INTELLENET *News*

Official Newsletter of the
International Intelligence Network, Ltd.

Intellenetwork.org *Spring 2013*

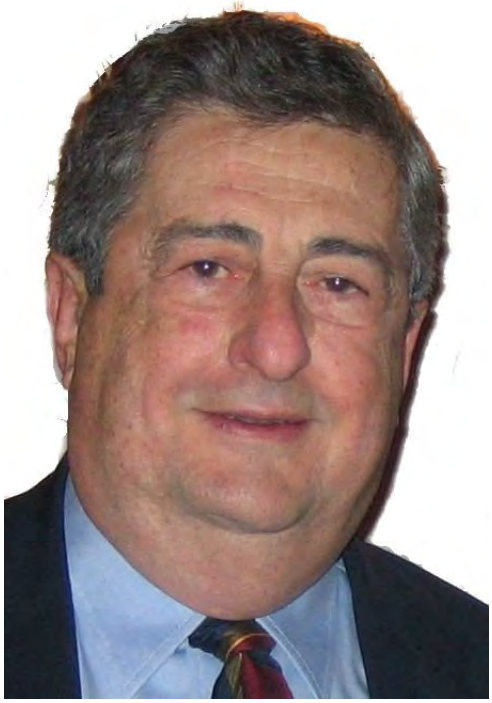
Special 30th Anniversary Issue!

Celebrating Jim Carino and the Founding of Intellenet

in Philadelphia at the Sheraton Society Hill, 24-27 April 2013

Details at www.IntellenetAGM.com

In this Issue ...



Carino's Corner

by

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

"The End of the Beginning"

***As* has been announced, after 30 years of serving as Executive Director I will be stepping down at our 30th Anniversary Conference in Philadelphia, 24 – 27 April 2013.**

From our humble beginnings of 25 members (all AFOSI) in 17 states, Intellenet has grown to over 450 members in virtually all states and almost 60 other countries.

It has been said that life is a journey and this Intellenet journey of 30 years has included visiting many countries with meeting and getting to know the finest investigators and security professionals, not only as colleagues but also as friends.

The decision to step down was a difficult but sensible one. It was difficult in the sense of "surrendering" a passion, but it was sensible by ensuring the continuation of Intellenet as a vibrant association, one that is more akin to family. And, just as families continue with the passing of the baton, so to speak, from parent to child, so must the leadership of Intellenet be passed in a logical and planned manner to ensure its continuation in perpetuity.

The growth of Intellenet from its infancy in 1983 to maturity in 2013 was accomplished by many individuals over the years, including quite a few who have already left us. It would be impossible to list all who share so much with me in this journey, but I would be remiss in not citing Brad Penny as the first among many equals and peers. Brad was my good friend and colleague in our Air Force OSI days in Italy, beginning in July 1961. Brad left us in 2009 but his spirit continues to serve as a motivating force.

As I close out 30 years of Intellenet as the Executive Director, my deep gratitude and thanks go to the Board and to all our members, past and present, who have made this part of life's journey filled with so many great memories.

Now let's proceed to the next chapter. I feel confident that Intellenet will provide a rich and rewarding experience and continue to grow and flourish for our members and bring personal joy and satisfaction to me for years to come. The transition comes only after in-depth succession planning. My hope and expectation is that all will continue to support Intellenet and my successor as you have me through the years.

"Thanks to you all for a great 30 years."

♦♦♦

The following profile of Jim Carino appeared in the Nov-Dec 2005 issue of *PI Magazine*, published by Intellenet members Jimmie and Rosemarie Mesis , who graciously allowed for a reprint of the article in *Intellenet News*. The profile was written by Intellenet member Kitty Hailey, CLI, and your editor had the honor of serving as editor of PI Magazine at the time. (As you will note, the spelling of Intellenet has changed since this article ran. There's a history to that story, not told here …)

Jim Carino - Living His Life's Work

Profile by
Kitty Hailey

"The problem with doing nothing is not knowing when you are finished."

Nelson DeMille in 'Plum Island'

"There are two types of people in this world. It's either us or them. Us is everyone connected with law enforcement, investigations, military intelligence, special investigations, etc. Them is everyone else." That's what Jim Carino has to say about his world. He's a man who lives by his convictions.

This unassuming, dignified gentleman is a living-breathing example of a professional committed to doing what he knows best. He's former Director of Criminal Investigations, Air Force Office of Special Investigations with command experience on both U.S. and foreign soil. With several decades of military and civilian experience, he's a man on the move who thrives on getting the job done. For the last twenty years he has served as head of Executive Security Consultants (ESC) specializing in conducting security surveys, training and major investigations for an impressive clientele. Still very active in his business and frequently appearing as an expert witness in complex civil litigation cases, Carino just can't seem to keep his fingers out of several other pies.

For example, he is currently serving as President of the Pennsylvania Association of Licensed Investigators (PALI), is on the board of the National Council of Investigative and Security Services (NCISS) and a member of the Vidocq Society, an association based in Philadelphia that specializes in solving cold cases. That's in addition to being founder and executive director of one of the world's most prestigious private association of investigative and security specialists, the International Intelligence Network (INTELNET). But that's a whole story unto itself.

INTELNET has the auspicious privilege of being host to approximately 350 members worldwide. INTELNET members are handpicked by Jim Carino to fulfill a need for exceptional investigative talent in prime geographic locations. The goal of this rather unique association is to bring together the brightest, most experienced and established investigators and security consultants in the world to network their ideas, information and services. INTELNET started with a core group of 25 people from OSI backgrounds who were all retired and working in the private sector. Carino realized early on that the work demands of the "real world" differed dramatically from the rank and file of military intelligence and criminal investigations. The rules were different on the streets stateside than they were in Italy, where he was based for so many years. He was intelligent enough to know what he didn't know. He was also smart enough to understand that he was not flying solo on this trip. So he brought together these former military types who were engaged in a second profession. By helping each other, sharing ideas and filling in the blanks for one another, they were all soon at the top of their game. What better staff to boast than 25 former intelligence and investigative agents with knowledge of everything from security to counter-terrorism. And the INTELNET family has grown considerably.

The makeup of INTELNET has expanded with the organization. Members with backgrounds from other military and government intelligence agencies soon swelled the ranks. They were followed by investigators representing a huge variety of disciplines. A pre-

-requisite of ten years experience in the investigative field insures that members have mastered the art of running and maintaining their own investigative businesses. INTELNET now boasts one of the most brilliant mind-trusts of talent ever assembled.

Carino understands the value of sharing. “Far too often I hear investigators complaining that they don’t want to go to meetings or seminars because ‘someone will steal’ their clients.” He quips, “These are the same people who never learn, never get business and starve to death.” He is ecstatic when he proclaims that he has multiplied his value 350-fold because of his INTELNET concept. That’s 350 times more brainpower, more resources and more connections for future work. INTELNET seminars -- held at locations around the world -- boast an average of one-third membership turnout. That in itself is incredible in a world where it’s difficult to get 50 investigators together for a state seminar.

Jim and Connie Carino
New York City 2008

There is a dignity about Jim Carino that is apparent the moment he walks into a room. He has a commanding presence that no doubt dates back to his stint as an accredited instructor at Alvernia College at Andrews Air Force Base in Washington, D.C. teaching OSI tactics. He’s like a magnet that attracts people by his very presence. Ten minutes after entering a cocktail party at a seminar he is surrounded by friends, colleagues and those who wish to be. Carino never gets loud, never makes demands, but firmly and confidently controls every discussion in which he participates.

Who would have thought that this dynamic individual wanted to be a garbage man at age three? Or that his early interest in cowboys and crime movies would propel him to become such a patriot and protector of our rights. He jokes that if he had had enough talent, he was truly destined to be a professional trombone player. Although he sat first chair throughout his school days, including college, and was a member of both dancing and marching bands, he recognized the limits of his musical talent in enough time to provide the rest of us with some sorely needed leadership.

At heart he’s just a family man who still loves his wife Connie with fierce intensity after several decades of marriage. He boasts of her accomplishments before he will even mention his own. These accomplishments are nothing to ignore. Connie Carino is Clinical Director of Psychiatric Nursing for the Hospital of the University of Pennsylvania. She is the recipient of the most coveted Gimbel Award (1996) following in the footsteps of the likes of Eleanor Roosevelt and Amelia Erhart. She is also the mother of their son and daughter and shares grand parenting rights with Jim for four fabulous children. In short, she’s a match for the wit, intelligence and accomplishments of her well traveled and super experienced mate.

Carino has learned to “turn it off” when he needs to. In spite of juggling four offices of responsibility with investigative associations and running a very lucrative business, he still finds time to sit on his deck at the Jersey shore and enjoy the sights and sounds of the aviary population in the bird sanctuary next door. It’s a calming respite that is well earned. Someone once asked him what he did for a hobby. To Jim Carino, life is a hobby and he enjoys it all. ♦♦♦

Member News

Welcome New Members …

These are our newest members since we last published. You should have seen their mention in one of Jim's *InfoBriefs,* or their own "e-introductions" subsequently. If we missed a name in this issue, we apologize. Let us know and we'll mention you in the next issue. Welcome one and all to the premiere network of investigative and security specialists. Hope to see you in Philadelphia.

- Bill **CLUTTER** (Springfield, Illinois)
- David **CUFFEE** (Stroudsburg, Pennsylvania)
- Marcus **TAN** (Vietnam)

Members in the News …

Congratulations to **Erick J. Flores Machado, CPP,** who recently became vice president of the Security Committee of the Venezuelan-American Chamber of Commerce, an honor he also holds for the British-Venezuelan Chamber. Erick is spokesperson for the Caracas chapter of ASIS.

Likewise kudos to **Patricia Shaughnessy** of Phoenix, who is now a certified Confidential Intermediary for the Supreme Court of Arizona, authorized to conduct adoption searches (natural and adoptive parents and siblings).

Susan Daniels of Chardon, Ohio, was personally responsible for proving a case against an attorney gone bad. Susan's pro bono work for a client who had been cheated by an attorney resulted in the Ohio Supreme Court finally "bringing the hammer down on him." Susan's investigation showed that the court had failed to act on numerous prior complaints against this attorney. They had not previously had the benefit of Susan's due diligence.

Intellenet member, retired federal special agent and current private investigator **David L. Ziegler, CFE, CFI** has combed through thousands of available smart phone apps in search for the select few which are invaluable to the modern, tech-savvy private detective or law enforcement professional. You will find information, resources and links for these special apps on his new website, www.appsforinvestigators.com.

♦♦♦

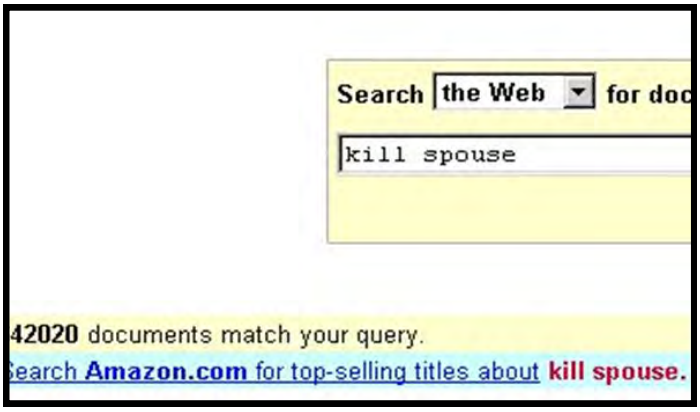
Finding Clues in Computers: Managing the Computer Forensic Process

By Gordon Mitchell, PhD

Everyone with a television knows the magic of CSI. It's possible to instantly identify, investigate and incarcerate crooks while protecting, empowering and encouraging the innocent. Well, almost …

CAUTION: This article includes adult language (computer words). If they are unfamiliar, consider www.wikipedia.org/ your friend .

The business of computer forensics really does have some of the investigative magic one might expect in today's technology era. Some cases are complicated but others have answers jump out. One of my favorite experiences was presenting a defendant's web searches to a murder trial jury. It didn't take much explaining when the following slide appeared.



Not all computer forensic activities are that clear. Often most of the effort goes into explaining subtle things to an attorney, to a judge and to a jury. Civil cases almost never get to trial so the most exciting event is a deposition.

Procedures for our work have changed. In the '90s we told first responders that the first action is "pull the plug." Now it is important to obtain live information from a computer that can identify network connections, malware running in RAM, and other evanescent conditions. The employee termination checklist that we give HR people illustrates this sort of *newthink*. It focuses on the computer used by the employee but also identifies external resources. Today's checklist for termination:

1. One week before termination make a forensic image of the computer hard drive and a live capture of RAM. *Caution: Most IT techs do not have the hardware or experience to do this properly.*
2. Ask IT to make sure that logging for all web activity is enabled.
3. Save copies of email files and stored files from servers.
4. Identify all network access that will need to be terminated. This can include external logins at the bank, partner organizations, ISPs, etc.
5. At the time of termination remove the computer from service, a forensic clone of the hard drive can allow continued use without overwriting critical files.
6. Collect information that would otherwise be lost. This includes phone and cellphone logs, physical access control activity, security camera video and computer network DHCP and proxy logs.
7. Safeguard the collected information by getting signed statements from those who collected the images and logs. Store all material where it will be safe from tampering.

Continued next page

This list may be just too much for many situations. If an employee departs to a non-competing business we recommend a much shorter list:

> *When the employee is leaving ask that business-critical files be copied to a server; then remove and store the computer hard drive.*

This simplified procedure can pay big dividends when the unexpected wrongful termination suit comes two years later. *Allowing the computer to be reused guarantees that information will be lost*. This happens in the normal overwriting process used by the hard drive.

If it is necessary to analyze a computer image the critical first step is to define exactly what the goals are. Sometimes clients ask us to "just figure out what is there." This could become full analyst employment for the next year. Modern computers have such large hard drives that a random or linear search is not practical. Even carefully crafted keyword searches can yield over 100,000 hits. This makes it critical to focus the investigation. Some questions at the outset can help this process, get better results and control costs. For example:

- In embezzlement cases – do you have copies of fraudulent documents that contain useful search terms?
- When trade secrets are stolen – can you give me a list of competitors' domains and personnel information?
- If threats are made – are exact texts available? The goal here is to focus the work and get results quicker. In one case that we worked the death threat mistakenly use a synonym of the grammatically correct word. Simply searching for that error in a computer quickly identified the suspect.

Once computer forensic work begins it is critical for the analyst and client to keep in touch. A complex final report delivered without consultation will almost certainly be off topic. In most cases this requires sitting down to review evidence for a few hours once initial analysis is done. It allows the analyst to ask questions and can prevent obvious mistakes. It is, however, important to not allow these consultations to become opportunities for the client to push their opinions into the report.

Welcome to the adventure. Enjoy the process and expect that it will help your investigations become more focused and accurate. ••••••••

Protecting Your Computer from the Internet
and
Protecting the Internet from Your Computer

By Gordon Mitchell

It's easy to believe that life would be easier if we all had the expertise of a sharp computer network geek. Downtime would disappear and threats would melt away when exposed to our skills.

Fortunately, it isn't necessary to be that good to take a big bite out of today's threats. Following some easy-to-do suggestions can make it lots less likely that disaster occurs. The motivation to prevent computer system problems is immense. Most local and national governments have laws that mandate disclosure of data losses from computer systems.

Continued next page

Let's assume that each week you work a case with one principal and 10 suspects. After 10 years personal data from all these folks adds up to more than 5000 computer records. If there is a breach you will be required to notify all of them – yes, even the people you have investigated. Some jurisdictions require that you also remediate the damage. The cost per record is often estimated at between $100 and $200. Who has $50K to spare?

There are two answers to this dilemma. First, all personal data on hard drives should be encrypted. Many disclosure laws don't apply if the data was encrypted. The second answer is to make compromise of the data less likely. It's not hard to make a great improvement in computer network hardening.

Microsoft's recent report www.microsoft.com/security/sir/default.aspx explains that 43% of malware spreads by abusing the autorun feature in CDs and USB devices. This is easy to fix. Just run a small file which fixes the registry and prevents the "convenient" automatic running of files when one of these devices is put into computers. See the solutions part of www.us-cert.gov/cas/techalerts/TA09-020A.html or write to me for a copy of the file.

Another 45% of malware propagation is from user interaction (user stupidity). It happens. Here are the best steps for preventing these problems.

Set your email viewer to only show the subject, sender, etc. Don't display complete messages until you have deleted the suspect emails. View suspect message header information to help in this process. Beware, just because an email comes from aunt Mary doesn't mean it's clean. Maybe aunt Mary's computer just got "owned" by an intruder.

Use a good antivirus product to catch incoming malware. My current favorite is from www.eset.com/business/products/smart-security/.

Use an up-to-date browser. That will help to catch links that are bad. I like Google Chrome because it runs downloaded programs in a sandbox that protects the computer.

Use a Domain Name System service like www.opendns.com/ to prevent going to known bad web sites. These guys have saved my bacon several times.

The pain of spam can be reduced by using disposable email addresses. A disposable email address that is getting lots of spam can be easily turned off if it is being misused. This is lots easier than changing one's "real" email address. Use one for web purchases, another for relatives and the rest for banks, etc. Look at the heading of this article and see if you can figure out my disposable email address scheme.

Another effective way to avoid disaster is to use a different long complex password for each website login. It's easy to manage a system like this with a free password program like http://sourceforge.net/projects/passwordsafe/. Older computer software is more vulnerable. Upgrade to Windows 7 or Mac OS X.

An interesting advantage of all these security hardening ideas is that your computer will be lots less likely to be the one that passes malware to clients. That's always a good idea. ♦♦♦

Gordon Mitchell has a PhD in Electrical Engineering with the usual certifications CPP, CISSP, GICH, GPEN, GSEC . He has worked in the U.S. Government, for huge companies and high tech startups. Now he runs Future Focus, a company in the Seattle area which provides sweeps for bugs and computer forensic services. Gordon has been on the Intellenet D-List for a long time. He can be reached by email at webresponse05@tempaddress.com, by phone at (425) 489-0446 and on the web at www.eSleuth.com.

ISPLA Report

by Bruce Hulme, CFE

Since my last column for this quarterly newsletter, I am pleased to report that no adverse federal legislation was enacted during the past two-year session of the 112th Congress. ISPLA will continue in its prime mission of lobbying against ill-conceived legislation and regulations at the federal level during the 113th Congress and, when requested, assist our member state professional associations in addressing issues of mutual concern.

This ISPLA Report to Intellenet members will cover additional some of the concerns of proposed recent gun control legislation, about which I commented upon in the last issue relative to the mass school shooting at the Sandy Hook Elementary School in Newtown, CT, the presentation of ISPLA's first "Legacy Award" and an item based on an article by Daniel Hood -- "Dispatches on the War on Fraud."

New York SAFE Act...

Recently enacted gun legislation in New York has presented concern to members of the Associated Licensed Detectives of New York State. It also has implications for investigative and security professionals in other states and potentially will affect some members of Intellenet. What follows is a report I gave to members of ISPLA which the reader may also find of interest. In the dead of the night, without hearing or input from those groups concerned with protecting the public, property and the interests of their clients, New York Governor Andrew Cuomo rammed through gun legislation.

New York's recently enacted Secure Ammunition and Firearms Enforcement Act of 2013 (SAFE Act), was poorly crafted and rushed through the state legislature by Governor Cuomo in the dead of night. It will cause a number of unintended consequences. It should be repealed now!

The Bushmaster used in the school shooting in Newtown, CT would be illegal. Armed police responding to any similar tragedy that in the future might occur at a school in New York would be violating law under this hastily drafted SAFE Act.

There are defects in the bill with reference to amendments in the Penal Law. For example, police officers would be violating this law if they were armed while entering a school without prior written authorization. That would include any armed first responder entering upon school property.

In part, the SAFE Act bans all pre-1994 high capacity magazines and any magazine that can hold over 7 rounds (down from a limit of 10, the number called for in one of President Obama's recent 23 executive orders). It requires "real time" background checks of ammunition purchases in order to alert law enforcement to high volume buyers. Universal background checks are required of all gun transfers between private parties, except those within the immediate family. The Act outlines a stricter definition of assault weapons. Weapons owned prior to the effective date may be grandfathered and registered within one year and then recertified every five years.

PBA associations in the City of New York are already lobbying for their own chapter amendment to in-

Continued on next page

-clude an exception for retired NYCPD officers to be exempt from Governor Cuomo's bill.

The Associated Licensed Detective of New York State (ALDONYS) is seeking a chapter amendment for an exception of the seven round magazine limit for NYS licensed private investigators and registered security guards under General Business Law Sections 7 and 7A. Several members of ISPLA, including me, also serve on ALDONYS' board and assisted in the preparation of document.

However, ISPLA believes the most responsible course of action is outright repeal of this ill-conceived legislation. In a landmark U.S. Supreme Court case it was members of the current ISPLA leadership who worked to file an *amicus curiae* brief in the defense of a security officer in the matter of District of Columbia v. Heller. That 5-4 Supreme Court decision affirmed that the right to self-defense is an individual one under the Second Amendment. Governor Cuomo and members of the New York state legislature took an oath to uphold both the state and U.S. Constitutions.

ISPLA supports full repeal and should such efforts fail, accept full enforcement. For when the legislature passes laws under the cloak of darkness without hearings or public comment, there should be no negotiation to peel back the layers of their rotten deed. Either everyone lives with the foul stench of the government's acts, or the whole thing is thrown out.

Neither ALDONYS members, nor any other special interest groups, will likely support full repeal. It's not in their self interest — yet another sad display of NIMBY (not in my back yard). "The legislation is fine, so long as it doesn't apply to me...." So active police want an exception. Retired cops want an exception. Security guards and private investigators want an exception. Anyone who already has one of the banned firearms / clips wants an exception. Those with the strongest lobbying pull might get protected. Meanwhile the average person gets sold out. Almost all of the groups will complain about protecting Second Amendment rights, but in the end, they are willing to sell their professed rhetoric about constitutionality for an exception for themselves.

"...For when the legislature passes laws under the cloak of darkness without hearings or public comment, there should be no negotiation to peel back the layers of their rotten deed. Either everyone lives with the foul stench of the government's acts, or the whole thing is thrown out."

Gun legislation throughout the U.S. is more expansive than President Obama's 23 Executive Orders at the federal level. State initiatives include expanding the 1993 list of banned semi-automatic weapons, banning magazines that can hold more than 10 rounds (7 in New York), instituting criminal background checks, including guns sold between private parties and at gun shows to curtail "straw buyers," licensing rifles and shotguns, banning the possession of body armor by civilians with an exclusion for military and law enforcement, creation of a "Gun Offender" registry for individuals convicted of gun crimes, prohibiting the purchase of more than one firearm in a 30-day period, mandating $1,000,000 liability insurance for owners and permit holders of firearms and implementing a 50 percent sales tax on ammunition.

In addition, legislation has been offered in states to make public the identities and personal information relating to owners and holders of concealed weapon permits and registrants of firearms, as well as the legislation having the opposite intent -- the sealing of such information. Along with the above are proposals relating to mental health directives and reporting as well as pressuring video game manufacturers to reduce the depiction of violence and limiting violence in the media and entertainment fields. These topics have privacy and First Amendment concerns. All of the rest have Second Amendment implications. ISPLA will keep you advised of further developments.

ISPLA'S "Legacy Award" Presented to ALDONYS...

At the ALDONYS Biennial Person of the Year Award held on March 8 at the Sheraton New York in Manhattan, I was privileged to present ALDONYS with the first *ISPLA LEGACY AWARD*. Initially it was to be presented in November 2012. However, the event was cancelled at that time due to the aftermath of Hurricane Sandy and postponed to March 2013.

ALDONYS was one of the first state professional associations to support the efforts of ISPLA's founders to create a professional association dedicated solely to addressing legislative and regulatory matters of concern to investigative and security professionals. The significant financial contributions and strong support received by ISPLA from ALDONYS since ISPLA's formation in 2009 has been greatly appreciated. Of equal importance have been the individual members of ALDONYS who have joined ISPLA, including their present officers: President Mario Doyle, Vice President Security Lisa Dolan, Vice President Investigation Gil Alba, and Treasurer Thomas Ruskin.

ISPLA was pleased to take part in the ALDONYS event which honored "The ALDONYS Person of the Year" to New York State Senator Greg Ball; John "Jack" Goldsborough, recipient of the "Eugene Fink Award"; and ISPLA member David E. Zeldin, recipient of the "Investigator of the Year Award."

Dispatches on the War on Fraud...

Private and corporate investigators and security professionals are not the only private sector fields concerned with fraud. Intellenet members (as well as ISPLA members) also include attorneys, Certified Public Accountants, digital forensic investigators, and Certified Fraud Examiners. Fraud investigators may have a number of forensic related credentials, including the American Institute of CPAs' Certified in Fraud and Forensics designation, the American College of Forensic Examiners' Certified Forensic Accountant and the Association of Certified Fraud Examiners' CFE designation. As a CFE, I have served many years as legislative liaison and board member of the New York Chapter of the ACFE. In recent years ISPLA and I have worked with that chapter's president, Alan Blass, who is quoted below and from whom permission has been granted to publish much of the information relating to fraud below.

For those looking to protect their clients -- or themselves -- from fraud, Randy Wilson, a CPA, certified fraud examiner, and partner and national director of fraud and fidelity services with RGL Forensics, has a sobering warning.

"Fraud can't really be prevented. You can try to detect it early or in the normal course of business, but you can't prevent it in its entirety …

… The average business owner doesn't know the magnitude of fraud and they don't realize it could be siphoning off funds for decades."

Randy Wilson, CPA, CFE

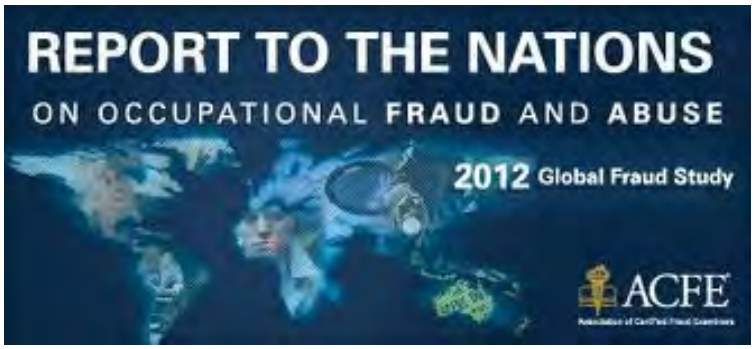
"Fraud can't really be prevented. You can try to detect it early or in the normal course of business, but you can't prevent it in its entirety."

Wilson is not suggesting that companies give up, or just resign themselves to fraud -- instead, he wants them to take a more informed approach to the subject, and he wants accountants to help. "Business owners just don't know what the risk really is. One thing accountants can do is to educate clients about the potential for fraud," he said, noting that the Association of Certified Fraud Examiner's authoritative annual *Report to the Nations* on fraud estimates that 5 percent of business revenue around the world, or approximately $3.5 trillion, is stolen through fraud every year. "The average business owner doesn't know the magnitude of fraud and they don't realize it could be siphoning off funds for decades."

One area they specifically need to be educated on is the protective value of an audit: "I'd like to let people know not to rely on an outside audit or review or compilation as a protection against fraud," Wilson said. "If you're going to have a system to detect fraud earlier, it has to come from the company. Too often, I hear business owners say, "I thought my

auditor was looking for fraud,' but no, they're not. Accountants do themselves a disservice when they don't make it clear to clients that they're not looking for fraud."

That may be a disservice, but there's a service opportunity there, according to CPA and CFE Alan Blass, the director of Fuoco Fraud and Forensics LLC, part of the New York- and Florida-based Fuoco Group: "Most companies in need react by bringing in a forensic accountant to quantify the fraud and, if possible, retrieve lost funds," he said. "Too few privately held small and midsized companies proactively hire a forensic accountant to review and test internal systems and controls before a fraud occurs. Often a relatively small and inexpensive system, control, accounting or reporting change could avoid the fraud or accelerate its detection" -- and a qualified accountant could help their clients by identifying the needed changes.



"More companies are [having] anti-fraud prevention assessments" performed by outsiders, Blass said. "It's money well-spent. It's tough for companies to analyze themselves."

John Warren, a CFE and vice president and general counsel of the Association of Certified Fraud Examiners, offers advice for clients on what works: "Consistently, the most effective way to detect fraud is tips -- between 40 and 45 percent of frauds that are detected are caught this way, and the next closest method of detection only accounts for 15 percent or so," he said. Hotlines to allow employees to report potentially dodgy dealings can be hugely useful, but only about 50 percent of companies have them, he said -- and even when they do, employees have to know what they're reporting.

"Anti-fraud training is very effective," said Warren, who is also a co-author of the ACFE's *Report to the Nations*. "It seems obvious what a fraud would look like, and almost invariably, someone knows or suspects, but they don't report because they don't know how, or they aren't sure that it's wrong, or they don't want to be seen as a snitch."

"Companies spent a lot of money on new controls and external audits," he continued, "but the training and hotlines don't cost that much, and they are so effective that there's really no reason not to have them."

The Latest Trends...

One of the reasons it's so hard to prevent fraud is that it keeps changing. While the profile of the fraudster may not change -- "The garden-variety under-appreciated employee with access is always going to be there," Blass said — their methods and the vulnerabilities of their victims are constantly changing.

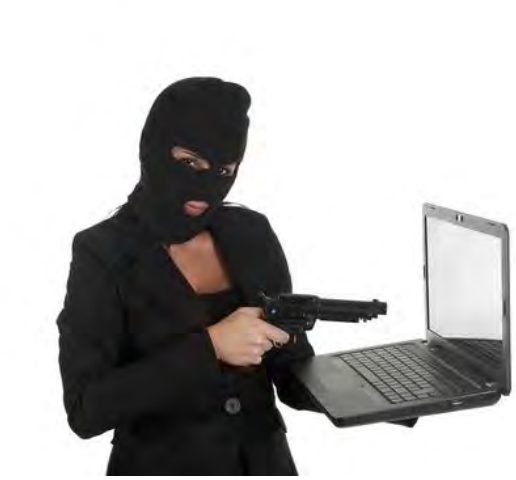
"We didn't used to see schemes that were that creative -- we're seeing more of them," said Wilson. "There's more awareness now -- business owners read about it. That just leads the employee to be more creative. If they have the motive and the rationale, they're going to find the opportunity."

An example of a new opportunity is the downsizing of finance and accounting departments. "The economy is causing business to operate with fewer staff - less people on accounting, finance, purchasing, and so on, so they have less ability to put in place controls and procedures for double-checking," he said. "That's a risk that sometimes the business owner doesn't understand. They have to understand that they are giving something up when they do that."

Wilson described a case that started with the departure of an employee in the bookkeeping department of a large school district, part of whose job was to go through a DVD of cancelled checks sent over by the bank, to make sure that the payee, amount and number were right. She wasn't the fraudster, though — she retired in perfect innocence, but her position was left unfilled, and "almost to the day," according to Wilson, her boss the bookkeeper started stealing, because there was no one to check the checks.

The bookkeeper's scam went on for almost eight years, siphoning off around $400,000, and was only uncovered when the bookkeeper fell ill and her replacement found evidence of the fraud in her desk.

Many frauds only recur when certain circumstances arise. "Only forensic accountants look at disasters this way," Blass said, "but unfortunately, there's going to be a deluge of fraudulent insurance claims" related to Hurricane Sandy in the Northeast. Earlier in his career, Blass worked with the New York City Department of Investigations, and said that he had uncovered a lot of fraud related to the recovery from 9/11. "Disasters often bring out the greed in some companies."



"Just as people used the U.S. Postal Service for mail fraud, now they use computers for computer fraud"

Christopher Cassar, Fuoco Group

The ACFE's Warren noted that new whistleblower laws are creating some unexpected issues: "Now staff have an incentive to take it outside the company. That's an exposure risk, not a fraud risk," he acknowledged, but it still brings along with it reputational risk, potential loss of market capitalization, and all the legal costs associated with an investigation. Better, he suggested, to create hotlines and implement training so staff are more likely to report fraud internally.

Warren pointed to data theft as a hot area for fraud. While most of the focus is on external hackers -- "We hear a lot about Eastern European syndicates" -- he said that he's more concerned about a different potential risk. "What keeps me up at night is what happens if an employee comes in intending to steal data? What if they come in and sit there for three or four months stealing data? I haven't seen a huge number of cases along those lines, but it's a big risk."

Technology...

An overarching issue in much of fraud today is technology -- as both an enabler of fraud, and a potent weapon against it. "Just as people used the U.S. Postal Service for mail fraud, now they use computers for computer fraud," said Christopher Cassar, IT forensic director at the FuocoTech unit of the Fuoco Group.

The pace of change in IT can make it difficult to keep up, but he had a number of current suggestions for companies to protect themselves.

- **Remind employees they're at work.** When staff log on, have a pop up that reminds them the computer they're using is the company's, not their own, and shouldn't be used for personal purposes.
- **Surf behind walls.** "Whether you're Fortune 100 or a mom-and-pop shop, when you're using the Internet, everybody should be behind a firewall -- they're cheap at this point," said Cassar.
- **Stay protected.** Virus protection software needs to be kept up to date, and businesses should make sure it covers e-mail, as well.
- **Stronger passwords.** In addition to requiring passwords that are less easily guessed, Cassar offered this advice: "Passwords are like toothbrushes - they should never be shared, and they should be changed every three months."
- **Treat phones and tablets seriously.** With more and more business being done on these devices, users need to remember that, "Phones are just miniaturized computers -- they're vulnerable to attack, too. The same thing applies to PCs as to smartphones -- make sure the patches are there, and that virus protection is updated."
- **Keep track of access.** When staff are let go, the IT department should be the first to know, so their access can be revoked — particularly now that

that data is so portable. "When you fire someone, are they walking out the door with their smartphone, going on the cloud and walking out with all of your data?"

- **Read your SLAs.** "When you're using the cloud, your data is no longer in your domain -- it's in California, in Ohio, overseas -- jurisdictions get complicated," Cassar said, so users should carefully check their provider's service level agreements to know what kind of protection they have, and what kind of assistance they can expect from the provider in the event of fraud or legal action.

While fraudsters frequently are among the first to take advantage of cutting-edge technology, sometimes they take advantage of lagging technology. RGL's Wilson described a case where a company's general ledger software didn't link up to the ACH system it used to send payroll, so an employee had to manually post the payroll each pay period. Needless to say, she included an extra four or five thousands dollars for herself each time and just made sure to understate the outstanding checks on the bank reconciliation when it came in to conceal the fact that more money was going out than was shown in the general ledger.

Conclusion...

Experts agree that one of the most effective tools to combat fraud is simply to make it clear to employees that it's unacceptable.

"You shouldn't blindly trust any employee," said Fuoco's Blass. "You should have controls on everyone, and companies should clearly communicate expectations to employees and the rules of the organization, in a clearly written handbook. The integrity of any company, the tone, starts at the top. If there's a finagling CEO who tries to beat the system, that CEO shouldn't be surprised if their employees operate similarly. They should imagine themselves in the shoes of their employees, seeing their bosses make money by lying." ♦♦♦

Bruce Hulme, CFE, is ISPLA's Director of Government Affairs (www.ispla.org). ISPLA is a resource for the investigative and security professions, U.S. and state governments and the media.

Latest News...

The Federal Trade Commission has released their February 2013 104-page *Consumer Sentinel Network Data Book* for January-December 2012.

Identity theft tops the list for 13th consecutive year in a report of national consumer complaints. 2012 marks the first year in which the FTC received more than 2 million complaints overall, and 369,132, or 18 percent, were related to identity theft. Of those, more than 43 percent related to tax- or wage-related fraud.

The report gives national data, as well as a state-by-state accounting of top complaint categories and a listing of the metropolitan areas that generated the most complaints. This includes the top 50 metropolitan areas for both fraud complaints and identity theft complaints.

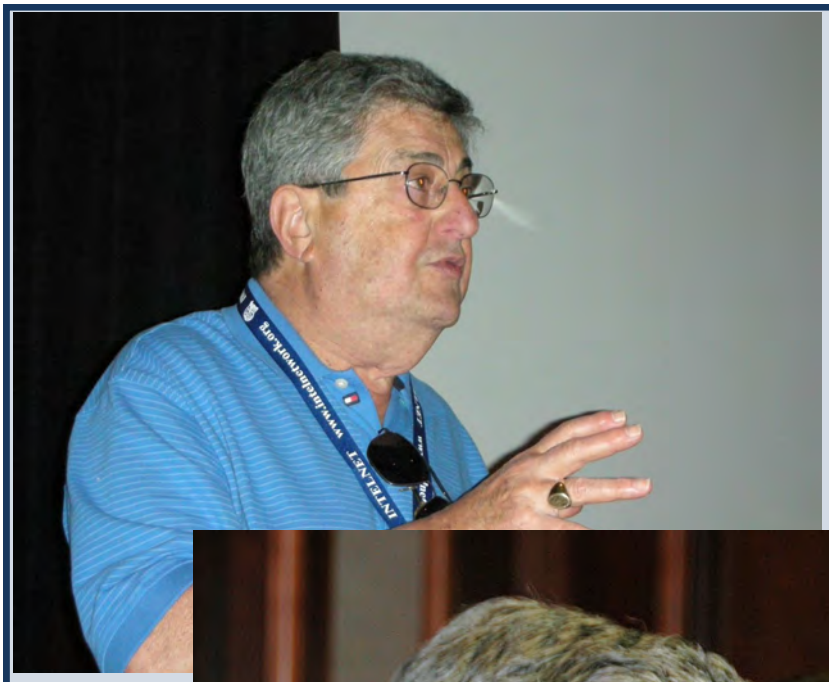
Completing the top three complaint categories are:

Debt Collection	*199,721 complaints*	*10 percent of total*
Banks and Lenders	*132,340 complaints*	*6 percent of total*

A complete list of all complaint categories is available on page six of the report.

The full report is available at: http://ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2012.pdf

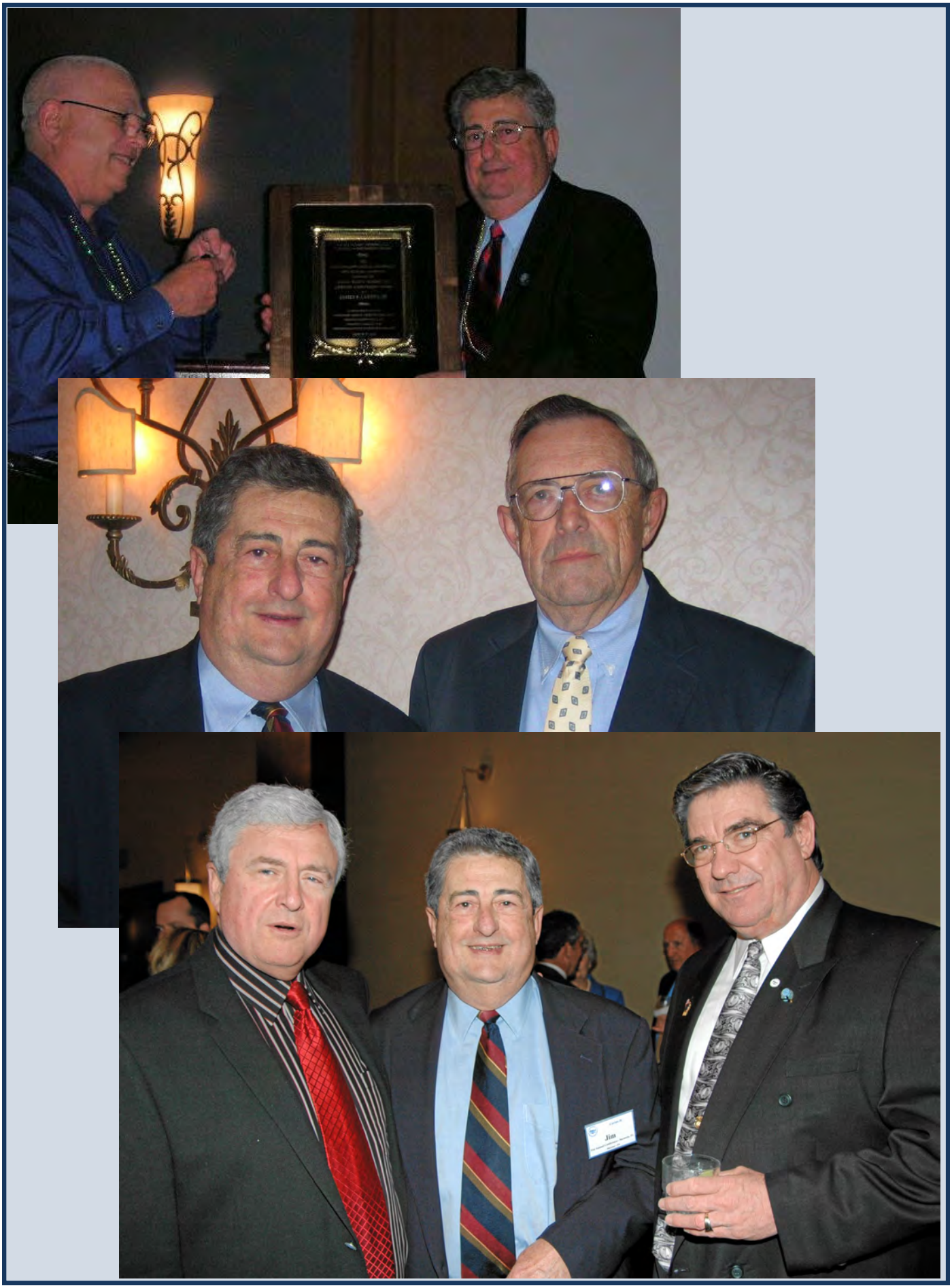
♦♦♦

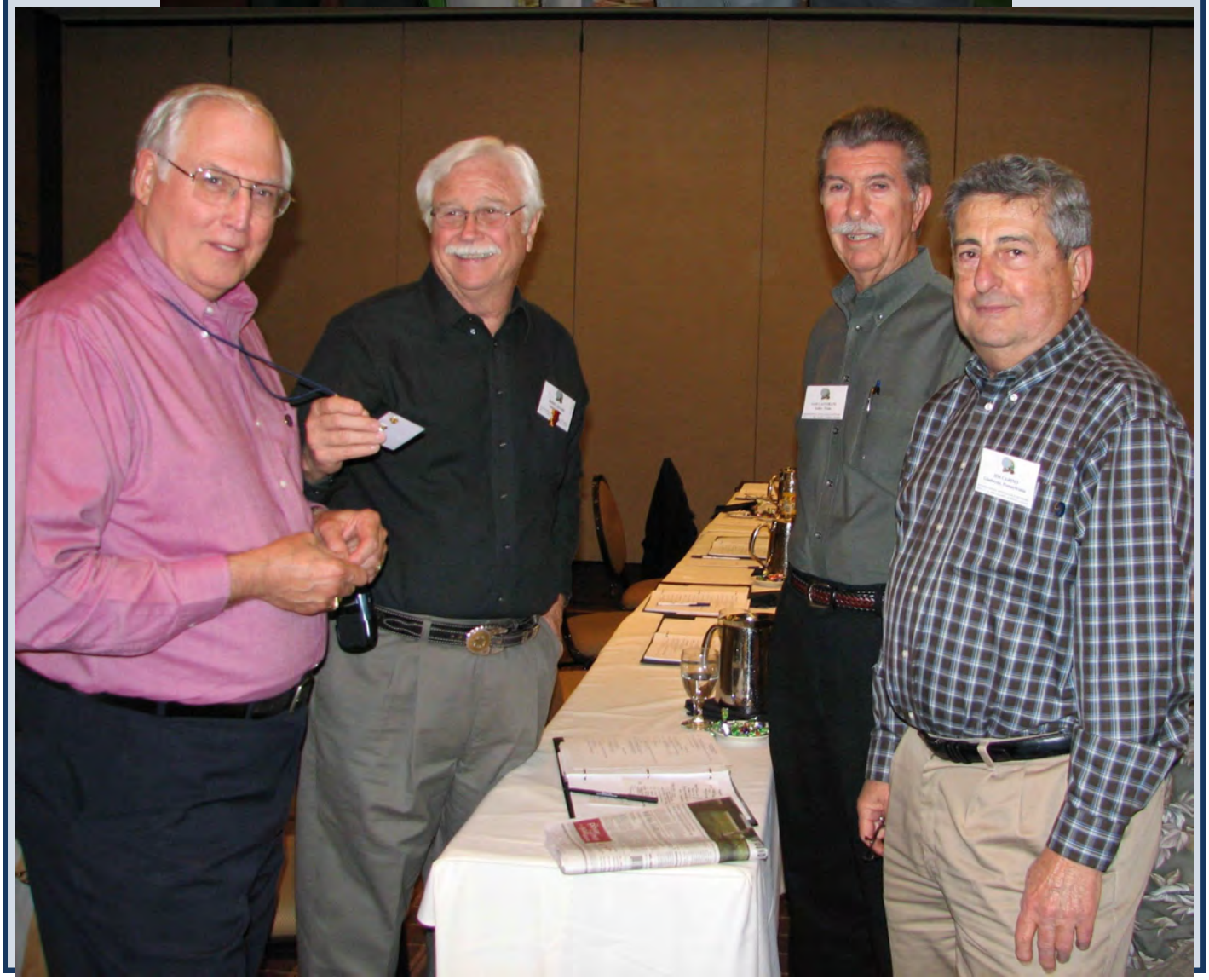


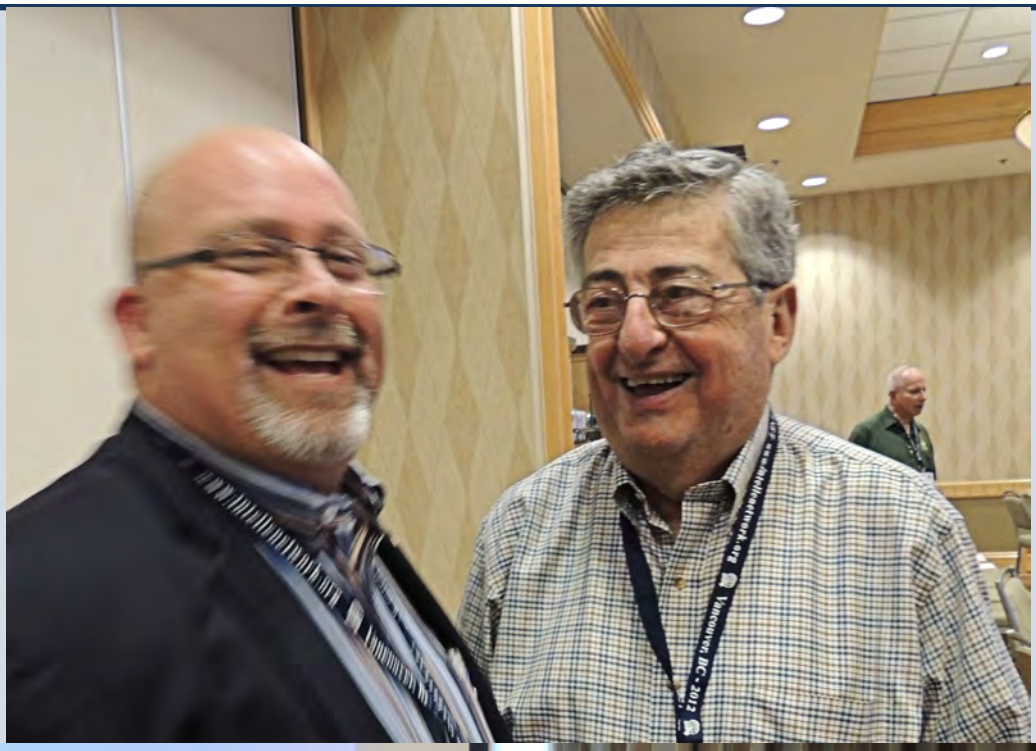
Jim and Friends

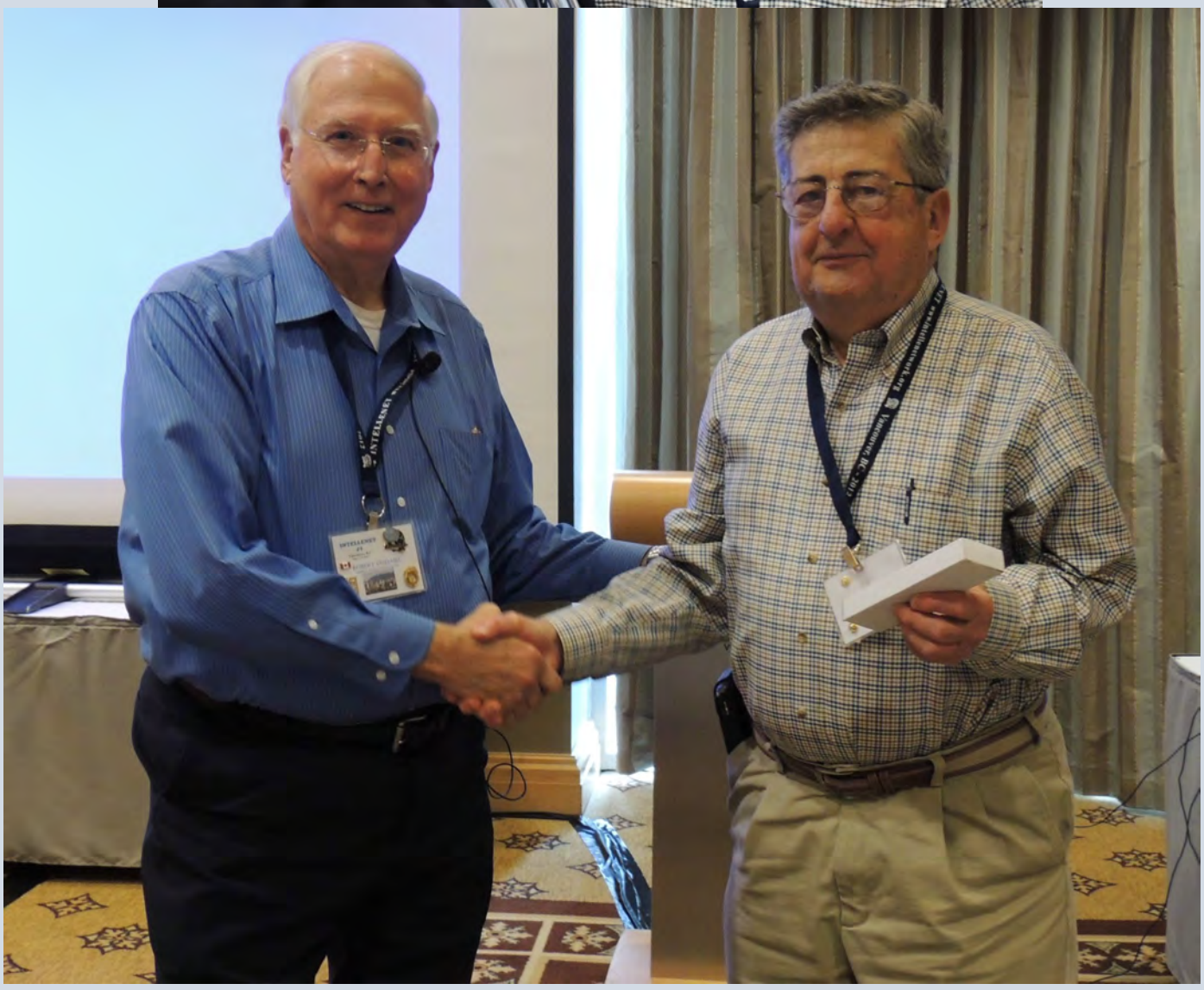
These are just a few of my photos from Intellenet gatherings and mixers in recent years. If you would like a copy of any image, let me know. Images are in JPEG format, 300dpi. Send me an email, mention page number and photo. Be glad to email you a copy.

Your Editor:
doncjohnson@comcast.net









Presented By PI magazine .com

EAST COAST INVESTIGATORS SUPERCONFERENCE 2013

Hosted By NJLPIA

Diamond Sponsor TRACERSINFO.com

Platinum Sponsor TLO

Proud Co-Host Intellenet

PIGEAR.com

PI bookstore.com

ISPLA Investigative & Security Professionals for Legislative Action

PInow.com

Smarter Academy

Yergey Insurance

NCISS National Council of Investigation & Security Services

WORLDWIDE INFO LOCATORS

World Association of Detectives, Inc. W.A.D.

Keynote Speakers

Diane Diamond
CNN, ET, Daily Beast

F. Lee Bailey
Former Attorney

Joe Pistone
"Donnie Brasco"

Anthony Capetola
Attorney

Vernon Geberth
"Mr. Murder"

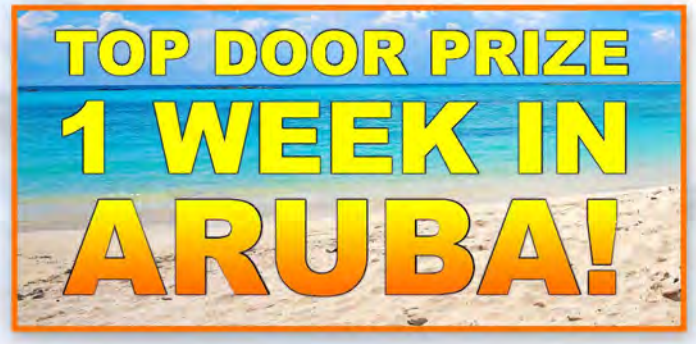
Pre-Conference Speakers

Jimmie Mesis
Michele Stuart
Joe Seanor
Mike Dores
Jim Carino
William Blake

Conference Speakers

Tom Shamshak
Susan Nash
David Ziegler
Jay Forget
Tom Owen
Barry Nixon
Kitty Hailey
Cynthia Hetherington
Elizabeth Rincon

* All Speakers Subject to Change



TROPICANA ATLANTIC CITY

Rooms Starting at $69!
Use Promo Code: HPIMAG 1 (800) 247-8767

Register Now! Save $100, Register Early!
www.PImagazine.com/AC2013