INTELLENET *News*

Official Newsletter of the International Intelligence Network, Ltd.

Intellenet.org ***Summer 2019***

In this Issue …

Marketing Your Business

William F. Blake

The Internet is a primary marketing tool for the private investigator and security consultant. Historically, if an individual wanted to locate a service or repair business, they went to the telephone directory Yellow Pages. Currently, many telephone companies do not issue telephone directories. Today, the Internet is utilized for many purposes and have become the primary source for business information as it has the capability of providing more business information that the one-line listing in a telephone directory.

During a recent search for potential Intellenet members, names were selected from various sources to determine the professionalism and capabilities of the individual's services. Many searches failed to identify a website for the business. In some cases, the website appeared to be outdated and less than professional in appearance and contained very little information on which to make a decision. Your website is a marketing feature that is part of presenting your business on a professional level. Your website is like your personal appearance. If your website appears similar to a T-shirt and shorts image, people will relate this to an apparent lack of professionalism.

Your website should have a professional appearance and not one that appears to have been constructed by a young person. Any designs or images should be of a high quality and not some that appear to be "cheap" or generic to a general business. Those websites containing "flash" can be distracting and are time consuming to get to the important information on a website. Flash allows for the incorporation of animations and interactive content on the website.

To be informative, selected information should appear on your website. An important item is "About Us" which gives the viewer an indication of your experience. You can also list the experiences of some key employees in this section. "Services Provided" is a list of the business services, either in-house or through a sub-contractor. "How to Contact Us" should provide listing of the business' physical street location, e-mail address, telephone, fax, and cellular telephone numbers. Some business websites provide an e-mail form which can be a distraction to some individuals who prefer telephone or face-to-face contact with a business.

Marketing your business is a continuing process and involves everything that you do as an individual or business. It is your appearance, speech, courtesy and the manner in which you interact with others. This applies to business contacts, attendance at meetings, conference and other assemblies. You're always marketing your business and yourself during any appearance, in private or public.

Peter's Posting

by
Peter Psarouthakis
Executive Director

Summer is now behind us & I hope everyone had a chance to enjoy it. As we move into the fall & winter season our attention is focused on our annual conference to be held in Las Vegas, NV at the Rio Resort & Casino from March 30 to April 2, 2019. If room reservations are any indication, this conference appears to be looking like one of our largest ever. I would recommend making a reservation sooner than later before our room block runs out. The costs for the rooms are $69 per night ($49 room rate plus $20 resort fee). Details about the conference can be found on our website (https://www.intellenet.org/annual-conference/)

We have seen a steady increase in membership referrals over the last few months. We thank everyone for keeping an eye out for qualified members & encourage everyone to keep up the good work. Remember the 10 year minimum investigation experience when referring someone. That experience does not have to be strictly from "PI" experience, but can come from past law enforcement, intelligence, military. If you know of someone & want to refer them to our membership committee send an email to Intellenet@intellenet.org & please include the person's name, contact information & a brief description on how you know them.

I will close out my column reminding everyone that we have an "initiative" program. This program is to help our members when they have a big client & need the support of investigators around the world. We have several of these programs currently operating that have generated a tremendous amount of billable hours for many of our members around the world. If you have a prospective client that you are courting & would like help utilizing Intellenet just send us an email & we will work with you as much or as little as you need. Remember, Intellenet is a business & education network with its main purpose is to help keep your business strong.

Thanks,
Peter Psarouthakis

Welcome New Members!

Lisa Dolan - Flushing, NY

Dennis Eberly - East Petersburg, PA

Dennis Franks - Austin, TX

William Gillis - Boston, MA

Daniel Lowney - Dighton, MA

Joe Peek (reinstated) - Auburn Hills, MI

Daniel Troidl - South Hero, VT

Robert Wigley - Navarre, FL

These are our new members since we last published. To update your membership listing on the web, or in our Briefcase Roster, send info to intellenet@intellenetwork.org.

Carino's Column

by

James P. Carino Jr, CPP, VSM, BAI
Intellenet Founder/ Executive Director Emeritus

AN INCOMPLETE HISTORY OF INTELLENET

THE BEGINNING

In the fall of 1982 my company, Executive Security Consultants (ESC), was invited to submit a proposal for the conduct of background investigations under contract with a major electric power company located in the mid Atlantic states. The invite was suggested by the company's Director of Security, a retired Air Force Special Agent whom I was acquainted with as a result of private sector interface. Oddly, this individual was not part of the decision making process.

Proposal preparation was highly suggestive of a visit. Early on I asked the question as to whether the selectee would be the low bidder and the response was "not necessarily." Buoyed by this non-negative response we discussed further the scope of the project as there was no formal Request For Proposal (RFP)/bid specs to be issued by the power company. Basically, the scope covered all of the 50 states except for the 100 miles radius of corporate headquarters. Those BIs would be conducted by in-house personnel.

Armed with the pertinent information necessary and faced with the formidable task of locating and recruiting in all 50 states contact was made initially with 25 former or retired AFOSI special agents located in 17 states with whom I was maintaining informal contacts. This was a small group to meet the scope but a start. Each was queried for interest (each was in the private sector investigative business) and each was solicited to additional PIs. Of course, this was done by letter and telephone as the internet was not yet up and running. All, were enthusiastic about the opportunity. While the number interested in participating increased somewhat we were still perhaps lacking sufficient US coverage.

A proposal was submitted and shortly thereafter the contract award was made. I note that at the conclusion of my initial visit I was asked why I raised the question about low bid. I responded that I would undoubtedly not be low bid but I could well be the low effective bid as the team I would put together would be professional investigators skilled and schooled in the conduct of background investigations and turn out a comprehensive and professional BI in less time, thereby being more cost efficient. The rather quick announcement of the selected bidder indicated the contractor had been pre-determined and additional proposals were solicited only to meet a minimum quota of three. Of course, a factor would also have been a lack of adequate coverage, a point I attempted to minimize in the proposal. The selectee was the low bidder. However, had they told me the determining factor would be the low bidder, as I stated to them I would have thanked them for considering me but broken off the meeting before it started and there never would have been an Intelnet. When I advised the 25 I was not the successful bidder I suggested this could be the start of something and asked if they had interest in forming a group of investigators. All replied positive and additional new names for members started to flow in – slowly at first. Also, investigative requests for assistance between and among the invited group began to flow and the association, to be officially named Intelnet (the Intelligence Network) was born in early 1983. The initial name OSINET was rather quickly discussed as it was recognized that a "mirror image" of AFOSI globally could never be attained by using only OSI personnel. (NOTE: The name change to Intellenet in 2007 will be discussed later.)

THE VISION

From the outset, Intelnet's vision was to form a worldwide network of private investigators & security professionals, modeled after the Air Force OSI organizational structure of offices throughout the world (where US Air Force interests existed). In essence by sending out "undeveloped leads" (i.e. requests for investigation support & assistance), a network, all former or retired OSI special agents similarly vetted,- *cont. page 4*

trained, and experienced would exist to support one another while still functioning as individual entrepreneurs. Unfortunately, many of those original 25 are now deceased. Emphasis was placed on forming a sole source network as purely an entity to provide professional investigative and security services to the private sector.

THE EARLY YEARS

Growth was slow initially and it became quickly obvious that a network, as stated above, exclusively consisting of former OSI agents could never successfully meet a global reach. Recruitment was expanded to include emphasis on other former federal special agents and select private sector investigative personnel lacking public sector experience but vouched for by fellow members. By late 1985 membership was at 64 members in 33 states with an additional 9 states being covered by "on call" capability and 8 additional specialized skills personnel (TSCM, polygraph, etc.). Absent, however, was international coverage. During this period the first Intelnet Newsletter was published and a consolidated roster was provided all members. During these formative first 3 years there were no annual dues as ESC funded and covered all expenses.

1986 was the year Intelnet began to come of age, with several significant steps taken to ensure sustainability, recognition and growth. The slow but steady growth and the quarterly mailing of a newsletter served as catalysts to spark additional names for membership. It also became apparent that ESC could no longer afford total funding of the network, leading to the introduction of dues, set at $15 per year primarily to cover mail costs. Intelnet also experienced its first dropout, a member who thought dues payments of $15 was exhorbitant since he had not received any billable time during his two years of membership. When I asked how many members he had used on a billable time basis he abruptly hung up on me causing a forever end of our relationship.

1986 was also the year Intelnet was officially registered as a corporate entity. Efforts to be approved as a non-profit entity were denied, thus the formation of a Sub chapter "S" corporation. The availability of the internet also brought about significant change. Members could now communicate quickly, exchanging requests for assistance, establishing websites as well as the exchange of ideas on a real time basis. Also, one day a full loaded computer, courtesy of Dave Parker arrived at my front door. Dave also designed our first website that year. Dave's brother Bill, a very active early member, gave me my first computer use tutorial. (Bill's nephew and Dave's son David is now a member)

Also in 1986 the first Board meeting was held, in Chicago. With local arrangements made by Tom Hampson (since retired but still on the Listserve), other attendees were Brad Penny (d. 2007), Bob Godman (d. 1996), Gary Brown (d. 2012), and Bill Parker. All voluntarily of us paid our own air, hotel, meals and other incidental expenses since there was not yet a fully funded treasury established. Unfortunately, minutes were not kept so no official record exists as to actual discussions or policy decisions. Undoubtedly, the establishment of a formal structure, membership growth, billable opportunities were on the agenda and the first Board was appointed. In addition to the attendees, the Board also included Bill Parker and undoubtedly others whose names are no longer recalled.

1986, possibly as an outgrowth of that initial Board meeting, also saw the implementation of several successful expansion steps. Many of our members were subcontractors for ARAMCO in their conduct of background investigations. Retired OSI special agent Ray Jungers (deceased) who I knew quite well from active duty days headed up the security department thereat. To further expand his investigative pool we exchanged membership lists, resulting in a number of his subcontractor investigators joining Intelnet. This was also our first initiative though one did not use that term back then. Also that year, member Horace Cavitt, based in El Paso TX had a group former GS 1811 investigators he was using to service a government background investigations contract. Through him invites were sent out to his team resulting in additional growth. Several of our former GS 1811's also joined his group.

The last significant growth step of 1986 was taken when Intelnet and an association called Assets 2000 headed by Denis Read established a working relationship. Assets 2000, primarily a European group but also with a few members scattered throughout Asia gave Intelnet its first entry into the international arena. Essentially, Denis is served as the contact points to set forth requests for investigative assistance between the two groups. Circa 1988-89 Read opted to retire and Intelnet offered full membership to all Asset 2000 personnel desiring to affiliate. All but one took advantage of the opportunity.

Cont. page 5

Some key players in addition to Jungers, Cavitt and Read who all assisted in both a quantitative and qualitative membership expansion were former OSIers Brad Penny, Gary Brown, Al Kaplin and Charlie Perkins (all deceased), Bill Cramer and Pete Kalitka (also deceased) and Bill Parker. Bill was the original "go to" person when no other resource was available. His accomplishments too lengthy to describe herein but served. Catch me at an Intellenet Hospitality Suite and I will be more than glad to relate some of his tales which are legendary. Several old timers will remember that Brad Penny who served with me at Aviano AB Italy 1961-64, was my "right hand" virtually since the beginning. Brad wrote the first By-Laws, the internal Code of Conduct, ensured (later) that our conferences ran smoother, and served essentially as our first administrative person – all on a volunteer basis while running a very successful PI business in CA.

By 1990 our membership was about 200, the Supplemental Support List was well established and the D List (corporate security directors and individuals by similar titles and functions) had been created. All were considered members. 1990 was also the year of our first conference. Initially called Regional Conferences 53 members and spouses attended this first gathering, held in the Poconos. Although a full member attendance list is not available, members from MD, VA, DE, PA, NJ, NY, CT and MA attended. As long time, now retired member Denny Crowley noted in a 2003 AFOSISA Global Alliance (newsletter) it was not called the first since we did not know whether there would be a second. This was the second feature article on Intelnet to appear in the Association of Former AFOSI Special Agents (AFOSISA) newsletter. Some of purposes outlined in the first article published in April 1986 which remain current today include:

- *"Professional and timely investigative support*
- *Access to open sources to obtain public records*
- *Specialized investigative assistance in areas of tech security, forensics, polygraph, expert witness, foreign language*
- *An exchange of ideas regarding business related to "selling" techniques, business development and marketing strategies*
- *Identification of potential markets and business opportunities*
- *A quick offering of advice when one has an investigative or security requirement where one may not be completely familiar with*
- *Assistance from those experienced in the preparation of proposals for investigative/security business opportunities and in responding to requests for bid specifications for prospective business"*

Thus, in 7 short years Intelnet grew from an idea emanating from a failed bid to provide investigative services in a background investigation contract to a global network of 200 or so members located in most US states and many key locations globally.

The End of the Beginning

To Be Continued

Thanks

Jim Carino Jr

Peggy's Page

by

Peggy Centonze
Intellenet Administrative Assistant

When Ed asked if I wanted a page in the newsletter, I happily said yes! For those I have not had the pleasure to meet yet, I have been updating the website for over ten years and assisting with membership renewals and conferences over the last six years. You may have seen my name in Intellenet-L Info Brief's from Peter referencing membership renewals or conference registration and I am grateful to have personally met many of you while attending my first full conference in Denver, CO in 2017, this years' conference in Charlotte, NC & look forward to meeting even more of you in Las Vegas in 2020.

Q: *What's the best way to find another member online?* ***A:*** *The Member Finder on www.intellenet.org.*

When's the last time you looked at your online listing? If it's been a while, view your membership listing now to make sure your details are accurate. If you recently moved, got a new email address or just want to add your cell number to your listing, email changes to intellenet@intellenetwork.org or peggy@plh.net and I will be happy to make the website edits as quickly as possible.

Member Finder Helpful Hints

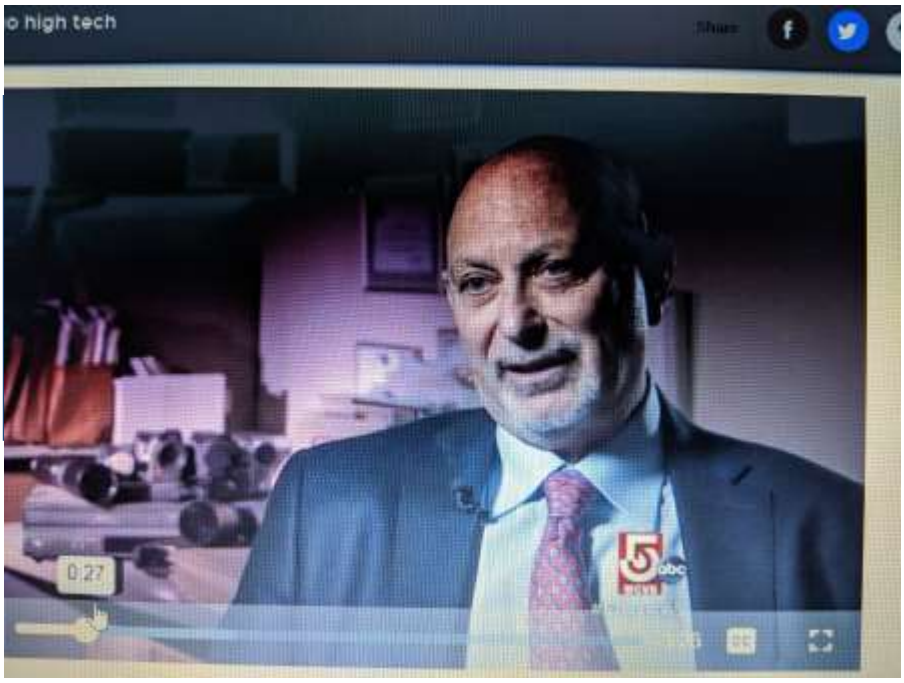
Intellenet launched a new website in 2019 and we continue to work with the developers to make improvements. Have you used the search features on the ***Member Finder*** *page yet to locate a member? The* ***Member Finder*** *page is your first source when looking for someone by Name, Company, Country, Specialty or Language proficiency, among other things. Keep in mind the search results are based solely on data found within member listings and are randomly displayed. For instance, if searching Jim Carino, Jim may be listed as James, so try searching by last name or the most unique information possible. You can search one or multiple fields at one time to narrow or broaden your search. Cities are similar, if you search Alexandria, those with matching mailing addresses will appear, but not necessarily those near that location. To see who is located within 50 or 100 miles of Alexandria, use the "****Search By Radius****" link found just below the* ***Search Members*** *text. This opens a new page with a map. Enter a city name and select fields from the dropdown list like state, country, radius (distance from location), specialty and/or language to narrow the search. Listings appear in alphabetical order by first name, but markers also appear on the map so you can zoom in or out and click on a marker to view member listing details.*

I am here to assist you with any administrative need or question you have, so feel free to contact me anytime by emailing intellenet@intellenetwork.org.

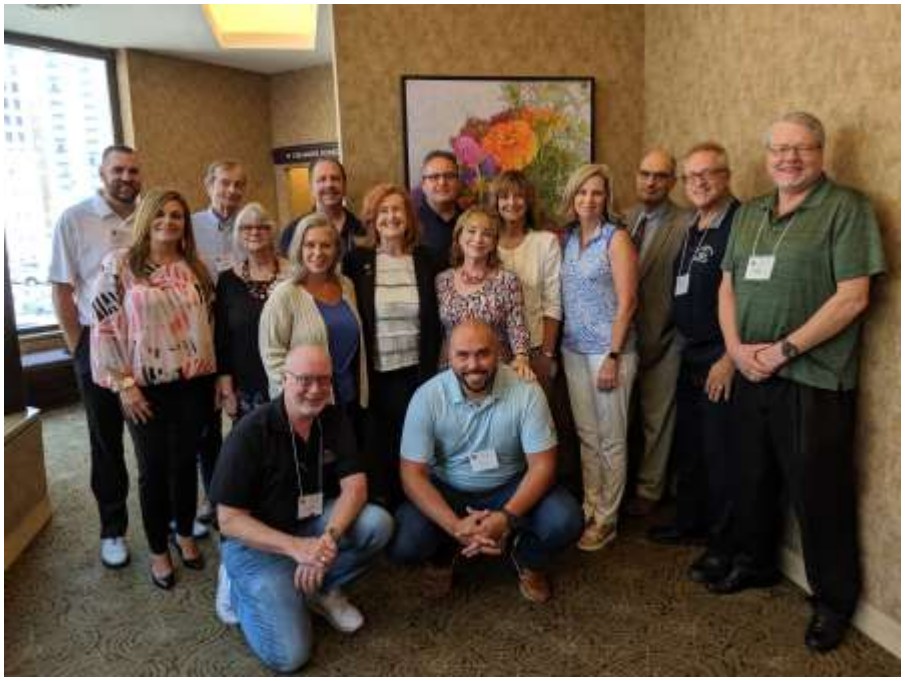
Thanks,

Peggy

Member Photos



Jay Groob interview on Boston Channel 5



Intellenet members at 2019 NALI Conference

Book Review

10 Minutes to Live: Surviving an Active Shooter Using A.L.I.V.E.

By Michael Julian, Intellenet member, CPI, PPS, CSP

"10 Minutes to Live" is a comprehensive examination of the modern active shooter, his motivation & intensions. The book, however, provides the reader much more. As the title suggests, when an active shooter attacks, his or her targets may have only minutes to respond & survive. The acronym A.L.I.V.E. reminds us that those in harm's way must Assess, Leave, Impede, use if necessary: Violence & Expose their position carefully, to escape or defeat their killers & survive.

Julian carefully weaves into his advice proven methods & tactics to not only survive an attack but protect others from harm by using force when necessary. Julian does not shy from advising the reader that their survival may depend upon their ability to recognize the threat & attack first. Though this concept is not necessarily new, the author alters the reader's mindset that survival & the duty to protect others is not only the responsibility of law enforcement, employers & school administers, but is also the responsibility of those who find themselves face to face with the killer. Julian points out that properly using the first minutes after becoming aware of the attack are the most critical to survival.

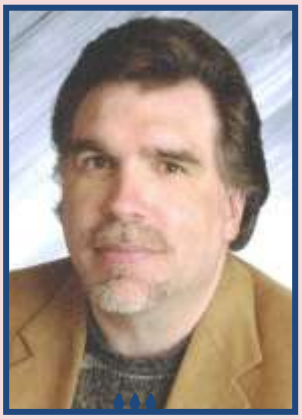
"10 Minutes to Live" is not just about surviving, it is also about living. Julian not only provides the tools needed to survive an attack by providing his readers the courage & strength to live in a dangerous world, but the peace of mind knowing one can indeed survive & in doing so, save others.

READI™ RESPONSE

Kevin McClain, CCDI, BAI recently announced the initial launch of his mobile application connecting investigators and clients in real time scenarios at accident and incident sites. The launch is scheduled for October 1, 2019 and it's not too late to sign up …

All Intellenet members who sign up before launch date will be grandfathered in and will never have a subscription fee!

Kevin already has over 450 investigators in his investigative network and clients are signing up for beta testing. The Phase 1 Launch in October will offer the app to over 300,000 truckers as a part of a strategic agreement with the trucking industry, offering real-time local investigative expertise at accident sites via the app's instant notification capabilities.



If you are ready to be a part of this exciting network or have any questions about READI Response, contact Kevin at 877-532-1152 or email mcclainpi@gmail.com or kevin.mcclain@readiresponse.com.

Internet links & email addresses of interest

"Is It Down Right Now" https://www.isitdownrightnow.com/

Life Insurance Policy https://www.lifeant.com/faq/how-can-you-find-out-if-somebody-had-a-life-insurance-policy-before-they-died/

Access to Official Military Personnel Files https://www.archives.gov/personnel-records-center/ompf-access

Online Detainee Locator System https://locator.ice.gov/odls/#/index

Trusted Traveler Programs https://ttp.cbp.dhs.gov/

Free Public Record Searches https://www.blackbookonline.info/

ISP List https://www.search.org/resources/isp-list/

Boston Police Public Records Request- publicrecordsrequest@pd.boston.gov

Members In The News

"Life Member Harvey Morse did a live interview on the nationwide TV show "Inside Edition" in regard to the Estate of the late Jeffery Epstein. In addition, he has done many press interviews from France, Spain and other countries relative to locating potential heirs. Ari Morse has also had a lot of press in South Florida such as the Miami Herald and other newspapers concerning the same case. Morse Genealogical Services, LLC/ Locaters International, Inc. created a specific website www.epsteinheirs.com for this purpose, and have been receiving calls from around the world".

IN MEMORY

Sixteen-year-old Ryan Driscoll, son of Intellenet member & Massachusetts PI Dennis Driscoll, was tragically killed in a motor vehicle accident on Route 93 in Andover, Massachusetts on June 8, 2019. Ryan was a vibrant young man with an infectious smile and a zest for life that was truly unmatched. He was an honor student who constantly challenged himself to "raise the bar" as well as a student athlete who played both ice hockey and lacrosse. Ryan spent many hours volunteering to help others at local food pantries, homeless shelters, and on the ice with a local sled hockey team. He organized many food drives for those in need and was always willing to help anyone who needed it. Ryan's future endeavors included pursuing a career in law enforcement. Please help keep Ryan's memory alive by donating to the "Ryan Driscoll Memorial Scholarship Fund", because even at such a young age, Ryan knew the importance of helping others. Donations can be made payable to:

Central Catholic High School

Ryan Driscoll Memorial Scholarship Fund

300 Hampshire Street

Lawrence, MA 01841

ISPLA Insights for INTELLENET

by

Bruce H. Hulme, CFE, BAI
ISPLA Director of Government Affairs

In my previous report as this organization's legislative liaison board member, I wrote: "It will be incumbent upon INTELLNET to take positive action as an association to ensure that no provisions of any anti-breach, artificial intelligence, or privacy legislation contain a provision defining private sector investigations as being synonymous with the business of information broker. Presently, the leadership in other national professional associations may not be effectively utilizing their resources to properly face the challenges we will be forced to deal with in the future. Will INTELLENET's leadership and its membership do so?"

The federal legislative branch of our government has failed to enact a comprehensive data breach security bill; however, each of the 50 states has. There will be a strong lobbying effort that any federal bill that eventually passes both the House and Senate contain a preemption provision over states' laws regarding a uniform notification time of security breaches to affected parties.

What's in your wallet? Mega-Hack at Capitol One

On July 29, Paige A. Thompson - a hacker who goes by the name "erratic"- was arrested and charged in the U.S. District Court of Seattle, Washington with a single count of computer fraud and abuse. She had obtained the credit scores, account balances, and security numbers of 140,000 Capitol One customers. The bank also indicated that the data breach also affected 100 million persons in the U.S and 6 million persons in Canada. However, presently Capital One believes that the stolen information was not used for fraud. Most of the stolen information was from consumers and small businesses that applied for credit cards between 2005 and 2019. The breach was discovered on July 19. According to the FBI, the bank was notified of the data having been leaked on two days previously on the code-sharing site GitHub owned by Microsoft. A month previously, a Twitter user with the handle of "erratic" sent Capitol One direct messages warning about disseminating personally identifying information. Rep. Maxine Waters (D-CA), Chairwoman of the House Committee on Financial Services, issued the following statement about this data breach that exposed account information.

"This data breach shows that it's not just big technology companies and credit reporting agencies like Equifax that are vulnerable to hacking and data breaches – big banks are vulnerable targets as well. As this is not the first incident in which Capital One's customer data was exposed, we need to understand what bank regulators have been doing to ensure that this bank, and other banks, have strong cybersecurity policies and practices. We must also understand what bank regulators are doing to ensure strong oversight of third-party technology providers that banks work with.

"As we learn more about this incident, I plan to work with my colleagues and take action in the Financial Services Committee on legislation to improve oversight of the cybersecurity of financial institutions.

"This massive data breach also underscores how important it is that the consumer credit reporting bills that the Financial Services Committee recently passed become law so that any consumer affected by a data breach is not further harmed. Among other things, the bills the Committee passed ensure that consumers can get a free copy of their credit score, provide better tools for victims of fraud, and make it easier for consumers to get errors on their reports corrected."

The House Financial Services Committee and the Federal Trade Commission are two governmental entities that bear close monitoring. The spate of recent data breaches has resulted in the House: ***cont page 12***

Financial Services Committee passing in July a series of consumer credit reporting measures.

H.R. 3642, the "Improving Credit Reporting for All Consumers Act," *introduced by Rep. Alma Adams (D-NC)- Addresses burdens consumers experience when removing errors from their consumer reports, including by providing a new right to appeal the results of initial reviews about the accuracy or completeness of disputed items on the report. The bill empowers consumers by clarifying injunctive relief is available to ensure reporting errors are actually fixed when a consumer is harmed.*

H.R. 3618, the "Free Credit Scores for Consumers Act of 2019," *introduced by Rep. Joyce Beatty (D-OH)- Directs the nationwide CRAs to give consumers free copies of their credit scores that are used by creditors in making credit decisions, as determined by the Consumer Bureau, or if not practicable, educational credit scores whenever consumers obtain their free annual consumer reports. A consumer can get their free credit score once a year, and they can get a free credit score if they have reason to believe that their file contains inaccurate information due to fraud.*

H.R. 3622, the "Restoring Unfairly Impaired Credit and Protecting Consumers Act," *introduced by Rep. Rashida Tlaib (D-MI)- Would, among other things, establish the right to free credit monitoring and identity theft protection services if a consumer is a victim of identity theft, fraud, or a related crime, or harmed by the unauthorized disclosure of the consumer's financial or personally identifiable information.*

H.R. 3614, the "Restricting Use of Credit Checks for Employment Decisions Act," *introduced by Rep. Al Lawson (D-FL)- Would generally prohibit employers from using credit reports for employment decisions, except when a credit report is required by local, state, or Federal law or for a national security clearance.*

H.R. 3621, the "Student Borrower Credit Improvement Act," *introduced by Rep. Ayanna Pressley (D-MA)- Removes adverse credit file information relating to defaulted or delinquent private education loans for borrowers who demonstrate a history of timely loan repayments for these loans. The bill would require repayment plans be affordable and reasonable and permits reasonable interruptions in the consecutive repayment periods for those facing unique and extenuating life events, such as service members who are receiving imminent danger or other special pay duty when deployed.*

H.R. 3629, the "Clarity in Credit Score Formation Act of 2019," *introduced by Rep. Stephen Lynch (D-MA)- Clarifies oversight of the development of credit scoring models by directing the Consumer Bureau to set standards for validating the accuracy and predictive value of credit scoring models. The bill would also require the Consumer Bureau to study the impact of having more non-traditional data on consumer reports and the use of alternative data in credit scoring models*

Equifax Reaches Settlement Over 2017 Data Breach

On July 23, 2019 it was reported that Equifax had agreed to pay up to $700 million to settle numerous federal and state investigations regarding its 2017 massive consumer data breach of 147 million American's sensitive personal identifying information that included Social Security numbers, dates of birth, credit cards held, and other confidential information. The breach affected more than half of the adult population in the U.S. To date, the personal data stolen from Equifax has yet to appear for sale on the "dark web" according to some security experts. It is thought that a foreign intelligence agency breached Equifax for espionage purposes. The sanctions not only include payments to affected consumers but include fines to federal and state regulators and require changes to the credit reporting agency's business practices. The settlement also provides extraordinary injunctive relief, far beyond that obtained in any other similar data breach case. The size of the fund dwarfs all previous data breach settlements; the specific benefits purportedly compare favorably to what has been previously obtained, including:

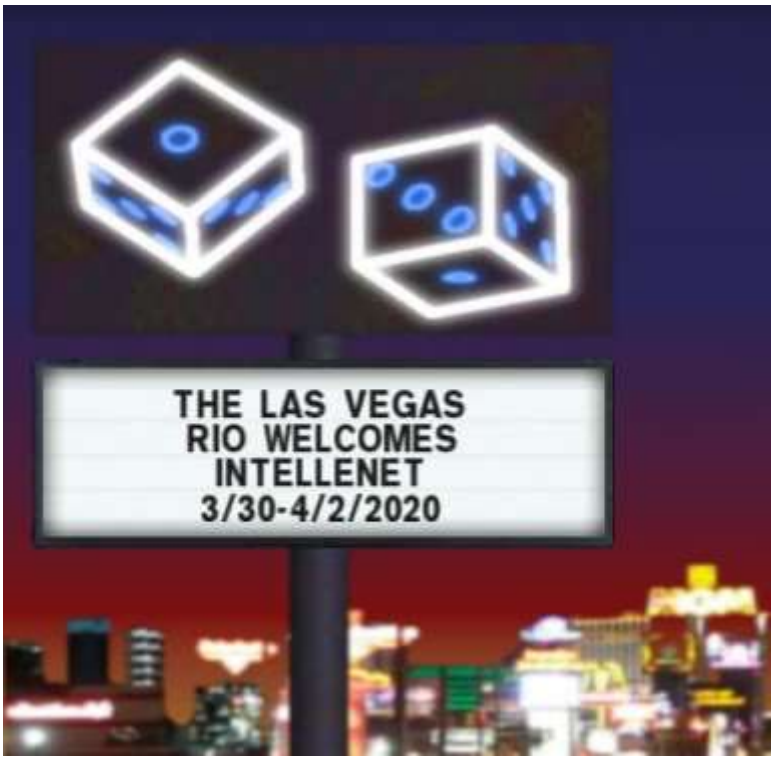
A $20,000 cap on out of pocket losses.
Compensation for up to 20 hours of lost time at $25 per hour.
Four years of three-bureau credit monitoring that would cost each class member $1,200.

Cont. page 13

An additional six years of one-bureau monitoring that would cost each class member $720.
$125 in alternative compensation to those who already have monitoring.
Reimbursement of 25 percent of the price paid by class members who bought identity protection services from Equifax in the year before the breach (notwithstanding that their claims were dismissed by this Court).
Access to seven years of assisted identity restoration services.

Equifax also agreed to spend a minimum of $1 billion for cybersecurity over five years and to comply with comprehensive data security requirements. Equifax's compliance will be audited by independent experts and subject to the Court's enforcement powers. Implementation of the proposed business practice changes should substantially reduce the likelihood that Equifax will suffer another data breach in the future. These changes address serious deficiencies in Equifax's information security environment. Had they been in place on or before 2017 in accordance with industry standards, it is unlikely the Equifax data breach would ever have been successful.

MAKE YOUR 2020
CONFERENCE HOTEL
RESERVATIONS HERE
https://book.passkey.com/gt/217467258?gtid=29c69ab1df2dc0329786d11d77c39e84



SIM Jacking

by

Michele Stuart

What just happened? I can only imagine that may have been the first thing many people thought when they woke up, their phone(s) didn't work, their social media and email accounts were taken over, passwords changed, money or bitcoins were moved from their accounts. So, what is SIM Jacking? It is really about social engineering. Someone calls your cellular provider acting like you and gets your SIM card assigned to a new phone. Once this is done, they have control of your phone and now can easily move on to taking control of most, if not all, of your digital life. Think about it. How many of your accounts are associated to your cell number? How many accounts do you have set up where you have it listed for password recovery or 2 factor authentication and have a text code sent to your phone?

One of the biggest platforms being hit by SIM hijackers is cryptocurrency. Using your text-based account recovery options they will log into your crypto account, seize the funds within the digital wallet and move the currency to their own wallets. However, it isn't just cryptocurrency but your good old fashion bank accounts. Also, we have the blackmail market arena coming full force, with the bad guy having access now to online social media platforms which give them access to photographs or private messages that someone may not want anyone to see.

So how are they doing it? A couple different ways. As mentioned earlier, by a simple social engineering call to your carrier or even reverse, a call or email to you by someone acting like your carrier. The amount of information that can easily be gleaned off open sources is a huge source of data for the 'bad guy'. Also, an alternative way is they pay someone on the inside of a cellular company to assist with the SIM card fraud. Think about how many companies have customer service centers located outside the United States. Their income is low and someone offers them a substantial amount of money to conduct this fraud for them. One cellular employee came forward under anonymity and said she had been contacted through Instagram and was offered $5000 for 25 new account pins or secret answers. In May of this year, the DOJ took down "The Community" which was a group of nine people (eight Americans and one Irishman – aged between 19 and 28 years) working together SIM swapping. Two of the nine accused were former AT&T contract employees and one former Verizon employee. They were found to be providing customer private information for bribes. Just this year, a college kid from Santa Clara County, California, by the name of Joel Ortiz is the first known individual to be sentenced on a SIM swapping case. Accepting a deal for 10 years, he admitted to hijacking around 40 victims accounts and stealing more than $5 million dollars.

Another problem is it comes down to a huge training issue. Many of these cellular companies are not trained on the art of social engineering and how in-depth it can be. How do you know? The first indicator is suddenly the loss of cellular service, no incoming or outgoing calls, texts or emails. If you notice this, immediately contact your cellular provider and then begin checking all of your accounts, change the passwords and remove your cell number as the contact number for recovery. Utilizing a secondary (anonymous) phone number / app is a suggested way to control this from happening. There are numerous apps that provide this service such as Burner app (paid – allows calls, texting and call forwarding), Tossable Digits (paid – supports call forwarding, calling rules and recording capability, numbers locally or in 60+ countries), Talkroute – used for businesses (paid – allows call forwarding to more than one phone, customized greetings, create extensions for departments and employees, texting, check voicemail by email / browser or phone) and then of course there is Google Voice.

Another proactive thing you should do is call your cellular provider and disable porting. Make it known you only want changes to be done ONLY if you are in person in a store. Utilize a password manager program (https://www.digitaltrends.com/computing/best-password-managers/) and make sure you use different passwords on all your accounts! Initiate a SIM lock, set a password/pin on your account and all accounts associated to your account. Close your online account and ask provider to block future registration. Additionally, create a secure email associated ONLY to your cellular provider.

Don't just think by using just a regular 2F is safe – upgrade to a secure 2FA method such as: Yubikey, Google Authenticator or U2F security keys. ***Cont. page 15***

A victim, Bob Ross, had $1 million dollars stolen within minutes of his SIM card being swapped. Once that occurred the bad guy immediately took over his Gmail account by using "forgot password" whereas he then was able to glean control over his financial accounts. He and other victims created a website to help victims: https://stopsimcrime.org

"StopSIMCrime was started in 2018 by SIM crime victims to raise awareness about the fast-growing problem of SIM crimes, be a resource for victims, and effect change through legal efforts." The FBI also has a Cyber Crime report page for SIM crimes: https://stopsimcrime.org/resources/988/

Every day it seems a new way is found to steal our personal and financial information. The only thing we can do is try our best to make it as difficult as possible – don't be the easy victim!

P.S. JUST as I finished typing this article I received this text from a friend of mine:

Michèle my email got hacked so my Netflix Hulu Amazon and credit card all got hacked. I changed my passwords but do you think I'm ok? Or should I get a new email account?

Take the time and protect yourselves. When this happens, it is such a mess and so time consuming! Now off to help my friend.

About the author:

Michele Stuart has 28 years of investigative and training experience. Beginning her career in financial investigations, she then formed JAG Investigations, Inc. in 1997. Ms. Stuart's area of expertise includes OSINT, counter intelligence, insurance fraud investigations, financial investigations, threat assessments, due diligence, organized retail crime, corporate and competitive intelligence.

Ms. Stuart consults and trains federal, state and local law enforcement agencies, the military intelligence communities, fortune 500 companies as well as the financial and insurance industries in open source, social media and threat assessments / mitigation. She has been an Instructor at Quantico (FBI Academy) for International

In 2017, Ms. Stuart partnered with Pennsylvania Office of Homeland Security creating a program "Keeping Kids Safe", training administrators, principals, teachers, SRO's and parents on the dangers of online and social media activity, predator grooming as well as the dangers of applications / cellular security.

The Failure of PI App Trustify and it's Impact on the Integrity of the Industry

by
Nicole N. Bocra/Gray

The brainchild of tech startup entrepreneur Danny Boice was dubbed "Uber for Private Investigators." Prompted by his negative experience working with an independent private investigator who he hired to keep tabs on his child during a tumultuous divorce, Boice developed and launched an app that provided affordable private investigator services from vetted private investigators. On June 1st, 2015, Boice and his new wife Jen Mellon launched the Arlington, Virginia-based app FlimFlam, later rebranded as Trustify.

This company did not have a private investigators license, initially offered one-hour private investigator jobs for $59, allowed the user to be anonymous, allowed for communication with the private investigator through the app, and claimed to retain 2,000 private investigators in the greater Washington, DC area. Private investigators across the country gasped.

Trustify raised a slew of concerns in the investigative community at its launch. Boice had a tech startup background, co-founding virtual conferencing service Speek, and started and sold the Jaxara Group. Mellon's background was in child welfare, highlighting Boice's original inspiration to develop this app. Neither had any experience or insight into the world of private investigation beyond Boice's negative experience during his divorce. Based on the structure of the new company, skeptical private investigators doubted they had consulted with anyone in the industry in the development process.

Beyond the pair's lack of experience in the field of their app, investors jumped on board. However, at the time the greater Washington, DC area did not have 2,000 licensed private investigators. Licensing varies by State and in some, licensed private investigator contracts are required to be two-party contracts between the private investigator and the client. Boice managed to maneuver around this and the fact that his company did not have a license by saying the app was a broker service, not a private investigator service. However, the license-compliant private investigator -client relationship in which the client remains anonymous not only harms the trust, integrity, and accountability of this relationship, but also skates on thin ice with this licensed relationship requirement.

The private investigator community also worried that charging $59 for hour jobs cheapened the profession and created unreasonable expectations from clients that jobs can be completed in such a short time. Boice and Mellon said at the launch that soon the app would allow clients to track the geolocation of the private investigator in real time to make sure they were working. Private investigators worried that this would put their professional peers at risk and emphasized that licensed private investigators were required to extensively document their work to be in compliance with their license. The private investigator community doubted Trustify could be a viable product in the industry.

Despite criticism from licensed private investigators nationwide, the app's June 1st, 2015 launch brought in over $1 million and the company was valued at $5 million. By 2017, Trustify's corporate office appeared on the cutting edge of modern and venture firm Anchorage Capital bought nearly $5 million of company stock on May 22nd, 2017. When approached to invest more, Anchorage Capital said they would not until Trustify reached the $15 million threshold.

Meanwhile Trustify employees were becoming suspicious that their company might be falling apart. In August of 2017, shortly after Anchorage Capital's investment, Boice and Mellon bought a beach house in Cape May for $1,275,000. The two became notorious around the office for their extravagant– ***cont. page 17***

purchases including expensive vacations & a documentary film to be made about themselves & about their marital turmoil that spilt over into the workplace. Employee turnover was high because people were fired for disagreeing with the company's founders & promoted based on loyalty rather than skill. Trustify promotional materials included the logos of companies that employees knew they did not partner with.

A past employee reported on GlassDoor, "Leadership of the company lack fundamental communication & management skills. There are overwhelming redundancies in titles & roles at the top of the company, yet no one really operates the company. The background & skillsets of the management team have huge gaps in experience, which clearly translates in the strategic day-to-day operations of the company."

A former account manager agreed on GlassDoor, "Upper management was not involved in the day to day operations; therefore didn't understand why there was ever any problems."

In June of 2018, Anchorage Capital received an email purportedly from fellow Trustify investor Nfluence. Nfluence said they had approved $7.5 million for Trustify, pushing the app company to the $15 million threshold. Anchorage Capital bought over 600,000 more shares before they were contacted by the actual Nfulence & told that they had not sent that email back in June of 2018. On closer inspection of the email sender, the email was sent from a .co address rather than Nfluence's .com address. Anchorage Capital called Trustify to get some answers that they would never receive.

In October of 2018, while Boice reported that Trustify had raised over $20 million in equity, vendors, private investigators & staff were going unpaid. On November 8th, 2018, public affairs firm Dini von Mueffling sued Trustify for over $240,000 for unpaid bills & damages. This was not the only company pounding at the door demanding payment. Trustify's landlord JBG Smith Properties, BIGFish Communications, ADP, Bill.com, Hubspot, Fond, Kastle Systems, Buckley Sandler LLP & many of the app's private investigators had been left unpaid by Boice and Mellon.

On November 15th, 2018, eight of Trustify's staff confronted their founders about their direct deposits not coming through. Boice left to go to the bank to get everyone's checks & never returned. Employees were notified via email on November 26th 2018 that they had all been fired, the office was locked & the company ceased operations. These eight former employees joined the list of lawsuits filed against Boice & Mellon.

Trustify failed because its co-founders built an app with no understanding of how the private investigative industry operates & because they siphoned company funds for personal use. Boice transferred $750,000 of Trustify funds to his own LLC every year & the couple regularly used company funds to support their extravagant lifestyle, neglecting the interests of their employees, vendors & shareholders. Their business structure did not cultivate the necessities of success, valuing employee loyalty to the co-founders over what employees could actually contribute of value to the company. Management was lacking, knowledge & skillset gaps ran rampant & communication was poor.

The fear of the failure of this app is that it hurt the integrity of the private investigator industry in the eyes of the public & created unrealistic expectations of PIs in the eyes of the consumer. However, it did vindicate private investigators who spoke out in skepticism of the app & it did demonstrate that working directly with a licensed private investigator without anonymity yields better results. Licensing requirements & due diligence exist to protect consumers & when these industry standards are shirked, the quality of services provided erodes.

Could a workable Uber for private investigators exist someday? Possibly, but it would have to be developed in collaboration with actual professionals with extensive experience in the field of private investigation, it would have to be in compliance with licensing requirements, and it would have to set realistic expectations for cost and for how long an investigation will take. Private investigation has never been quick, cheap, and convenient work, which in many ways puts the industry at odds with tech startup and app industry objectives. It is far from impossible that these industries could be reconciled through tactful collaboration.

The National Epidemic of Identity Theft

by
John M. Gaspar

Tic Toc, Tic Toc, two seconds have gone by and statistically there is a new identity theft victim (ITV). ITV is a National epidemic; many experts agree that Americans as compared to other Countries are three times more likely to fall victim to identity theft. To put this in perspective, next time you are shopping at your local Mall look around you and pick 14 people. Use your psychic superpower and you determine that none of the 14 fell victim to Identify fraud. You are elated and then you get an alert from your bank that you fell victim to Identity theft. One out of every fifteen Americans have their Identity stolen. Unlike lightening, identify theft can strike more than once. One in five Identity Theft Victims (ITV) revisit that vulnerability of having their identity stolen. Most of us don't realize what an epidemic ITV is. Millions of children and family members who have passed are also victims of Identify theft? The Elderly is one of the most common targeted groups of Identity Theft. So many State Laws have upgrade punishments for crimes against the elderly in an attempt to deter crime. There are best practices that can minimize your risk of being an identity theft victim (ITV).

Prevent being an ITV by applying preventive measures:

Protecting personal data

Computer Practices

- *Use a firewall and secure browser.*
- *Don't download files from strangers.*
- *Update current virus protection.*
- *Password-protect any personal or financial information.*
- *Avoid automatic log-in processes (which store your account name and password).*
- *Passwords*
- *Create secure random passwords*
- *Use different passwords for different accounts*
- *Do not write them down in accessible areas to view.*
- *Apply Activity Alerts on your bank relationships*

Shred bills and documents with personal information.

Take prescription labels off the bottles before you discard them.

Phone calls- Do not give personal information over the phone unless you are sure the call is legitimate. If someone asks you to verify information, ask them to give you the information. If you are comfortable, verify it and do not add additional information.

**Social Media (SM) awareness – people can harvest information from your SM account(s)including but not limited:*

- *Age and or dates of birth*
- *Pets names*
- *Children and family members' names*
- *Names of School you attended*
- *Sports teams*
- *Favorite movies*

Cont. page 19

What do I do if I become a victim of Identity theft and Fraud?

Contact the FTC and get started with a recovery plan: *https://www.identitytheft.gov/*

Free Government Resources include: *https://www.bulkorder.ftc.gov/publications?f%5b0%5d=field_campaigns%3A1587*

If your Social Security number was used to file a tax return to the IRS:

IRS TAX FRAUD WEBSITE
https://www.irs.gov/newsroom/taxpayer-guide-to-identity-theft
Identity Theft Contact Information for CREDIT REPORTING AGENCIES
https://www.transunion.com/fraud-alerts
https://www.experian.com/fraud/center.html
Experian: www.experian.com to add an alert and view your report immediately; 1 888 397 3742.
Equifax: 1 800 525 6285, www.equifax.com.

TransUnion: 1 800 680 7289, www.transunion.com.

Credit Reporting Agencies (For a family member that has passed)
Immediately contact all three national credit reporting agencies by telephone to report the death: Experian (888-397-3742), Equifax (800-685-1111) and TransUnion (800-888-4213). Request the credit report is flagged as "Deceased. Do Not Issue Credit"
Sample letter- http://www.meyercapel.com/sites/default/files/Notification-of-Death-Sample-Letter.pdf
When reporting the Identity Theft (Fraud)to the Police
As a Detective Supervisor (OIC) working for Sheriff Donald Fleming at Flagler County Sheriff's Office Economic Fraud Division and a NYPD Major case Squad Detective I was surprised to see how little the Police and Prosecutors know about Fraud, identity theft Investigations, and theft schemes.

Tips from me when talking to the Police

- *If you are elderly report the crime with a competent trusted family member.*

Do not assume that a uniformed Police Officer will know how to navigate your incident at first or even designate it as a crime. In most jurisdictions you can ask the officer to make an Information Incident Report if the Officer doesn't classify the event as a crime.

- *Come prepared and provide a timeline with a chronology of events that include:*
- *Dates / Times, Places of the incidents and other case related information (credit card numbers, statements, etc.)*
- *When and who you spoke to at the bank and or credit card companies. Provide their full names/ titles, phone numbers, emails and other contact information. Also provide a brief account of what was said.*
- *When the Police ask you questions answer the who, why, when, how and why if applicable.*
- *Get the officer's full name (s), phone numbers and email addresses when possible (obtain a business card if available).*
- *Ask the officer what you can do to help yourself.*
- *Ask them what is the Detective's name that will be assigned to your case and if he/she will be contacting you and when.*
- *Do not give them unrelated information or spend time on the phone talking with them about things other than the case.*
- *Summary*

Tic Toc, Tic Toc, two seconds have gone by and statistically are you going to be a victim of identity theft (ITV)? Be vigilant to prevent and or terminate your vulnerability to identify theft fraudsters. In addition, be tenacious during the process. Understand it may take time to reverse the financial injury.

Cont. page 20

**Some of that information noted above may be used as your security questions. Control your settings and your content.*

References

https://www.acfe.com/

https://www.acfe.com/article.aspx?id=436

http://www.leg.state.fl.us/statutes/

https://www.consumer.ftc.gov/features/feature-0014-identity-theft

https://www.bulkorder.ftc.gov/publications/identity-theft-recovery-plan

About the author

John M Gaspar, B.S, M.S, CFE, BAI CSI is a licensed private investigator in the State of Florida. Presently the President of All Florida Investigations & Forensic Services, Inc. He is a former President of the Society of Professional Investigators (SPI), current board member of FAPI, Intellenet Net Education Board BAI Program Director , former Kesier University Academic Dean & Department Program Coordinator for CSI, St John's University adjunct professor C.J, Bethune Cookman University adjunct professor C.J, retried Daytona State Colleges Adjunct Professor and FDLE Instructor for advanced and specialized courses. John is a retired NYC Detective working in Major Case Squad, Retired Flagler County Florida Detective Supervisor in charge of the Economic Crime Division. He has written curriculum for FDLE, NYPD, Keiser University Daytona State College on Criminal & Crime Scene Investigations. John's published works include: Fraud Magazine November/ December 2013 Volume 28 the "Shutter Bug case" ($800,000 Construction Fraud Scheme).

http://www.afipi.com

Tentative 37th Intellenet Annual Conference Schedule of Events March 30 – Apr 2, 2020 As of September 11th

Sunday March 29, 2020

4:00 PM	*Board of Directors meeting*

Monday, March 30, 2020

7:30 AM - 8:00 AM	*Check-in*
8:00 AM - 9:00 AM	*Welcome, Introductions, Overview; Peter Psarouthakis & Jeff Stein followed by personal Intro ductions by attending members.*
9:00 AM - 12:00 PM	*Nicole Gray, Daniel Loper and Michele Stuart – Session 1: Aspects of a Fraud Investigation – from A to Z In this presentation our firm is engaged to investigate a new fraud case involving financial exploitation. This case has three key components: the financial fraud; obtaining & analyzing digital evidence & identifying & reviewing open source intelligence.*
12:00 PM - 1:30 PM	*Lunch on your own*
1:30 PM - 4:00 PM	*Nicole Gray, Daniel Loper & Michele Stuart - Continued*
4:00 PM - 4:20 PM	*John Gaspar - Board Accredited Investigator Certification*
5:30 PM	*Cocktail party*
7:00 PM	*Welcome dinner for all paid attendees*

Tuesday, March 31, 2020

8:45 AM - 9:00 AM	*Additional Opening Remarks, Introductions for new attendees*
9:00 AM - 10:00 AM	*Barry Ryan - The Future of our Industry*
10:10 AM - 10:45 AM	*Bruce Hulme - Legislative Updates*
10:45 AM - 12:10 PM	*Wesley Clark - Investigative Statement Analysis*
12:10 PM - 1:15 PM	*Lunch*
1:15 PM - 2:20 PM	*Tony Olivo - AEGIS:Beyond Surveillance-Using State of the art technology for security & video analytics*
2:20 PM - 3:20 PM	*Lisa Dolan - Growing your Security Business, including marketing and sales techniques.*
3:30 PM - 4:30 PM	*Panel of International Investigators – Discussing overseas/international perspective on investigations & what can & can't be done in their respective countries*

Wednesday, April 1, 2020

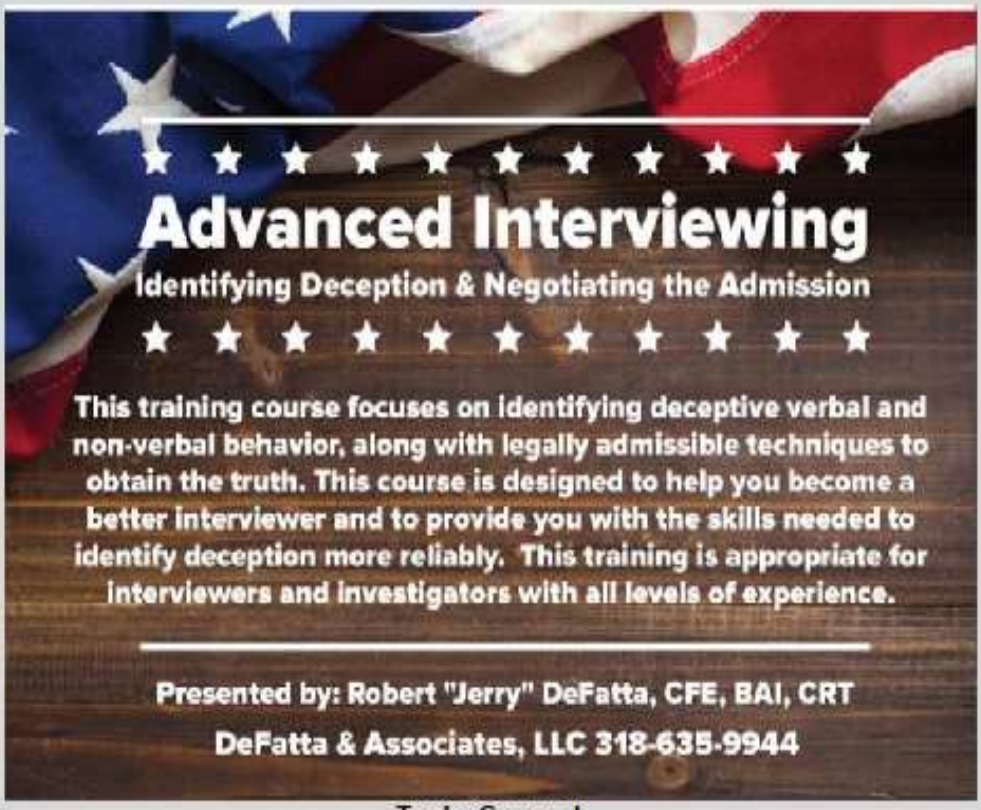
9:00 AM - 9:15 AM	*Announcements*
9:15 AM - 12:30 PM	*Michael Julian - ALIVE; Active Shooter Survival Training*
12:30 PM - 1:30 PM	*Lunch on your own*
1:30 PM - 2:30 PM	*Kelly Riddle - "Cases That Can Land You in Jail"*
2:30 PM - 3:30 PM	*Eric Flores - Kidnapping Express*
3:30 PM - 4:30 PM	*Kitty Hailey – Ethics*
5:30 PM	*Cocktail party*
7:00 PM	*Gala Dinner for all paid attendees: Speakers, awards, scholarships, auction, etc.*

Thursday, April 2, 2020

9:00 AM - 10:30 AM	*"Thomas Brooks; Probate Investigations - an overview of "how to" investigate disputes involving a descendant's estate upon their death. We often hear about someone changing their will & giving all their money to their housekeeper…cutting out the family. Presentation provides an example of how this occurs & how to invalidate a Will. I also show "how to" market your service in this area to Trust Companies and Attorneys."*
10:30 AM - 11:30 AM	*Kelly Riddle - Marketing your business to make money*
11:30 AM - 12:00 PM	*Closing Remarks– See you in 2021 in ???????*

Calendar of events

9/25-9/26	*Minnesota Association of Private Investigators Conference* *https://www.mapi.org/* *All Intellenet members are welcome to attend at MAPI Member rates*
10/1/19	*Michigan Council of Professional Investigators Seminar* *https://mcpihome.com/index.php*
10/5/19	*Washington Association of Legal Investigators Conference* *https://wali.org/conferenceannual.asp*
10/13-10/15/19	*Osmosis 2019 Conference* *https://www.osmosiscon.com* *Discount code of 19INTEL saves INTELLENET members $100 off registration*
10/24-10/25/19	*Alabama Private Investigators Association Conference* *https://apianow.org*
11/7-11/9/19	*North Carolina Association of Private Investigators Conference* *https://www.ncapi.com/*
11/8-11/9/19	*NEPIN/Intellenet 2019 Fall Seminar, Beverly, MA* *See agenda & registration form on page 24-25 of this newsletter*
11/12-11/14/19	*Southern California Fraud Investigators Association Conference* *https://scfia.org*
2/4-2/7/20	*Florida Association of Private Investigators Conference* *https://myfapi.wildapricot.org/*
3/30-4/2/20	*Intellenet 37th Annual Conference, Rio, Las Vegas, NV* *https://www.intellenet.org/annual-conference/*



Topics Covered:

♦ Review of good interview techniques ♦ Understanding Deceptive Attitudes ♦

Identifying Deceptive Verbal Responses ♦ Identifying Deceptive Body Language ♦

Techniques for Obtaining Admissions

Cost: $93.50 - if paid in advance and $110.00 - day of event if available.

Date: Friday, October 4, 2019

Time: 8:00 AM—4:30 PM

Location:

Courtyard by Marriott

2421 Acadian Thruway

Baton Rouge, LA

To Register -

Contact Jerry DeFatta - 318-426-0199 or e-mail **jerry@defattapi.com**

North East Professional Investigators Network 2019 Fall Seminar

hosted by Intellenet

Friday/Saturday November 8 & 9, 2019

Cummings Center Conference Room

100 Cummings Center, Suite 221E

Beverly, MA 01915

ATTENDEE REGISTRATION FORM

Agenda & Speaker info on next page

Full Registration includes lunches & breaks

- **Early registration thru Oct. 15, 2019 . . . . . $120.00**
- **Registration after Oct. 15-Nov. 8, 2019 . . . . . $150.00**

PRE-REGISTRATION REQUIRED-55 seat limit

ALL PROCEEDS BENEFIT RYAN DRISCOLL SCHOLARSHIP FUND

PLEASE CHECK WHERE APPROPRIATE:

Intellenet member _____ **Member of State/National Associations**:_____

Spouse/Employee/Guest of Member _____

OTHER - Please state qualifications _____

METHOD OF PAYMENT:

Check Enclosed (Payable to Intellenet)

TOTAL DUE BY CHECK: _____

LAST NAME: _____ **FIRST NAME:**_____

FIRM NAME: _____

ADDRESS: _____

CITY: _____ **STATE:** _____ **ZIP:** _____

TELEPHONE: _____

E-MAIL: _____

Mail to: ***Intellenet , c/o Ed Spicer, 300 Andover St., # 108, Peabody, MA 01960***

EMAIL CONFIRMATION WILL BE SENT UPON RECEIPT

QUESTIONS: Call Ed Spicer 978-473-4154 or ed@oceanstatesinv.com

Friday Nov 8, 2019 schedule

7:30 AM	**Check in, networking & coffee**
8:15 AM	**National Anthem- Boston Bruins singer Todd Angilly**
8:30 AM	**Maneuvering Indigent Criminal Defense Investigations in Mass-Dan Collins**
10:45 AM	**Branding your PI/Security Company thru Social Media- Robin Pinzone**
12:00 PM	**Lunch served onsite-Lunch speaker TBD**
1:00 PM	**Public Records Presentation- Greg Stewart, Office of the Secretary of the Commonwealth**
1:45 PM	**How forensics can help your investigations- Brian O'Hara**
2:45 PM	**Executive Protection 101-Bill Connors & Cleve Coats**
4:15 PM	**End for day- Networking @ Acapulcos, 900 Cummings Center, Beverly (next building)**

Saturday Nov 9, 2019 schedule

7:30 AM	**Networking & coffee**
8:00 AM	**Retaining video date/time stamp when transferring from camera to computer-Jim Doyle**
9:00 AM	**Enhancing your investigation with Bug Sweeps-Milt Shull**
10:00 AM	**Conducting Background Investigations-TBA**
11:00 AM	**Hands on Cell Phone Forensics- Dan Loper**
12:00 PM	**Lunch served onsite-Lunch speaker TBD**
1:00 PM	**Hands on Cell Phone Forensics- Dan Loper**
2:30 PM	**Sexual Assault Investigations- Elaine Gill**
4:00 PM	**Seminar concludes**

Unscheduled speaker(s)- Assistant Majority Leader Senator Joan Lovely and/or State Representative Paul Tucker will speak to attendees on pending bills in the legislature that effect Private Investigators.

Exact speaking day/time will depend on their State House schedule.

WHY BECOME A BOARD ACCREDITED INVESTIGATOR?

INTELLENET is the first international professional investigative association to offer a unique credential specifically designed for professional investigators.

MEMBERSHIP BENEFITS

- **Expanded professional network & opportunities to showcase your expertise at professional and global events.**
- **Increased fee potential - Certified practitioner's fees are up to 30% more than non-certified professionals.**
- **Backing of the world's most respected association of investigative professionals.**
- **Certification indicates mastery/competency as measured against a defensible set of standards, acquired by application or examination.**

APPLICATION PROCESS & REQUIREMENTS

BAI INFORMATIONAL TRIFOLD http://baipi.org/resources/Documents/BAI_Trifold.pdf

APPLICATION

https://www.baipi.org/membership-application

INFORMATIONAL WEBSITE

www.BAIPI.org

Intellenet Scholarship Award

Started in 2017 Intellenet plans to award at least two scholarships annually to a child, step child, grand child or grand step child of an Active Member in good standing of Intellenet.

The scholarships are intended to provide financial assistance to students entering their first year of college, a post graduate year, vocational/trade school or students presently attending a college or university.

A scholarship will be awarded to one child of an active Intellenet member's family.

The recipient or recipients will be chosen by the Scholarship Committee, selected by the Intellenet Executive Director, and their decision will be final.

After 2017 previous Intellenet scholarship award recipients are not eligible.

Only those who plan to be enrolled the ensuing fall semester are eligible.

It is the expectation of Intellenet that the applicant be in good standing with their present academic institution.

CRITERIA

All applicants must meet the following eligibility requirements:

Be child, step child, grand child or grand step child of an Active Member in good standing of Intellenet, and one of the following:

A high school senior who will be continuing their education at an undergraduate college or university, junior college, vocational or technical college.

A high school senior who will be continuing their education in a post graduate year.

A post-secondary student attending an undergraduate college or university, junior college, vocational or technical college.

APPLICATION PROCEDURE

The application is on the next page and can be submitted electronically to the Chairperson of the Scholarship Committee or intellenet@intellenetwork.org. Applications must be submitted no later than March 1st. The scholarship recipients will be announced at the yearly Intellenet Conference gala banquet. Recipients of the scholarship will be required to provide proof of enrollment at an eligible post-secondary institution prior to the funds being dispersed.

Intellenet Scholarship Application

Name: _____

Address: _____

_____

Telephone #: _____

Intellenet member's name: _____

Relationship to Intellenet member: _____

High School and year of graduation: _____

_____

Post-secondary undergraduate institution you (choose one)

Are attending: _____

Will be attending: _____

Will most likely be attend: _____

or _____

Major or anticipated major: _____

Anticipated year of graduation: _____

It is the expectation of Intellenet that the applicant be in good standing with their present academic institution. *** Please submit a 1-2 page essay telling the committee about the activities that you have been involved in as a High School student & College student if applicable. The essay should also tell the committee what your plans after college are, and how you plan to utilize your college degree.