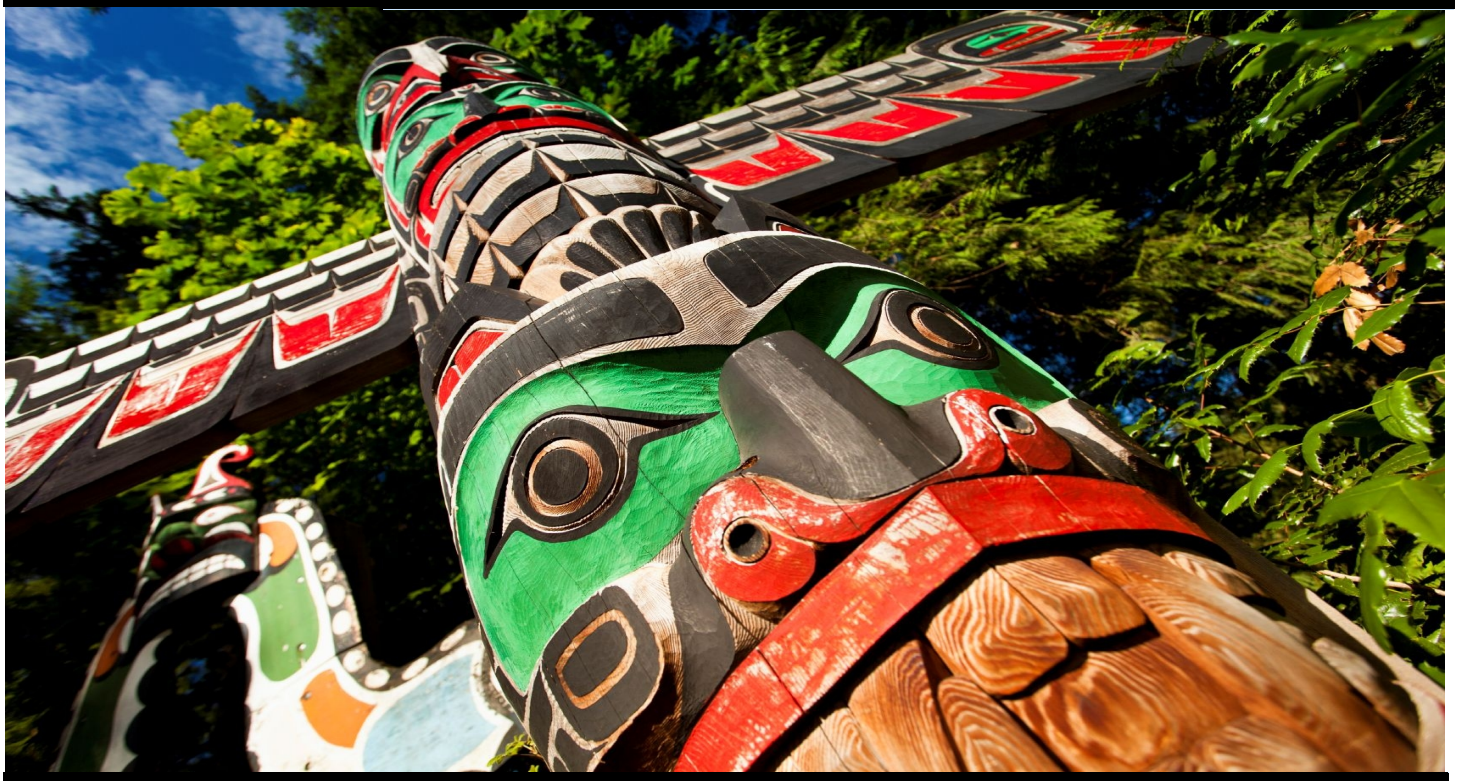
INTELLENET *News*

Official Newsletter of the
International Intelligence Network, Ltd.

Spring 2012

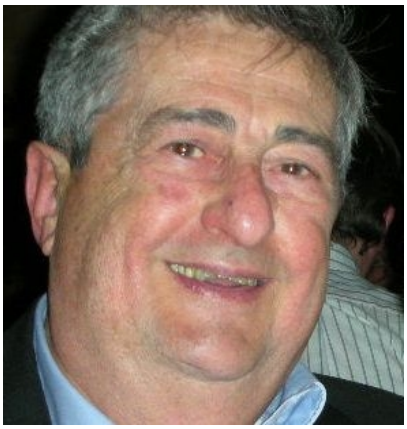


Conference 2012 Vancouver

" It's not too late to register!"

Details at www.IntellenetAGM.com

In this issue ...



Carino's Corner

by

James P. Carino, CPP, VSM

Executive Director, Intellenet

Each year virtually all associations hold one or more conferences. Several of the nationals and internationals hold two or more with attendance -- if not restricted to membership -- rarely heavily marketed to non-members. Many state PI associations use their annual conference as a recruitment tool for new members and also encourage out of state PIs to attend.

Intellenet both encourages non-members to attend and prices its conferences only to break even and not as a revenue generating event. We also pick "gateway" cities so that our international attendees do not have to book a local domestic flight, whether our event is held in the U.S. or at an international location.

Conferences should have, in the opinion of Intellenet, two major objectives as a target: 1) sessions that keep attendees current on the technical, new technologies and methodologies, on trends/developments within the PI field and on legislative matters; and 2) networking opportunities. Intellenet controls conference costs by using primarily our members speaking on their subject matter expertise. Our presenters are also conference attendees. Intellenet carefully intertwines social events with educational opportunities. As examples, for our 2008 Sorrento, Italy conference, a trip to Pompeii included a briefing by their security staff and how Pompeii protects its property and its treasures. The next conference in Vancouver in May features a Great Rocky Mountain Train ride to Whistler – site of the recent winter ski Olympics – and will include a briefing by the security professionals who planned and executed security for that event. Intellenet also plans a separate tour/entertainment program for non-session attendee spouses.

Two other major conferences will also be held during 2012 which all PIs should consider. If you are a PI interested in keeping current with legislation, new technologies and trends and want to extend your networking resources, closely look at the TALI Conference 1-4 August in San Antonio, TX and the East Coast Conference sponsored by Jimmie Mesis' PI Magazine 10-13 October in Atlantic City. Intellenet will be a sponsor and exhibitor in support of both of these important conferences. Encourage those you know who might be interested in attending one or more of these events. We hope to see many of you at one or more. ⊡

In Memoriam

As has been reported previously, we lost two longtime Intellenet members in the past few months ...

- **Cam Crowley** of Houston, Texas, passed away in February after a long battle with cancer. Cam was one of the earlier members of Intellenet (probably from around 1986). For years he was partnered with member Sam Castorani. Cam was a quiet, compassionate, true professional. He maintained a low profile, perhaps a throwback from his days with "The Agency."
- **Dave Gainer** of Evansville, Indiana, also lost a noble fight with cancer, "not a friendly foe," as he described it near the end last October. Dave was a veteran of the U.S. Army CID. Prior to Dave's funeral, our editor was able to visit with Dave's wife and son on behalf of Intellenet. Dave was a devoted family man and another true professional.

We have lost true friends dedicated to the profession and to Intellenet.

Welcome New Members 2012!

- Todd MISCHKE, Auburn WA
- Bruce SACKMAN, Bellmore (Long Island) NY
- James CARROLL, Oklahoma City
- Maurice HICKS, Las Vegas
- Bruce HALL (MD) as a new member on the staff of member Doug WOLFE (MD)
- Russ KOLINS (PA)
- Mark MABREY, Evansville IN
- Danielle SHULL (PA)
- Richard (Rick) KELLY, Mechanicsberg PA (newly licensed PI from the D List)
- Chris PETERSON, Vancouver WA
- Walter (Wally) BAKER, London, Ontario Canada
- Robert (Bob) KOWALKOWSKI, Farmington Hills MI

If we've missed a recent member in this issue, apologies; we'll mention you in an InfoBrief email and in the next newsletter.

▶▶▶

Members in the News!

Seen here at the ASIS gathering in Kuala Lumpur last June is ASIS Malaysia chapter chair **Siti Nadu** and Intellenet member **Werner Preining**, Captain, CPP, CMAS, Interpool Security Ltd, Vienna. ▶

Intellenet in Partnership with IAAR

Our executive director is seen above with **Bill Blake**, Colorado, left, and **Al Ristuccia**, Los Angeles, at the annual conference of the International Association for Asset Recovery last November in Las Vegas. This year IAAR is scheduled to merge into the Association of Certified Financial Crimes Specialists. Intellenet member **Joe Dickerson**, Colorado (right), and other members were also present in Las Vegas. Member **Steven Rambam**, New York, was a featured speaker. ▶

Congratulations to **Sean Mulholland**, CLI, CFE, CPP, Jacksonville, Florida, who was recently elected president of the Jacksonville chapter of InfraGard, the FBI's private sector partnership program. Sean was also a featured speaker at the mid-winter seminar of the National Association of Legal Investigators, along with members **Michele Stuart** of Arizona and **Don C. Johnson**, CLI, Indiana. Members **Terry R. Cox**, CLI, Mississippi, and **David W. Luther**, CLI, Houston are NALI National Director and Assistant National Director, respectively. Intellenet members will also play prominent roles in NALI's annual conference this year in Chicago. Details at **www.NALI.com.** ⦿

Behind the Numbers:

Critical Financial Analysis in Litigation

By Tracy L. Coenen, CPA, CFF

The financial portion of a lawsuit is often high-stakes. This is especially true in cases of divorce, breach of contract, securities fraud, tax fraud, money laundering, and white collar criminal defense. Whether the other side is an individual, a company, or the government, you need an accurate analysis of the numbers for the benefit of your client.

There is almost always a story behind the numbers. Things are not always as they appear, and it is unwise to take the financial story at face value. A case can be won or lost based on your ability to find out the hidden truth about the numbers.

"The best, most reliable documentation ... is provided by an unrelated third party."

Finding the Data

Getting your hands on the right financial data depends on knowing what to ask for. The financial statements and tax returns are the obvious places to start. While they may not always be truthful, they still hold many clues to the financial story.

Manipulated financial statements may be unreliable, but they are often still useful because they may inadvertently provide clues about a company's true income and expenses. Tax returns could provide information on property owned, new lines of business, and related companies.

We can verify the authenticity of tax returns provided in discovery by getting data directly from the government. This doesn't mean that the income and expenses were reported correctly on tax returns, but it does offer us one way to check whether the data we receive was actually filed with the government.

Other Data Sources

Analyzing the numbers can include inspecting source documents such as invoices, receipts, contracts, and other financial documents. By examining these documents which are used in the accounting process, we are able to learn more about the detail behind the reported income and expenses.

This type of analysis helps identify customers, vendors, payment terms, and other details of transactions. While these documents can be fabricated or manipulated, a seasoned expert should be on the lookout for the signs of fraudulent documents and should be skeptical when examining documents.

The best, most reliable documentation in a financial investigation is provided by an unrelated third party. A great example of reliable third party data is that contained in bank statements, deposit slip copies, and check copies. Except in the rare case in which there might be collusion between a bank employee and a party under investigation, bank documents are very reliable. They show exactly where money has flowed to and from, reliably reporting the truth about the funds.

Banks may also provide helpful data from loan applications and credit card applications. While an applicant may misrepresent information while applying for credit, there is often valuable information contained in the application. At the very least, manipulated figures on a loan application may confirm that the target of the

investigation is dishonest.

Other third parties that may provide information and documentation include customers, suppliers, business partners, and former spouses. The accessibility and reliability of this documentation varies, and subpoenas might be needed to get the information.

Digging Deeper

After the right financial documentation is gathered, the heart of the investigation can begin. The analysis is often very labor-intensive, especially in cases of money laundering or Ponzi schemes, in which many accounts, entities, and transactions are deliberately used to create a web of confusion. The financial investigator must harvest the data and put it into a format that allows for verification of accuracy, tracing of funds, and connection of people, organizations and money.

People lie about money, so it is important to have the assistance of a financial investigator who can get behind the numbers to find the truth. Finding this truth creates an advantage for the client in litigation. It can take considerable time and expense to find the truth, especially if other parties to the litigation have deliberately attempted to conceal things. However, with the right expert and the right documents, it is possible to determine where the money went. That knowledge can be used to win cases for clients. ▣

Tracy L. Coenen, CPA, CFF is a forensic accountant and fraud investigator with Sequence Inc. in Milwaukee and Chicago. She has conducted hundreds of high-stakes investigations involving financial statement fraud, securities fraud, investment fraud, bankruptcy and receivership, and criminal defense. Tracy is the author of Expert Fraud Investigation: A Step-by-Step Guide and Essentials of Corporate Fraud, and has been qualified as an expert witness in both state and federal courts. She can be reached at tracy@sequenceinc.com or 414.727.2361.

The Doctor's Worst Nightmare!

A Financial Crime Saga

By Ken Wilson, CFE, CSAR

The facts in the following scenario are not based on an actual case and the names and titles used are for illustration purposes only.

It all started late Friday afternoon as the doctor was finishing up with the patient charting. This particular Friday, he was in the office alone because Mary, his office manager and part-time bookkeeper, was attending her mother's funeral. The funeral was scheduled to start at 4:00 PM and Mary didn't leave the office until 2:30 PM. The doctor convinced Mary he would be able to handle everything himself and she should leave and not worry about the office. Mary had worked for the doctor for eighteen years and was responsible for every aspect of the business, with the exception of patient care. That was the doctor's sole responsibility.

Mary was considered part of the doctor's extended family and both he and his wife, who had passed away only four years earlier, thought the world of her. The doctor ran a small family practice by himself and was highly regarded in the community.

About eight months earlier, Mary had convinced him to change banks in order to get better interest rates and better service. The new bank offered things such as on-line banking, paperless bank statements and a host of other services. Because the doctor trusted Mary's judgment on such things, he agreed. As far as he knew or cared, everything was running smoothly. That is why the phone call he received from the new bank manager was a huge surprise.

"Hello doctor, this is Ron, the manager at your bank. Mary must be out of the office today for you to be available and having to answer the

phone. Normally, I wouldn't bother you with this. Mary has always told us she had checked with you and relayed what you wanted to do whenever these issues came up in the past, but I am glad we finally have a chance to talk. I am calling to find out from which account you would like us to transfer money in order to cover the shortages in your general account. We can take the money from your line-of-credit, your savings or cash out one of your certificates of deposit. I know you understand that if you elect the last option, there will be a penalty associated with the interest, just like last time."

> "O, what a tangled web we weave when first we practice to deceive!"
>
> *Sir Walter Scott*

"Wait one minute Ron, there must be some mistake", the doctor said. "I always have sufficient funds in my checking account to cover my expenses and what do you mean by, like the last time and issues in the past. I have never spoken to you or anyone at your bank. Mary handles all of those matters for me and I can assure you she has never mentioned there ever being a problem."

"That's funny. Every time we've talked with her about this she said she had spoken to you. She would then give us your instructions. Normally, we moved money from your line-of-credit account or one of your savings accounts, but there was at least one time we cashed in one of your CD's early in order to have enough funds to cover your expenses. I think we should meet and get to the bottom of this. Right now, there isn't much money left in any of the accounts to cover payroll and the current credit and debit card charges."

"You are absolutely right we need to meet," the doctor replied. "I will be at your bank in ten minutes and I hope you have the documentation to back up what you are suggesting!"

And so begins the doctor's worst nightmare, much like those of many other small businesses. After meeting with the banker, the doctor learned he apparently had one additional employee on the books that he knew nothing about. The business debit and credit cards issued through his new bank were being used for much more than he ever knew. Both cards together were running almost $10,000 per month. In fact, the doctor didn't even carry either card with him because he knew they were always in Mary's desk, or at least that is what he thought. He learned there were some automatic payments set up through his business checking account that went to a credit card company, yet he knew he never had an account with that company. In some months, these payments also reached $10,000.00. Then there were the automatic transfers to a bank he never heard of before. These payments appeared to be for some type of a loan. His $1.0 million line-of-credit, which he had set up when he anticipated doing a major remodel of his clinic, was nearly maxed out. Apparently this account was being used to cover over-drafts in his general and payroll accounts. To top it all off, his CD's, which once totaled five, were now down to one. These too, he learned from the bank manager, had been systematically cashed out early, or in some cases allowed to mature and then cashed, and used to cover over-drafts.

The doctor asked Ron to pull together all of the bank statements for all of his accounts, along with all of his cancelled checks and transfers. He knew he would have to go through all of the statements himself, for the very first time. He also decided to call his attorney for advice and possible referrals and then contact the Certified Fraud Examiner he had heard about. Maybe this person would be able to help reconstruct all of

the transactions and assist in locating his money.

Walter Scott once said, "O, what a tangled web we weave when first we practice to deceive!" This was indeed a tangled web of financial transactions and deception. But for how long had the deception been going on? The full extent of his financial loss remained to be learned.

As it turned out, Mary's embezzlements had started long before she had changed banks. It started about four years earlier when Mary's mother became seriously ill and shortly after the doctor's wife had passed away. The doctor learned the real reason Mary recommended changing banks was because the previous bank was getting ready to close all his accounts because of the large number of insufficient fund checks that required the bank to transfer money from other accounts. The investigation also determined the extra employee on the payroll was Mary's mother. The payroll checks were set up as a direct deposit into her mother's account, who didn't know anything about them because Mary also handled her financial affairs. Upon her death, all of the money in the mother's account automatically went to Mary.

The doctor was just beginning to come to the realization of his situation. Everything pointed to his trusted office manager Mary, but he still did not have any real proof. Should he call her that evening and demand an explanation or wait until Monday? What if he fired her on the spot without having any proof or provide her an opportunity to explain? Might he face legal repercussions for slander, libel, defamation or wrongful termination? He then realized it was a good thing his wife had passed away, because the shock of all this would have certainly killed her. If the doctor fired Mary immediately, would he ever see any of his money again? What if she offered to repay him all the money, should he keep her employed? After all, her mother had been ill for several years and now she too had passed away. The doctor didn't know who to call first or what to do. Sure, he had an attorney he had used on a few occasions, but he wasn't an employment law attorney or even a criminal law attorney. He never had an accountant, because Mary always took care of his taxes and all his books. If he called the police without any real evidence, would they even be interested or would that cause Mary to pack up and leave and hide whatever assets she might have acquired with his money? The doctor had so many questions his head was spinning. What to do? Why me? Why didn't I know what was happening sooner? How could Mary have done this and why? This case illustrates some of the legal and emotional issues embezzlements present.

Lessons Learned

It is imperative for a business owner to actively participate in good fiscal management of the business:

- To have separation of job duties and not have one person responsible for all aspects of the business.
- Have all bank and credit/debit card statements mailed directly to the owner's residence and review them monthly.
- Use a bank that provides at least a copy of the front of all cancelled checks included with the bank statement.
- Use the bank's on-line access to review checks and all statements frequently.
- Be aware of the "red flags" of fraud.
- Lastly, the doctor learned any one of these preventative steps would have stopped the embezzlement before it got started.

These types of embezzlement schemes are more common than most businesses know. Some go unreported because the business owner is too embarrassed for having allowed it to happen. Small businesses and not for profit entities are particularly vulnerable because they lack the staff to have separation of duties between employees. Professionals like doctors, dentists and lawyers are too busy running their practice and have no involvement in their own financial business affairs, choosing instead to hire someone to handle all of that for them. In addition, few employers conduct any form of background or reference checks. In one recent dental clinic embezzlement case I worked on, the employee had been terminated and was awaiting trial. She was able to get another job at a different dental clinic while out on bail. Granted, she had not been convicted yet, but the fact she had been arrested, formally charged and was awaiting trial was all public record and available on-line at no cost.

In the above case, the doctor hired the Certified Fraud Examiner who analyzed all of the financial documentation with the assistance of a private attorney who filed a civil lawsuit against the bookkeeper. Together, they were able to identify over $800,000.00 of assets that had been acquired with the doctor's money. Those assets then became available for civil forfeiture under Washington State's Criminal Profiteering Act. Once the assets were firmly identified and legal proceedings initiated against them to freeze them from being transferred or sold, the evidence was forwarded to law enforcement. The detective accepted the case that was prepared by the Certified Fraud Examiner and took the case to the local prosecutor, who filed multiple counts of theft, money laundering, and forgery against the bookkeeper. Just prior to trial, the bookkeeper accepted a plea deal from the prosecutor and was sentenced to ten years in prison. This unusually long sentence was due to the position of trust held by the bookkeeper, the long period of time over which the fraud was conducted and the large financial loss of $1.5 million. The judge also noted the complexity of the embezzlement and the fact the bookkeeper had allowed the doctor's employee dishonesty insurance policy to lapse.

The Fraud Triangle

The Association of Certified Fraud Examiners uses an investigation model called the "Fraud Triangle." The principle behind which is when an employee has an "Opportunity," a "Financial Need" and is able to "Rationalize" their conduct, they will steal. Prior to that time, they will likely be the ideal employee. In the above scenario, Mary always had the opportunity and was always able to rationalize. However, it was not until her mother became seriously ill that she had the financial need. Rationalization statements might include such things as:

- ***The owner will never miss it.***
- ***I am not paid enough.***
- ***I need this money more than the owner.***

Below are actual rationalization statements made by a convicted embezzler at her sentencing hearing:

"I would catch myself getting high on shopping … like an addiction."

"You're just borrowing the money."

"Each time you do it, you're able to kind of justify it."

"I was writing checks and paying bills like it was my money."

"It got to the point where I felt like it was my business."

Remember, as the owner of the business it is your responsibility to put the safeguards in place and to monitor those safeguards in order to protect your money. Failure to do so might result in your worst nightmare. ⊡

Ken Wilson, owner of Wilson Investigative Services, is a Certified Fraud Examiner (CFE) and a Certified Specialist in Asset Recovery (CSAR). He has been conducting financial investigations for over thirty-seven years. During his career, Ken worked as an investigator for Washington State and has been in business for the past ten years. His goal is to educate businesses about their fraud risks to prevent a problem before it happens, and work with businesses to recover as much of the stolen funds as possible and hold the employee accountable. Ken can be contacted through his website: www.wilsonis.com or his e-mail: ken@wilsonis.com. This article may not be reproduced or reprinted in any way without the express written permission of the author.

The Legislative Report

By

Bruce Hulme, ISPLA Director of Government Affairs

Since the formation of Investigative & Security Professionals for Legislative Action (ISPLA) in 2009, I have had the pleasure of working with newsletter editor Bill Blake, and I thank him for all that he has done in that regard. As in the past, ISPLA will continue submitting reports on the legislative and regulatory work it is doing under our agreement with Intellenet (see sidebar), and for our colleagues in the investigative and security field. I look forward to again working with Intellenet's new editor, Don Johnson. During my five-year tenure as NCISS' legislative director, I had the pleasure of submitting articles to Don in his capacity as editor of The NCISS Report.

ISPLA has been furnishing periodic updates on breaking legislative and regulatory news, as well as our federal lobbying efforts in Washington, DC. Numerous alerts by ISPLA have been posted regarding the GPS Supreme Court decision, recent federal bills offered, and updates on privacy issues and information security breaches. This report will cover just some of the issues ISPLA has handled since the start of 2012, including assisting state professional associations, commenting on ISPLA committee members' work for the profession, and a report on our ISPLAPAC operations.

State GPS Tracking Bans:

Private investigators in Virginia have been fighting against proposed anti-GPS legislation since it first was floated nearly two years ago because it excludes them.

We are happy to report that the bill was defeated in the Virginia Senate on February 20 by a vote of nine to six. ISPLA supporter Phil Becnel informed us there was a slight chance the bill would be introduced this year, but not likely. Phil extended thanks to the Virginia associations, PIAVA and PISA, and ISPLA for working together to defeat the bill. He sent a special thanks to ISPLA executive committee member Nicole Bocra of Infinity Investigative Solutions.

In an earlier message to the Associated Press, Nicole summed up the objections to the bill: "Private investigators perform a public service by working on insurance fraud, embezzlement and other white-collar crimes," she said. Their efforts will be hampered if they can't electronically track suspected embezzlers as well as cheating husbands. "We play a vital role in this system." She noted that, unlike the police, they cannot obtain a warrant, which by the 2012 U.S. Supreme Court decision in U.S.

vs. Jones is now required of law enforcement. After the bill passed out of a Virginia House of Delegates committee. Nicole continued the fight to either defeat this bill, amend provisions to it or seek an exception for lawful investigations.

In Michigan, where ISPLA Chairman Peter Psarouthakis of EWI & Associates, Inc. has handled legislative matters, GPS tracking by professional investigators conducting lawful investigations is legal. He has furnished legislative material used to enact the favourable GPS statutes in Michigan to our colleagues in Arizona, Georgia, New York and Virginia.

Indiana Attempts Deregulation of Licensing of Private Investigators and Contract Security:

In Indiana, HB 1006 called for the elimination of licensing for private investigation firms and security guard agencies, in addition to three other boards regulated by the Indiana Professional Licensing Agency. According to Indiana investigator Ralph Garcia, the bill would expose the public to "... unvetted, uninsured and unscrupulous operators. Licensing came into existence over 50 years ago in Indiana to provide these valuable safeguards. All changes to the codes since that time have been designed to further enhance the protections for the citizens and businesses of Indiana, while keeping the costs for licensed businesses low." Garcia went on to state in part:

> *Unlicensed operators would be uninsured and unbonded, leaving their clients with no recourse but to address grievances of fraud and failure to perform in the crowded civil courts, where cases often linger for years. No civil court will issue a judgment against an unlicensed operator unless the plaintiff can provide identifying information on that unlicensed operator, including a social security number. Even when attempting to file a civil complaint, a plaintiff may not be able to accomplish service of process because the unlicensed operator has no business address and provided no home address at the start of the engagement.*

ISPLA worked closely with the leadership of the Indiana Society of Professional Investigators (INSPI) and the Indiana Association of Professional Associations (IAPI) to head off this ill-conceived de-regulatory measure. We were also in contact with the International Association of Security and Investigative Regulators (IASIR) and, to a limited extent, with NCISS. At an "eleventh hour" hearing, ISPLA's Peter Psarouthakis went to Indianapolis and testified against the bill, along with other investigative and security representatives. The bill was withdrawn within days by the sponsor. Intellenet's newly appointed newsletter editor, Don Johnson, who is president of Indiana's Private Investigator and Security Guard Licensing Board, was also present at the hearing. Don reported that efforts were made to keep board presidents from testifying against the bill.

Assuming False Identity Versus Impersonation:

In New Jersey, on behalf of Intellenet members in that state as well as the New Jersey Licensed Private Investigators Association (NJLPIA) -- one of our state association financial supporters -- ISPLA expressed strong reservations regarding a proposed section of Assembly Bill 2105 concerning impersonation via electronic means and amending N.J.S.2C:21-17. Our concern centered on the provision of "assuming a false identity" rather than limiting the definition to just "impersonating another" whether or not such act is done in person or by any other means of communication, including social media or a website. We advised the sponsors that we anticipate that there will also be unintended consequences arising out of the definitions of the benefit, which may or may not inure to the investigator assuming a false identity; and that allowing mental suffering or distress as a factor will also present problems. We wrote there should be an exception granted for investigators who are conducting lawful investigations. We also referred the sponsors to federal legislation passed in the 111th Congress that concerned "spoofing" a telephone caller's number that

contained an "Intent to harm" clause, which might be applicable to their proposed bill.

We pointed out that false identities are not only assumed by investigators locating witnesses, obtaining information from reluctant sources, or conducting undercover operations; they are also used in the investigation of theft of trade secrets, intellectual property, and inventory losses. Social media and the creation of websites are also often utilized in such investigations, particularly in major cases involving large monetary losses and in recovering ill-gotten gains taken from our clients by thieves.

In the investigation of international crime rings, similar investigative techniques using false identities, pretense, social media and fake web sites are a key element used to locate, identify, and lure thieves into a jurisdiction where they may be criminally prosecuted—or, at the very least, sued civilly. Such cases are usually initiated by private and/or corporate investigators and then turned over to federal or state prosecutors for criminal action or to attorneys for civil remedies. Private sector investigators and security professionals comprise more than twice the number of public law enforcement in the United States. In times of budget constraints, it is the private sector that members of the public and business community turn to when seeking redress.

ISPLA emphasized that the use of pretexts and assuming a false identity (not impersonation) are recognized tools when utilized while conducting lawful investigations by both public and private sector investigators. Any alleged actions of those who impersonate are not representative of the many licensed private investigators who work every day to fight fraud, locate witnesses, and support the U.S. system of justice.

Homeland Security – Muslim Homegrown Terrorists:

ISPLA executive committee and Intellenet member attorney Richard Horowitz, also a licensed private investigator concentrating in corporate, international, and security matters, is a recognized expert in the area of terrorism and security issues. He served in the Israel Defense Forces for six years, attaining the rank of captain, where he researched, planned, and implemented national security projects. He has now been asked to do a weekly segment for InfraGard-NY TV on security and legal issues. He was the terrorism consultant on Fox New York during the week of September 11, testified to the Public Safety Committee of the New York City Council on post-September 11 security in New York, and has appeared on NBC, MSNBC, and the Fox News Channel.

He served as security consultant for a public relations event held in 1993 for Bosnia under the auspices of the president of the United Nations General Assembly and has prepared educational material for the U.S. Department of Defense. He is a member of the steering committee of the Business Threat Awareness Council and has served as a member of the International Security Affairs Committee of the New York City Bar Association, the Trade Secrets and Interference with Contracts Committee of the American Bar Association, and the Economic Crime Council of the American Society for Industrial Security. He has been published in Security Management, the Journal of Counterterrorism and Security International, and the International Journal of Intelligence and Counterintelligence.

Please take eight minutes and listen to the February 14 interview of Richard Horowitz regarding Muslim terrorists by the InfraGard, New York Metropolitan Chapter, which will become a weekly event. It can be found at:

www.youtube.com/watch?v=bFiVHhQez9Y&context=C34dcc2aADOEgsToPDskJ-I6jJuP7Dlpzo1QlVYBXV

FBI Seeks Developer for App to Track Threats on Social Media:

On February 17 Fox News reported that "The FBI is getting in on the law enforcement app game--posting documents online recently to seek industry input on developing the equivalent of a web alert system." FBI Social Media Application, a 12-page document, provides a detailed picture of the bureau's specifications which must have the ability "... to rapidly

assemble critical open-source information and intelligence ... to quickly vet, identify and geo-locate breaking events, incidents and emerging threats."

"I think what you are looking at is a Google news feed specifically targeted for law enforcement, focusing on their specific needs," said Frank Ciluffo, who presently leads George Washington University's Homeland Security Policy Institute. "We're on our mobile phones, and we're on our various iPhones, BlackBerrys and the like that transmit data that locates individuals."

I was a speaker at an ASIS led post 9/11 event in Washington, DC with Ciluffo, when he was Homeland Security adviser in the George W. Bush White House. He recently described tracking social media as "... the tip of the spear for national security investigations and that it raises privacy questions, over whether law enforcement officers are allowed to monitor public social media posts."

"According to the American Civil Liberties Union, which reviewed the FBI documents for FOX News Channel, information pulled from sites like Facebook, Twitter and blogs could be cross-referenced with other databases to identify potential threats. Mike German, a former FBI agent who runs the national security section of the civil liberties group, said the data could be used to increase video surveillance in a neighborhood."

The FBI states that if this program is implemented, it "... will not focus on specific persons or protected groups, but on words that relate to 'events' and 'crises' and activities constituting violations of federal criminal law or threats to national security. Examples of these words will include lockdown, bomb, suspicious package, white powder, active shoot, school lockdown, etc."

To read more go to:
www.myfoxdc.com/dpp/news/fbi-seeks-developer-for-app-to-track-threats-on-social-media-ncxdc-021712#ixzz1mgwwRU2l.

The Law and Ethics of Investigations:

Lawyers in many practice settings and in many practice areas are frequently called upon to conduct, oversee, plan, or use the fruits of investigations. The ethics rules and case law limit a lawyer's role and activities in investigations: Is any deception permitted? Is any contact with an opposing party permissible? Many other laws also govern the conduct of lawyers and their investigators: When does surveillance stray into trespass, stalking or invasion of privacy? Are some forms of online interaction forbidden? When does creative online digging turn into violations of federal law? As private investigators routinely interact with attorneys, I will be answering these questions and more, as well as covering other aspects on ethics and the laws governing investigations at an ALDONYS/SPI Seminar to be held at Vernon Downs Casino and Hotel on April 19 and 20 in Vernon, NY. Other speakers will include notable experts on forensic psychiatry, major case investigations, computer forensics, undercover investigation, and surveillance equipment and techniques. There will be CPE credits issued for approved CFE requirements. Additional details are at www.aldonys.org.

ISPLAPAC 2011 Year End Report

ISPLAPAC as of December 31, 2011, had a year-end closing account balance of $2033. On January 1, 2011 its cash on hand was just $135. During the previous two years, it had disbursed almost all of its funds to candidates. During 2011, it received $2310. It made no political contributions in 2011 as, except for several special elections to fill vacancies, it was not a Congressional election year

Since the inception of ISPLAPAC, it has contributed $2000 to Rep. Peter Sessions, Republican from Texas; $2000 to Rep. Barney Frank, Democrat from Massachusetts; and $1000 to Rep. Hansen Clarke of Michigan. Sessions has been a long-time supporter of our professions. Frank, who chaired the House Financial

Services Committee while the Democrats controlled the House, assisted us on several ill-conceived bills. He is not running for re-election. Clarke, a freshman congressman who won a special election in 2010, has been working with ISPLA in a proactive fashion in an attempt to sponsor a bill that would be favorable to our sector.

Special thanks to the Intellenet members and to the ISPLA executive committee who have financially supported ISPLAPAC: Ellis Armistead, Nicole Bocra, Jim Carino, Dennis Crowley, Paul Dank, Jeff Frey, Harriet Gold, Alan Goodman, Paul Jaeb, Jim Olsen, Peter Psarouthakis and Bill Vincent.

During 2012, ISPLA will be researching additional potential candidates for possible endorsement and/or financial support in the fall 2012 congressional elections. It should be noted that many present members of Congress have opted not to run for re-election this year. In selecting such candidates ISPLA will consider the following:

- Candidate profile and background;
- Dynamics of political race;
- Leadership position in political party;
- Political potential;
- Leadership position in the Congress;
- Committee assignments / chairmanships;
- Sponsorship or co-sponsorship of key bills;
- Voting records on issues of concern to investigative and security professionals;
- Working relationships with investigative and security constituents; and
- Lobbyist and other governmental affairs recommendations.

We are now ratcheting up our voluntary ISPLAPAC requests for contributions towards the fall 2012 congressional races. I hope a few more of you will support the work we are doing. Should anyone have need of further clarification or wish to donate to ISPLA or its political action committee, I may be reached at (212) 962-4054, or go directly to: *www.ispla.org/isplapac.* ⊡

Bruce Hulme, New York, is ISPLA's Director of Government Affairs and Treasurer of ISPLAPAC

ISPLA - Intellenet Agreement

ISPLA will be retained to independently handle legislative and regulatory monitoring, government affairs, advocacy programs, and report on significant proposals, acts, treaties, agency and commission rulings, court decisions and laws which may affect INTELLENET members and the private investigations profession and the security industry.

ISPLA and/or the INTELLENET Legislative Liaison Board member will be the sole authorized entities to provide information concerning legislative and regulatory issues to the listservs and publications of INTELLENET. ISPLA will have authority to conduct political action activity of INTELLENET members through ISPLA-PAC and through its government relations work on behalf of INTELLENET, to seek periodic voluntary individual contributions from INTELLENET members to fund to its non-partisan ISPLA-PAC, and to utilize INTELLENET's resources, in compliance with Federal Election Law and/or to periodically seek voluntary contributions or assessments authorized by the INTELLENET board, should such be enacted, from business and corporate members of INTELLENET to fund ISPLA's operating expenses in compliance with rulings and provisions of the Federal Election Commission.

▣▣▣

The following "FAQ" article is used by the **eurosec, GmbH** agency of Wuestenrot, Germany, informing potential clients on how information is obtained in the course of an investigation in Germany. We send special thanks to Intellenet member **Karlheinz Buchzik** for sharing this information.

Obtaining Information in Germany

You are asking for some information service from abroad do be done in Germany. Since you are probably not familiar with the authority structure and the data protection laws in Germany, we prepared this PDF-leaflet with answers to the most frequent asked questions, to provide you with a brief overview about the situation in our country. If you have any further questions, do not hesitate to contact us (addresses: see footer line).

1. Data Protection in Germany

As a part of the European Union, Germany is obliged to fulfill the European Data Protection Act (EU-DPA). However each European country has its individual way how to handle this legal aspect. Therefore, the Germans executed the EU-DPA less hard into their own, more than 30 years old and best proven national law (that was the first one in the EU), rather than what other European countries implemented first a couple of years ago. Therefore a lot of things are still possible in Germany that aren't in Belgium, the Netherlands or England.

For example, since data protection is state law and Germany is a federal republic with 16 states, the DPAs of the various states are sometimes partly different, but there are common factors in all German states. We have several hundred different DPA regulations on how to access certain information. You need to be an administration and law specialist to cope with all of them. However, they all are mostly based on the following fundamental conditions on how to get legal information:

- The legitimate interest (that means, you have to disclose who is your client and what he needs this data for); and
- The legal interest (that means you or your client must have some credible (or provable) reason for obtaining the wanted information, like preparing for civil or criminal proceedings at court or claim a legal case against the subject. As a proof in its best form a letter of attorney with a clear outlining of the background is acceptable.

If both requirements are fulfilled, normally our authorities have to hand out the wanted information. However, we can just make a request to the competent official and it is a decision of his own legal assessment, whether he finds our arguments or documents acceptable or not. If not, we can go to his supervisor for a short decision, and, in the end, to the administration appeal court, to fight against the decision. This last chance will need at least several months, sometimes even years, and doesn't help really in solving he actual problem. Normally there are no problems with getting information if a legitimate and/or legal interest can be proved.

2. What information is available from what authority?

Germany has a finely meshed registration and information system. Each citizen up from sixteen must have an identity card and each citizen up from his birth is registered at the registration office of his city or village. This means a huge, decentralized authority system. Since Germany is a federal republic with 16 different states the systems are sometimes partly different, but mainly alike. A lot of registers are accessible on various authority levels. Most registers are at the referring local authority. A requesting private party needs mostly to prove its legitimate or legal interest to get access. Only security and financial authorities have the right to use this data pool among each other. Few registers are open. In the following you'll find an overview of the most important authority registers:

- Residential register (locally based; partly open source/needs partly proof of legitimate interest)
- Family registrar data based (locally based; needs proof of legal interest)
- Land registry (locally based; needs proof of legal interest)
- Commercial register (locally based; needs proof of legal interest)
- Register of companies (locally based at district courts; open source for capital companies)
- Small business register (locally based; needs proof of legitimate interest)
- Debtors register (locally based at district courts; open source)
- Bankruptcy register (locally based at district courts; open source)
- Register of associations (locally based; open source)
- Craftsmen register (locally based; needs proof of legitimate interest)
- Chamber of Industry and Commerce (locally based; partly open source/needs partly proof of legal interest)

3. How is information accessed?

In Germany nearly no authority publishes its registers on the Internet. That means all requests to authorities have to be done in written form or personal, since they will normally not provide any information over the phone. These written requests normally need at about two weeks to be answered. On urgent matters we can contact the authorities via phone and fax, and can sometimes get an answer within two days. The fees for each authority request are between 7 up to 30 Euros. In extremely urgent matters there is no other way than direct personal inquiries with additional costs.

4. How much personal data is available in Germany on a digital basis?

Especially if you are from the US, you probably have access to huge data provider companies, which offer a broad range of information about individuals, businesses and their backgrounds. Sometimes you will even find information about real estate property, social security numbers or even the criminal and civil court records. This never can expected in Germany or other European countries.

Of course, as professional investigators we have contracts with the most important German credit information companies as well as to database services like GENIOS or DATASTAR, so that we are able to order some basic information online. These credit information databases are the main open online resources in Germany. However, it is not to compare with the US data providers and it depends very much on the individual case how much information is available regarding a certain person or company. If it is a capital company (Ltd. or Inc.) and if the requested person is a long time in business, we will find probably a lot of information, but if it is a small business and if the person is new in this field, it may happen that absolutely no information is available.

There are few further databases (e.g. postal forwarding data base), allowing us to trace an address history. However in the public databases each person can opt out to be not listed.

5. Phone directories and unlisted numbers

The federal German phone directory is available on the Internet for free at: http://www.dastelefonbuch.de/.

However there are two problems with it. First, you can't look up an address or a phone number and search for a name in connection with a city, and, second, each person can opt out and not be published. It is estimated that we have at about 25% of these not listed records in Germany at the moment.

Special resources are necessary to crack a not-listed number. It isn't legal, of course, but some sources are selling this kind of information for price ranges between 150 to 200 Euros, and more depending on whether it's a landline or a mobile phone.

These special requests have to be handled carefully.

6. Special off-line resources

Some data providers are offering their databases not just online but on CD-ROMs or nowadays DVDs on a regular basis, monthly, quarterly or annually. You can subscribe to the federal registeries, the half-year issued phone record database, the residential registers of major cities or the full text databases of some newspapers. You will spend about 5.000 Euros a year to get all that is possible to get.

However, an EuroSec partner owns the most important CD-ROMs, so we can do address histories back to the beginning of the 1990's. The opt out problem with the CD-ROMs is the

same as with the online directory. But a big advantage of CD-ROMs is segregation of data fields. It is also possible to carry out so-called "backward searches" using available phone numbers for identifying previous phone owners, for instance.

7. How to obtain business information

If the requested company is a capital company, Ltd. (GmbH in German) or Inc. (AG in German), the best source is the federal companies register, to which we are connected online. We get nationwide background information, quickly and deeply, on a company including registration number, set-up certificate, the bylaws, shareholder contracts, shareholders, share capital, corporate mission, managing personnel, annual managing director reports, shareholder meeting reports and most annual accounts. (All capital companies and especially stock corporations have to provide their annual accounts to the commercial register. Although it's an obligation, there are only small penalties for non-compliance for small and mid-sized companies.) Our search costs are easy to understand and are shown before each download.

When old paper files are not completely digitalized, we recommend looking into the register of a company's paper files directly at the local district courts, which sometimes contain more historic information (see next point).

It is much harder to obtain information about small companies. Small businesses are registered only at the local town hall where they are located. Some small businesses have their names listed with the commercial register for special reasons, but that is voluntary. Very often we can find records at the credit information agencies, but not in all cases. If you have just the name of a small business without any address, it might be difficult to obtain more background.

8. How are commercial registers organized?

For a few years the register of companies in Germany has been centralized mainly at the district courts of county cities. Visitors can have a look into the original register paper file and can get a copy, with copy charges.

Each copy costs one Euro per page on an average, depending on local rules. A copy of the register's overview costs between 10 to 20 Euros. The copy of an entire file can reach 50 to $150 USD or more. Therefore we just copy important pages and extract an overview about detailed information in the other pages.

Because it is much cheaper and faster to download files as PDF or JPEG formats via our online access to the federal register of companies, we have avoided original paper copies for several years. Nevertheless, such downloads come with costs and expenses, depending on available files and job oriented demands.

9. Financial information / covered financial investigation

Like in other countries, bank information in Germany is not public and hardly accessible with special sources. Covered financial investigation is not forbidden in Germany. You can phone a bank, stating to be the account owner and ask for information. However, even German banks are prepared for financial “investigative games” (pretexting) and therefore normally don't provide any information over the phone. Some agencies are calling the subjects directly, stating to be from a bank or other financial institution, to obtain information. But even those calls are normally long shots. Therefore, hard-fact financial information can be obtained from:

- Available annual accounts at the commercial register;
- Information from debtor-/bankruptcy registers; and
- Out-of-credit information or debt collection agencies, that may have some experience with the requested person or company.

10. Press and media Information

Nearly all big and well-known newspapers and magazines have online full text databases for at least the last 10 years of their publications. Sometimes they are for free on the Internet, sometimes just accessible with contracts to certain data providers. We can access all big ones.

However the smaller local newspapers are often not accessible via Internet or through data providers. The smaller papers contain more information about the persons and companies in the requested area.

Nearly all local media give the public access to their internal full text databases. Sometimes we can request it via phone and fax, sometimes it's necessary to send a local investigator into the archives. Now and then it's for free, sometimes they are charging for this service. However, a local press research should be included on principle in each background investigation.

11. What's about criminal background checks?

Criminal records are one of the most protected data banks on the federal and state level in Germany. They are available only for police and justice authorities for internal use. There is no legal private way to get any of this information. Only the related target person itself can request its own old records, but not whether there are new investigations or entries into the wanted list. Detailed information including self-request forms are available on the Internet.

The central crime register with entries about sentenced criminals is named 'Bundeszentralregister' and based in the German capital of Berlin. Just the state attorneys and judges have direct access to it, not electronically, but on written requests. The police can request as well, but don’t have direct electronic link either. It's important to know that records for minor offences get deleted automatically, normally after five years, if the person has not been accused and convicted for further crimes in the meantime. Minor offences in this sense mean all offences with a minimum penalty of

less than one-year sentence. Those are most crimes like burglary, assault, fraud, etc. Felonies records are stored up to 10 years; these are for crimes with a minimum sentence of one year and more, like robbery, homicide and arson. Only murder records are stored for lifetime.

Some investigators in Germany are collecting criminal background information illegally from friendly police officers, but both can be punished very hard for that and if this information is delivered abroad, the punishment will be much more painful. Another problem is that the police store just records for police investigations and the relating subjects. It doesn't mean that the subject gets convicted at court later. Therefore, it may happen that a requester receives bad background information about an innocent person, who had been under investigation only.

Criminal information is to be handled carefully. It cannot be used as evidence in court and never can be forwarded directly to a client.

12. What's about civil proceeding records?

Information about civil court records is only available on the district court level and not in a central federal database like in the USA. All types of civil court records are secret and there is normally no way to obtain them. Each court has its own file database, in which normally just the names of the plaintiffs and defendants, a subject line and the referral number are stored. There are some agencies that try to get this information by phoning under pretense, but the information obtained would not be reliable.

On the private side, only lawyers have the right to obtain information about files and details in civil proceedings.

13. Car registration information

The federal car registration database is located at the 'Bundesverkehrs-Zentralregister' at the 'Kraftfahrt-bundesamt' in Flensburg, in the far north of the country. Each police station, local authority and even the tax authority has online access to this database. However, it is absolutely not accessible to the public. On the other hand, the car registration office must hand out information about a car owner, if a citizen is able to prove his legitimate and legal interest.

14. Social Security System/Personal Identifiers/Workplaces

Information out of the Social Security System is top secret and just accessible with special sources, which is not legal, of course. Despite the fact that we have a Social Security Number in Germany, this number is not important for an investigator. In Germany the use of the date of birth as the personal identifier is common. All authorities are storing the DOB in their records and you will find the DOB on nearly each official document.

However the DOB is - for example - not released on a normal residential record request but it's possible to make a special request for that, if you prove a legitimate interest.

Workplace information is also under strict data protection like all other personal information. There is only one legal way to find out an actual workplace of a target person, and that is by making an observation (surveillance).

15. Educational information

High schools, Universities and all other types of educational facilities are refusing any information about their school boys/girls or students, so that titles can only be verified by looking personally and hand made in all year books, if available (not so at high schools).

16. What information is available with the target person's authorization?

Detailed personal information - no matter of which type - is available only under the circumstances described under points 1and 2 above, or with the official authorization of the target person, documented with a full name, address and handwritten signed paper. Under this circumstances, authorities and all other involved institutions have no right to refuse the wanted information.

For more information on the eurosec agency, visit their web site at [www.eurosec-gmbh.de.](http://www.eurosec-gmbh.de)