are cartels of the following nationalities; Chinese, Italians, Thaïs, Vietnamese, Zimbabweans, Mozambicans, Nigerians, Somalis, and Pakistanis involved in gambling, drugs manufacture and trafficking, people trafficking, prostitution, illegal trade in marine and wild life products, illegal trade in human body parts, fraud, kidnapping, cash heists, and receiving stolen property. A great many illegal immigrants are "employed" by organised crime.

For this paper I will list what I consider the relevant crimes. But ALL crime to some degree or another could well affect visitors from around the world for the FIFA World Cup 2010. I am not providing figures on crime trends or statistics. For the official crime statistics in South Africa go to;

http://www.issafrica.org/index.php?link_id=24&slink_id=2489&link_type=12&slink_type=12&tmpl_id=3

GENERAL

In general terms the centres where World Cup matches are due to be played will attract prostitutes, pimps, drug pedlars, and criminals not only from other parts of South Africa but, due to the porous state of our borders, also from Zimbabwe, Mozambique, Botswana and farther afield such as Nigeria.

Despite assurances to the contrary, the SAPS (South African Police Service) "master plan" may not cope with the anticipated influx of criminals as well as about half a million visitors. They are under strength and for additional manpower they may have to draw heavily on Police Reservists and in all probability they will strip classes out of the Police Training Colleges.

Morale in the SAPS is not good. The Ex SAPS National Commissioner Jacob Sello 'Jackie' Selebi is currently on trial for many counts of corruption and defeating the ends of justice. Serving white officers are resentful as they are being jumped for promotion by juniors who have little or no qualifications other than party loyalty, or the correct ethnic background. There is distrust of Asiatics by other races and amongst the Africans there are strong divisions and distrust on tribal and clan lines. Add to this that the men will be working twelve hour shifts with limited rest days which, as

the event progresses could lead to heavier than usual absenteeism due to sickness.

Notably, private security companies are now boosting their manpower in Event Management and other general security products.

CRIMES OF VIOLENCE

Generally speaking most murders that occur are black on black, but there has been a disturbing trend lately for excessive violence to be used during the commission of less serious crimes. There are far too many illegal firearms in circulation and they are readily obtainable if one has the right connections. The sources are weaponry stolen from/lost by RSA citizens, the armed forces and the SAPS; as well as weaponry smuggled in from Zimbabwe and Mozambique.
In the cities where the match venues will be held the expectation is that there will be a lot more money floating around resulting in improved cash takings in shops, bars, clubs and so forth. This will mean more cash in transit to the banks, ergo more cash in transit heists?

CASH IN TRANSIT

Cash in Transit (CIT) heists are generally very bloody and violent affairs and in this respect there are indications that some heists have been carried out by members of the Zimbabwean National Army who have used their Army issue weaponry and then returned to Zimbabwe with the loot. In general however, heists are the work of well organised gangs run by syndicates and carried out with ruthless efficiency.

A sinister development from CIT heists are shopping centre/mall robberies which are carried out with the same degree of organisation and ruthlessness and a complete disregard for casualties amongst by-standers.

RESIDENTIAL

There is an increase in house robbery as opposed to housebreakings. Now these tend to occur when the occupants of the house are awake. Simplistically the complainant opens the front door in response to a knock only to find them selves staring down the barrel of a gun. In a recent case a housewife opened the front door and got a face full of pepper spray. Resistance to these attacks can result in serious consequences. There have been cases where occupants of houses have been tortured to reveal the whereabouts of firearms, cash, safe, or vehicle keys.

Similarly more and more housebreakers are carrying guns and/or knives by day and by night which they will not hesitate to use if they are disturbed during the course of the breaking.

VEHICLE HI-JACKS

Vehicle hi-jacks are a daily occurrence in the larger centres and can be accompanied by senseless violence and murder. Volumes have been written about this crime, but the nuts and bolts are that unless a person drives extremely defensively and refrains from driving a model car that is popular with hi-jackers, anyone can end up as a hijack victim.

SMASH AND GRAB

Allied to hijackings are vehicle smash and grab attacks, where the window of a stationary vehicle is smashed so that the criminal can steal handbags, laptops, mobile phones or any other attractive items from the car seats. In some of these cases the complainant has suffered serious injuries trying to protect his or her property.

STREET VIOLENCE

Victims of street muggings (robberies) are often confronted and sometimes stabbed by knife wielding criminals some of whom are as young as nine or ten. The use of such young criminals by "Fagans" has been prompted by the law's failure to mete out appropriate punishment to the so called "street children" and the activities of "bleeding heart" organisations who maintain that the offender is "more sinned against than sinner."

SOCCER VIOLENCE

A word needs to be said here concerning organised soccer violence, which seems to be endemic in some areas of Europe. It is a phenomenon which is uncommon in South Africa although it does occur from time to time. There is a general feeling that should there be an outbreak of this brand of soccer violence between groups of fans/supporters then the SAPS would deal with it as a riot and use of rubber bullets, tear gas, police dogs, the lot!

THEFT

Thefts can and do occur at any time and any place. Favoured items are mobile phones, lap-tops, i-Pods, other electronic goods, cash, jewellery, bank and credit cards. Thefts occur from leaving accommodation unlocked, leaving one's property unattended, items of value left in plain view in parked motor vehicles, or being the victim of a pick-pocket.

MOBILE PHONES

Mobile phones and lap-tops are easily converted to cash. The receivers, who in many cases are of Pakistani origin and known as "The Taliban", use illegal programmes which enable them to reformat mobile phones and give them a new identity, and also over-ride password protection on lap-tops. Bank and credit cards are of course as good as money.

CREDIT CARD FRAUD

Last but by no means least the use of card skimmers and cloning devices has increased dramatically lately. The devices are mainly employed by organised criminal syndicates and are rarely used by individual criminals working on their own.

The new generation of card skimmers / cloners are actually smaller than the card itself, making it very easy for the card to be swiped usually by the waiter/waitress when they take the card to the till or if the card holder is distracted when signing the authorisation slip.

During a recent arrest at a restaurant at Cape Town International Airport Police found a "state-of-the-art" skimming device on one of the suspects which could hold details of up to 500 cards and they have been able to link it to fraudulent withdrawals from accounts totalling about US$15,000.00. Similarly in Johannesburg a waitress from Bulgaria was arrested with a skimming device in her possession which when full was sent to Europe where on the strength of the duplication in Johannesburg, fake cards were manufactured.

In conclusion, hereunder are some views expressed by personnel currently employed by security companies in South Africa;

"In SA many a security business and "wanna be security businesses" lick their lips for this event. But, the security business that is serious about customer service and long term relationships will realize that the security threat during the 2010 WC stretches beyond the stadiums, the hotels and busses.

It is about the threat against their current clients, especially business and residential areas as well as a threat to operational capabilities of security companies.

The risk is four fold or more;

* On the one hand will the WC event security companies lure away existing security officers from reputable security companies with lucrative cash offers to get involved in temporary jobs relating to the WC security

* A second risk is that staff would have difficulty to get to and from work with existing public transport and logistical supply to security companies could be hampered due to transport system.

* Thirdly is there the desire by all South Africans to watch the games, even if only on television which could result in probable alcohol abuse before work, late arrival for work or even plain absenteeism due to alcohol abuse or the desire to watch a specific game.

* The fourth and most dangerous risk, against the background of the three a foregoing risks, is intensified criminal activity against business and residential areas whilst the focus is on WC protection and the rest is "neglected".

A proper risk assessment at the beginning of 2010 followed by regular monitoring of the risk profile of SA or specific business areas linked to a detailed plan would be essential.

It is evident that the WC could cost business and residential areas more in terms of security - placing more security officers at probable higher "WC Rates", improving electronic security at businesses, improved response services, etc could be the order of the day."

Investigative & Security Professionals for Legislative Action (ISPLA)

Peter Psarouthakis
EWI & Associates, Inc.
Chelsea, Michigan

The primary functions of Investigative & Security Professionals for Legislative Action [ISPLA] include reviewing proposed federal and state laws and regulations in order to identify critical issues; developing policy statements; serving as a resource to the profession, government lawmakers and regulators, and the media; giving testimony before hearings, boards and study groups; and serving as an advocate for or against specific bills and regulations affecting investigative and security professionals.

In addition, ISPLA provides speakers and serves as a resource to organizations and government entities conducting workshops and educational seminars. It also identifies third-party stakeholders with mutual interests and acts as their liaison to government. ISPLA also administers a nonpartisan political action committee.

Numerous bills are considered by Congress regarding privacy issues, breaches of personal consumer information from databases or by the illegal use of pretexting, limiting the sale and distribution of the Social Security number, and the redaction of the SSN and other personal identifying information from public records.

ISPLA shares the concerns of Congress regarding the sale of personal data to the general public by firms that may have obtained such data by using a pretext. However, we are also concerned that any legislation to limit the use of pretext or access and use of the Social Security number in locating missing witnesses will impact traditional investigative techniques that are essential for conducting investigations in the private sector. There are far more investigations conducted by the private sector than by public law enforcement which generally obtains an exception to proposed legislation. And when budget constraints limit the areas of investigative concentration by prosecutors and law enforcement, victims, whether they are individuals or businesses, turn to investigative and security professionals to gather the necessary evidence.

Private sector investigations include insurance fraud, identity theft, employee theft and drug abuse, embezzlement, bank and accounting fraud, mortgage fraud, workplace violence and sexual harassment, trade secret theft, industrial espionage, asset searches, recovery of ill-gotten gains, elder abuse, child support, missing persons and locating heirs.

It is seldom possible to catch perpetrators in many crimes without some use of subterfuge. In many cases, a pretext may be simple and designed to merely identify a subject and confirm a presence. This is the case in most insurance fraud surveillances. In other cases, the subterfuge must be more elaborate where drugs or contraband are purchased, or in international counterfeiting and trademark cases.

We are very concerned that legislation banning the use of Social Security numbers will curtail our access to what is often referred to as the "credit header," that part of a comprehensive document used to locate missing witnesses, but contains no credit history. It is the quickest and most economical manner in ascertaining leads on the whereabouts of witnesses. In many instances it is the only means!

Without access to identifying personal information, it would be extremely difficult or impossible to solve many of these cases. In using Social Security number information investigators have on occasion located identity thieves and informed unaware consumers that their numbers were being used by others. In other cases this information has been used to help clear innocent individuals falsely accused of crime. In one such case, through the use of the "credit header", an innocent man was released from prison after serving 20 years! Some state regulators have regarded the work by licensed private investigators as quasi-law enforcement in nature. Investigative and security professionals, who are licensed and fully vetted, need continued Social Security number access to locate and properly identify individuals. They also must continue to be allowed to use pretexts, a recognized investigative technique.

Over the past decade Congress has turned its attention to identity theft, theft of intellectual property and crimes against children. In recent years they have sought to address financial fraud in the financial services industry, particularly mortgage fraud. Professional investigators play an

important role in helping to solve these crimes and are an integral part of the justice system. Our members are presently involved in conducting investigations in multiple cases arising out of the Bernard Madoff fraud. Limiting their ability to utilize recognized investigative techniques would severely curtail their ability to solve such cases.

Investigative & Security Professionals for Legislative Action will continue to work with Congress to address any concerns in this area. Our members assisted drafting the 1994 Drivers Privacy Protection Act exceptions for state licensed private investigators and security firms; testified before the Federal Trade Commission in hearings on consumer information privacy and database services which helped form the basis of the FTC's analysis of computer database services, testified before Congressional hearings, including the House Committee on Banking and Financial Services on Identity Theft and Gramm-Leach-Bliley Act Implementation and before the House Committee on Ways and Means regarding Social Security number use and privacy issues; and prepared written comments to the FTC regarding the roles of the SSN as an authenticator and identifier, as well as the private sector's use of the SSN in fraud prevention and identity theft for use by the President's Identity Theft Task Force.

ISPLA is available to lend further assistance regarding these issues to government legislators and regulators as well as testifying before hearings. It looks forward to being a valuable resource to other professional associations and stakeholders with these same concerns, and invites them to join our association. Professional investigators, certified fraud examiners, attorneys, forensic accountants, computer, digital, and other forensic experts, and litigation support services providers are invited to join as well. Membership information can be obtained by going to WWW.ISPLA.ORG.

Governance, Risk and Compliance: Unlawful Business Relationships

Barry W. Ryan
Information Network Associates, Inc.
Harrisburg, Pennsylvania

Introduction:

Little is published about compliance with the government requirement to screen and restrict business transactions with those individuals and entities that are classified as terrorists, terrorist-funded organizations or those otherwise posing a threat to the security of the United States of America. Executive management and boards of directors are now held legally accountable for a company's business transactions and operations and for compliance with government laws and regulations. There are long and short term severe penalties for failure of business to comply with a continuously evolving set of government standards. This white paper serves to explain unlawful business relationships, identify the applicable statutes and cite the repercussions for violators.

Office of Foreign Assets Control (OFAC):

The Office of Foreign Assets Control (OFAC) is a division of the United States Treasury with its roots being traced prior to the War of 1812. Since its inception, this organization has worked to advance the safety and international agenda of the United States using its enforcement powers to achieve its goals. By issuing embargos and sanctions and fining violators, OFAC attempts to stem the flow of cash to parties deemed hostile by the state and, through this, cripple their endeavors. These government measures apply to individuals, businesses, organizations or entire nations, classifying them as personas non grata in any transaction with US-affiliated entities. Typical recipients of this debarrement include terror-related entities, nationals of hostile countries, or entities connected to narcotics trafficking.

OFAC is the agency which has taken the primary lead in prosecuting violators. The judgments and settlements imposed have clearly established that the responsibility of compliance rests with the US affiliated parties transacting business. Although current legislation and regulations do not mandate a proactive screening process, OFAC imposes strict liability and harsh consequences when prosecuting perpetrators, thereby eliminating ignorance as an acceptable justification for offenses. While OFAC is the agency with the highest profile, there are other agencies with equal enforcement powers within the US Departments of Commerce, Treasury and State.

Legal Evolution:

The current structure of OFAC sanctions and enforcement are essentially based upon three federal legal actions. These are the Trading With the Enemy Act (TWEA), the International Emergency Economic Powers Act (IEEPA), and Executive Order 13224 (E.O. 13224).

Created originally in 1917, the Trading With the Enemy Act (US federal law, 12 USC. § 95a) is the oldest of the aforementioned documents. The TWEA enables the President of the United States to direct and control trade primarily during times of war. As of the date of this paper, Cuba is the only country with complete sanctions under the TWEA. North Korea is still subject to a bevy of trade barriers but had its total sanctioning lifted in June of 2000.

The International Emergency Economic Powers Act (Statute 1626, US Code Title 50, § 1701-1707) also granted powers to the President, but did not limit its primary scope to times of war. Rather, this legislation allowed the President to proclaim a threat to the nation based either primarily or exclusively outside of US borders. Upon enactment, assets and accounts may be frozen, seized, or confiscated. This act also provides congress a means to override the presidential declaration. Sanctions stemming from the IEEPA have been used against organizations and individuals, as well as against entire countries. The Supreme Court has traditionally backed the "broad scope" of the Executive branch under the IEEPA (Dames & Moore v. Reagan, 435 US 654) despite the congressional measures intended to limit these powers. In 2007, the IEEPA Enhancement Act (Public Law 110-96) sharply increased penalties for entities caught violating the IEEPA.

It should be noted that this legislation also grants power to the Bureau of Industry and Security. This government agency maintains its own listings of parties that US affiliated entities must seek explicit permission to export to. These lists are the Export Administration Regulations, the Denied Persons List and the Unverified List. Though different, these lists bear resemblance to OFAC lists in purpose, enforcement and power.

Executive Order 13224 was issued in the days immediately following September 11, 2001. Through this act, the President enabled the Department of the Treasury to wield his economic sanctioning power. By vesting the Treasury with this ability, a more complete and forceful execution of the IEEPA was enabled. This investiture primarily, but by no means exclusively, was done for the search and seizure of terror-related assets and, with this, the OFAC became fully capable of creating, maintaining, and enforcing the lists of sanctioned parties and individuals.

These three documents do not represent the entirety of legal documentation that supports the OFAC and its policies, but rather provide a general framework by which the operating system can be roughly gauged and understood.

There is a common misconception that OFAC's power stems from the USA PATRIOT Act (Patriot Act). This may be due to parts of the Patriot Act which updated the IEEPA and also may be attributable to the spotlight the Patriot Act shone on these heretofore relatively obscure regulations.

Primary Government Lists:

There are multiple listings of barred parties that are maintained by OFAC. Of these listings, there are two main types: country-based and list-based. The former serves as a blanket ban on conducting business with nationals, organizations, businesses or government entities relating to the offending state. Currently, the countries that fall under this jurisdiction are: The Balkans, Belarus, Burma, Cote d'Ivoire, Cuba, Democratic Republic of Congo, Iran, Iraq, Liberia/Former Liberian Regime of Charles Taylor, North Korea, Sudan, Syria, and Zimbabwe.

List-based compilations are composed of individuals, groups or businesses that are not tied down to a specific geographic area and must, therefore, be listed individually. Entities may be added to these lists for a variety of reasons; including being linked to terrorist causes, affiliation with diamond trading, narcotics trafficking, weapons proliferation, or undermining certain democratic institutions. All of these lists are lumped into a comprehensive single listing called the Specially Designated Nationals (SDN) list.

Both types of listings are dynamic and publicly available. Entities are constantly being added and removed, as deemed appropriate by OFAC. As an example, entries on these lists resemble the following:

"HUSSAIN, Saddam (a.k.a. ABU ALI; a.k.a. AL-TIKRITI, Saddam Hussein; a.k.a. HUSAYN, Saddam; a.k.a.

HUSSEIN, Saddam); DOB 28 Apr 1937; POB al-Awja, near Tikrit, Iraq; nationality Iraq; named in UNSCR 1483;

President since 1979 (individual) [IRAQ2]"

The following lists comprise the majority of those individuals and entities that are restricted from business transactions with our government and US persons and/or corporate entities. This information was extracted from their respective websites where more detail is available.

- *US Department of Commerce, Bureau of Industry and Security (BIS), Entity List*

  The Export Administration Regulations (EAR) contain a list of names of certain foreign persons, as well as businesses, research institutions, government and private organizations, that are subject to specific license requirements for the export, reexport and /or transfer (in-country) of specified items. These persons comprise the Entity List, which is found in Supplement No. 4 to Part 744 of the EAR. On an individual basis, the persons on the Entity List are subject to licensing requirements and policies supplemental to those found elsewhere in the EAR.

  The Denied Persons List consists of individuals and companies that have been denied export and re-export privileges by BIS.

  The Entity List consists of foreign end users who pose an unacceptable risk of diverting the technology of US Exports to alternate destinations for the purpose of developing weapons of mass destruction. Accordingly, US exports to those entities may require a license.

- *US Department of State Directorate of Defense Trade Controls,(DTC), Lists of Administratively and Statutorily Debarred Parties List*

  The entities and individuals listed on documents referenced below have been convicted of violating, or conspiracy to violate, the Arms Export Control Act (AECA). As a consequence, they are subject to "statutory debarment" pursuant to §38(g) (4) of the AECA and §127.7 of the International Traffic in Arms Regulations (ITAR). Thus, these persons are prohibited from participating directly in the export of defense articles, including technical data, and defense services. The names of these parties and their ineligibility for defense trade have been previously published by DDTC in the *Federal Register*. Statutory debarment remains in effect unless the debarred individual's/entity's application for reinstatement of export privileges is granted by DDTC. The notice of reinstatement will be published in the *Federal Register* and the individual's/entity's name is removed from the list.

  This search is a check against the US Department of State watch list for debarred parties. The DTC list identifies individuals and entities barred for convictions of violating, or conspiring to violate, the Arms Export Control Act (AECA). This search also includes individuals and entities administratively debarred for violations of the AECA and ITAR. These individuals and entities are potential threats to the security of the homeland.

- *US Treasury Department, Non-Specially Designated Nationals Palestinian Legislative Council (PLC) List*

  Section (b) of General License 4 issued pursuant to the Global Terrorism Sanctions Regulations (31 C.F.R. Part 594), the Terrorism Sanctions Regulations (31 CFR. Part 595), and the Foreign Terrorist Organizations Sanctions Regulations (31 C.F. R. Part 597) authorizes US financial institutions to reject transactions with members of the Palestinian Legislative Council (PLC) who were elected to the PLC on the party slate of Hamas, or any other Foreign Terrorist Organization (FTO), Specially

Designated Terrorist (SDT), or Specially Designated Global Terrorist (SDGT), provided that any such individuals are not named on OFAC's list of Specially Designated Nationals and Blocked Persons (SDN List).

- *US Treasury Department, Office of Foreign Assets Control (OFAC), Specially Designated Nationals and Blocked Persons List*

  The Office of Foreign Assets Control, under the US Department of the Treasury, administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security and economic foreign policy of the United States. OFAC acts under Presidential national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and freeze assets under US jurisdiction. The specially Designated Nationals (SDN) List is a publication of OFAC that lists individuals and organizations with whom United States citizens and permanent residents are prohibited from doing business.

- *US Department of Commerce, Denied Persons List (DPL)*

  The DPL list covers those persons from whom the US American Bureau of Industry and Security has withdrawn export privileges for an unlimited or limited period of time. Persons listed on the DPL are neither eligible to have delivery of goods of US origin nor delivery from multinational companies nor may the mentioned companies purchase goods from those on the list. It's irrelevant whether or not those goods are registered on the US American Commerce Control List (CCL). Any form of aiding and abetting to receive those goods or the supply of any services connected with US goods are furthermore strictly forbidden.

- *US Department of Commerce "Unverified" List, Bureau of Industry and Security (BIS) World Bank List of Ineligible Firms List*

  The Unverified List includes names and countries of foreign nationals who in the past were parties to a transaction with respect to which BIS could not conduct a pre-license check (PLC) or a post-shipment verification (PSV) for reasons outside of the US Government control. Any transaction to which a listed person is a party will be deemed by BIS to raise a red flag with respect to such transaction within the meaning of the guidance set forth in Supplement No. 3 to 15 C.F.R. Part 732. The red flag applies to the person on the Unverified List regardless of the country where the person/ entity is located.

Penalties and Impact:

The US Treasury has not mandated a proactive approach to screening potential debarred parties. In layman's terms, there is no penalty assessed for a lack of screening, in and of itself. However, when OFAC determines a US affiliated company has committed a violation in one or more business transactions, ignorance will not be accepted as a justifiable reason for doing business with a debarred party. If the offense is deemed civil in nature, then the agency employs a theory of strict liability. Criminal proceedings are different, in that they require a "willful ignorance"; however, case history indicates that failure to conduct appropriate background investigations has fulfilled these criteria. There is also no minimum monetary figure for a violation under the jurisdiction of OFAC. So, theoretically and while highly unlikely, a convenience store could be prosecuted for simply selling incidentals to a banned party.

The IEEPA is the primary legislation that is used to pursue most offenders. Prior to 2007, civil and criminal offenses incurred a maximum penalty of $50,000 per violation. Since the passage of the IEEPA Enhancement Act, civil offenses now start with the greater of twice the amount transacted or $250,000, and can reach up to $1,075,000 per violation. Criminal violations now carry a penalty of

up to $10,000,000 along with up to twenty years imprisonment. The actual sentence levied on violators is dependent on different factors; including intent, compliance programs in place, cooperation and creating an effective deterrence of future incidents., The US Treasury Department has established baseline amounts for punitive fines that rely primarily on two factors: nature of disclosure (self-disclosure versus involuntarily disclosure) and nature of offense (egregious versus non-egregious). Below is a simple schematic depicting the baseline punishment amount.

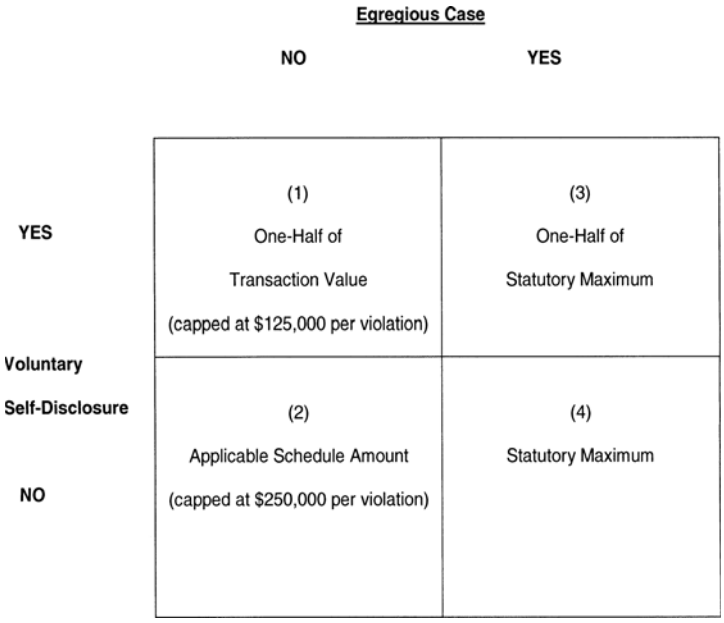

Image taken from Federal Register – Vol. 73, No. 174, 51940
Via
(http://www.ustreas.gov/offices/enforcement/ofac/policy/enf_guide_09082008.pdf)

In section (2) above, the diagram references schedule amounts, which is a previously established guideline put forth by OFAC and portrayed below.

Amount Transacted:
Penalty Levied:
Less than $1,000
$1,000
Between $1,000 and $9,999 (Inclusive) $10,000
Between $10,000 and $24,999 (Inclusive) $25,000
Between $25,000 and $49,999 (Inclusive) $50,000
Between $50,000 and $99,999 (Inclusive) $100,000
Between $100,000 and $169,999 (Inclusive) $170,000
$170,00 or greater
$250,000

Information transcribed from Federal Register – Vol. 73, No. 174, 51936

Beyond the monetary penalties ascribed by OFAC, violators will likely have to deal with public relations damage since offenses are publicly disclosed by the Department of the Treasury. Such a gaffe could easily be seen as 'aiding and abetting enemies' of the United States and could adversely affect a company in the marketplace.

The true short and long-term impact of barred party violations is very difficult to gauge. Possible considerations include loss of government contracts, suspension of approved vendor status, increased financial scrutiny from regulatory agencies, higher probability of investigative audits, and possible loss of CT-PAT status. The simple fact is that OFAC violations have a negative impact for any business. It is in the corporate best interest to understand the ramifications of "banned parties screening" and to proactively address the issues before a violation unwittingly occurs and sanctions are imposed.

Maintaining Compliance:

The breadth of these sanctions is both their bane and their brawn. Keeping track of these constantly evolving lists and cross-checking them with all parties related to a business can be quite a daunting task; however, we as citizens recognize the necessity and nobility of it.

The most up-to-date versions of these lists can be found on the website of the US Treasury in both spreadsheet and text format for public use. These listings are commonly searchable for exact matches using simple word processing tools, but this method will only yield exact results. For instance, in the previous listing excerpt of Saddam Hussein, a search conducted on "Sadaam Hussein" would not yield "a hit." This means that, even though a search was executed, if business was conducted with a banned individual, in spite of its due diligence, it could be subject to OFAC penalties because of the application of strict liability.

Arguably, the best approach a business can take to minimize the risk of OFAC violations is the utilization

of a preemptive screening program. Whether this is done in-house or contracted out, the establishment and employment of a proactive research plan will help to limit transactions that are contrary to the current US embargos and sanctions. Furthermore, these measures would certainly help a company that is already under scrutiny for illegal or other regulatory transgressions perform damage control. Any violations would be more likely to qualify as 'non-egregious' if there is an established and documented screening process in place by the company in question. In addition to significantly decreasing any monetary penalties, such processes would help classify all violations as accidental instead of malicious, a valuable difference with regards to sanctions and public opinion.

Proactive Screening Options:

In order to employ a preventative screening program, one of two distinct paths may be chosen. The first is conducting the screening process with internal staff while the second is outsourcing the program to a third-party vendor.

In-House Screening: For some companies this may be this preferable option. However, it requires staff expertise; being informed and continuously updated on applicable legislation, complying with legislative and administrative updates, updating all the relevant listings, being well-versed in identifying possible matches and possessing the analytical resources to determine the accuracy of a potential positive match. Once again, all transactions conducted by a business are subject to OFAC compliance, necessitating continuing education on the evolving laws and administrative rulings.

Another factor to consider is plausible deniability. If screening is conducted within a company, any incurred violations could be seen as a deficiency, short changing the screening process, or even the aforementioned "willful blindness". That being recognized, an internal screening process may still be the most efficient approach for a business entity because full control of the process is internally maintained.

Outsourcing: There are a number of benefits for relying on a third party to conduct screenings on current or potential vendors. Perhaps the most obvious of these benefits is both cost and convenience. It may be much simpler and less time-intensive for a company to transfer a listing of business affiliates than it is to carefully filter this list and update software programs and match them with continually changing government lists of barred parties. Another benefit is the plausible deniability of blame should a barred party be inadvertently engaged as a vendor. A company would quite reasonably assert their efforts merit a 'non-egregious' label on any offenses and, furthermore, posit that any errors or oversight originated from a source outside of their immediate control. This last factor is crucial in minimizing any public relations damage or mitigating loss of business.

Outsourcing Considerations:

When seeking to outsource compliance screening, there are several factors to consider. First and foremost is the scope and integrity of the services to be performed.

- Does the provider understand the scope and nuances of compliance, the legal implications, the administrative client issues, and the driving purpose of this program?
- Is the provider knowledgeable about minimizing risk through proper documentation of processes and records?
- Will the provider resolve the names with "hits" or will this entirely be a company responsibility?
- Does the provider utilize simplicity and clarity in its method of operation?
- Will the company provide its internal list to the provider, or will it access the provider's database and conduct a self-examination search?
- Are prices clearly stated or are there uncertainty on the pricing issue?
- Will the available screening service conform to the needs of the company or vice versa?
- Is the program easily understood and manageable?

Service fees should be understood and reasonable. This consideration should also apply to procedural documentation. A well-qualified screening service is open and flexible about its procedures so that all parties involved fully understand the coverage and liabilities and can utilize the services that conform to business operations. Another consideration is the quality of service. Top-tier services will fulfill the needs and expectations of the customer, enabling them to focus on the management of their core business and not divert excessive overhead expense to be government compliant. The quality of service also plays a key role in risk mitigation. Quality

screening services will help to mitigate punitive exposure while marginal services may not fulfill compliance requirements. Knowledge, clarity and service are valued in any business but, when dealing with potential OFAC violations or barred parties screening, these factors can reduce a company's risk exposure.

Conclusion:

Aside from government sanctions, with narcotics trafficking and international terrorism in the foreground, it is prudent to take proactive measures to do business with law abiding partners. Mitigating risk to safeguard corporate assets and to assure continuity of the supply chain is critical in today's global economy. INA has been a leader in corporate due diligence since 1982. If you have questions on barred party screening or if you need further clarification on any issues, contact INA at 1-800-443-0824.

How Investigators Tracked Down a Modern Warfare 2 Cyber Pirate

"A Tribute to Rob Holmes"
IPCybercrime
Dallas, Texas

The posting last Thursday on Craigslist was alarming. Someone was selling a Modern Warfare 2 Xbox 360 bundle, with both a console and a game, for $500. The problem was that Modern Warfare 2, one of the most anticipated games of the year, doesn't officially go on sale until Nov. 10.

Activision Blizzard, the game's publisher, called in IPCybercrime.com, a Dallas private investigation firm that specializes in online investigations. The investigators tracked down the seller and stumbled into a scheme to pirate the game and sell a bunch of fake copies over the Internet. While the bust led to the arrest of just one hacker among many, it sheds light on the shadowy underground of the business of illegal piracy. It also offers a peak at how investigators try to head off a major piracy disaster before it happens.

"It all happened very fast," said Rob Holmes, owner of IPCybercrime. "If these guys get their stuff out, then they can do some major damage to sales and spoil it for everybody. We plug leaks every day, but this was one of the biggest ones of the year."

The investigators started by calling the Craigslist ad phone number and talking with the seller, who said he had two items for sale. They negotiated a deal to buy two bundles for $800 each. Then IPCybercrime dispatched its investigators in Los Angeles to perform an undercover pickup. Then another Craigslist ad appeared for the same Modern Warfare 2 bundle. A search on social networks revealed that the first seller was a friend of the second seller. And the second seller said on his social networking page that he worked as a "box boy at a major retail chain."

IPCybercrime's client, Activision Blizzard, approached the sellers, who then admitted having stolen a crate of the bundles from the backroom of a game retail store. Then IPCybercrime folks turned the case over to the loss prevention department at the retailer, which dealt with the thieves. This kind of inside job involving physical theft is becoming common, though it's hard to do because retailers get a major game just a week in advance and then lock the boxes up in a high-security part of their warehouses.

On Oct. 30, the client told IPCybercrime that an individual going by the name "cedelamo" and "cdelamo815" had posted a message on the piracy forum at xbox360iso.com. The post asked for users to donate funds to him via PayPal so that he could buy one of the above-listed Craigslist bundles and crack the anti-piracy code. Once he did that, he could distribute counterfeit copies of the game widely and make a bundle of money doing it.

There wasn't an obvious way to track the person who made the post. But IPCybercrime checked on Facebook to see if the email address belonged to someone with a Facebook account. The search turned up a page for someone who was anonymously offering "modding services." Modders are people who hack into Xbox 360 systems and turn them into repositories for pirated games. They stand in a gray area of the law, as it's legal to make your own backup copy of a copyrighted disk, but it's not OK to sell that copy commercially. To evade the law, the modders often describe their services in ads as selling "backup disks."

The Facebook page had a cell phone number and it said that customers could contact that number via text message. Holmes' investigators stayed in contact with the person sending text messages for four days as they negotiated a business deal. At

one point, they convinced the person to call them with a cell phone. Holmes called that number back and then managed to get a business address out of the person.

Meanwhile, the person on the web forum said that he had received a copy of Modern Warfare 2 on Oct. 30. Over the weekend, the hacker went to work on the copy protection built into the DVD disk with the game on it. He cracked the code — something that isn't that hard for hackers to do these days — and announced that he had done so on Monday. Coincidentally, pirate digital copies of Modern Warfare 2 flooded onto torrent sites, which are peer-to-peer sites for sharing software, on the same day. That has likely caused untold losses for Activision Blizzard, Holmes said.

Holmes was looking into the business address he got from the Facebook modder. The location was a computer business in Miami, owned by the subject's father, Hiram Del Amo. IPCybercrime sent an investigator to the address and then determined that the cyberhacker was Christian Del Amo, an 18-year-old who was known as a modder and had a site for selling modded Xbox 360 hard disks on iOffer.com, an eBay-like site. The modder advertised 250-gigabyte Western Digital hard drives, loaded with 125 hacked games, for $150.

IPCybercrime handed the case over to the Miami-Dade police department. They conducted a buy-bust sting where Del Amo had sent a "runner" to make the exchange. The runner gave them a disk with the Modern Warfare 2 limited edition image on it. That meant that not only was Del Amo making pirated digital copies on DVDs, he was also sophisticated enough to know how to make disks that look like legitimate copies. On his Twitter account, Del Amo was in a conversation with an underground hologram maker. Holograms can be used to make the disks look like legitimate copies of the game. Those who bought the pirated game would be able to play it in modded Xbox 360s.

"This kid was in a position to sell thousands of these," Holmes said.

Police interrogated the runner, who led them to Del Amo's home. They then arrested Del Amo yesterday. Del Amo's attorney has not returned a call for comment. The whole process, from finding the first tip to the bust, took less than a week. While the operation snagged a perpetrator, it didn't move fast enough to prevent the massive copying of the game on the torrents on the Internet.

"Hopefully it is a lesson," said Holmes. "If you try to do piracy on a large scale, you will get caught. When you use the Internet, you always leave tracks somewhere."