INTELLENET NEWSLETTER

JUNE 2009

Table of Contents **Page**

Carino's Corner

As all private investigators are keenly aware, the economic downturn has seriously impacted negatively on business. Many are reporting a significant drop in revenue. Private sector investigative associations are also experiencing a decrease in membership renewals in 2009, especially state associations as PIs are reducing expenses wherever possible. Whether dropping association memberships is a wise idea or not cannot yet be empirically ascertained and may not be truly measurable even in the future. Certainly, however, membership in fewer associations can and will undoubtedly translate into fewer referrals and less networking opportunities, ergo less business.

The PIs thriving in these economically depressed times are those with a solid clientele base. In discussions with PIs in the US and internationally, a common denominator in the successful businesses (in addition to solid networking referrals) are those who have developed recession and legislative proof niches. However, there is still another variable to consider and one in which Intellenet has placed significant effort – that of developing initiatives for business opportunities which can translate into billable time for the membership.

Not all initiatives, of course, have a pay off but creating an atmosphere which encourages members to seek business opportunities with Intellenet wide application foster a climate conducive to association camaraderie, and personal – professional interaction and friendships. We have already seen an increase in billable time for many of our international members and soon, most of our US members will realize similar increases.

Our known and potentially successful initiatives to date have had two very interesting results – new member applications are up and our renewal losses are at the lowest level in our 26 years of operation. Our initiative selling points are, simply stated, our professional competence, dedication, commitment to "mission", and disciplined approach to problem

resolution. Our high standards for membership – to include a minimum of 10 years investigative experience is a major factor in recent contract awards.

The future of Intellenet is indeed bright!

Know Your Fellow Members

Terry Korpal
Korpal Associates
Baldwin, Missouri

Terrence J. Korpal is a retired Special Agent of the U. S. Secret Service and security consultant to numerous Fortune 500 companies. He has conducted over 200 security surveys in the past 25 years related to the protection of Presidents and Vice-Presidents of the United States as well as the human and economic assets of companies and other entities. He specializes in the assessment and evaluation of security policies, procedures, technology, training, and hardware for premises ranging from stadiums, universities, and theme parks to casinos, supermarkets, banks, hotels, and parking lots. He designed, developed, and co-directed security operations for the 1994 United States Olympic Festival in two states, 6 counties, and at 26 sites including stadiums and other athletic venues, parking lots, administrative offices, training sites and the residential village, directed a staff of 1500+ and was responsible for the security of over 3,000 participants and 250,000 spectators. He has been retained as an expert witness in over fifty lawsuits by both plaintiff and defense involving inadequate security in Missouri, Illinois, Oklahoma, Nevada, Tennessee, and Texas.

Mr. Korpal is the Associate Editor for Research and Review of the Protection of Assets Manual (POA), the security manual published by ASIS International--the largest security and assets protection trade group in the world. He has taught security management and crime prevention courses at the graduate and undergraduate levels at universities and colleges in the St. Louis area from 1989 until 2005. He has an MA in the Administration of Justice from the University of Missouri-St. Louis and a B.A. in Legal Justice and Political Science from Maryville University, and an AA in Law Enforcement from the St. Louis Community College District.

Members in the News

Tom Reilly, New York City, received the Christopher Nolan Investigator of the Year Award for 2008 at the Annual Conference of the World Investigator's Network (WIN) on March 7, 2009 in San Diego.

Paul Jaeb, Minneapolis, Minnesota, **Michele Stuart**, Gilbert, Arizona, and **Jim Whitaker**, Wooster, Ohio, were speakers at the Associations One Investigations and Security Seminar, in Detroit, Michigan.

David Forbes, Perth, Western Australia became a United States citizen on April 8, 2009.

Phil Johnson, Keighley, West Yorkshire, UK, was elected as an international representative of the National League of Licensed Investigators.
Jim Whitaker, Wooster, Ohio, **Michele Stuart**, Gilbert, Arizona, **Ellis Armstead**, Denver, Colorado, and **Paul Jaeb**, Minneapolis, Minnesota,

were presenters at the 2009 Associations One Conference, in Detroit, Michigan, May 13-15, 2009.

Membership Changes

Retirements/Non-renewals: Bob Annenberg, Tucson, Arizona; **Norm Healy**, Prescott, Arizona, **Jack Rossiter,** Blue Bell, Pennsylvania, **Al Schumann**, Hillside, New Jersey, **Jim Silvia**, Phoenix, Arizona. **Victor Budanov,** IRIS, Moscow, Russia, Jack Struble, Orange, California.

Reinstatements: Brian and **Mary Ritucci**, Park City, Utah. **Jim Goss**, Raleigh, NC has been added to the Supplemental Support List.

Death: John Brown, Philadelphia, Pennsylvania

Data Changes: Charles Castro, Whitman, Massachusetts, Telephone--508-659-4436; **John Patterson**; Address--Spring Hill, Florida; **Eileen Law**, Address/telephone—Wilmington, Delaware, 302-475-3584

New Members

Brian Ingram, Consulting Investigation Services, Waxahachie, Texas.

Troy Nuss, Nuss Investigations, Grand Junction, Colorado.

Jim Laws, Jim Laws Investigations, Las Cruces, New Mexico.

Darrell Gindin, Investigative Solutions, Centennial, Colorado.

Life Membership

At the 2009 Board of Directors Meeting, **Bill Parker**, Islamorada, Florida, was granted Life Membership in Intellenet.

Brad Penny Special Recognition Award

The Brad Penny Special Recognition Award was established to honor **Brad Penny** for his services to Intellenet over many years. The award is intended to be bestowed upon individual Intellenet members and any individual professional who has given above and beyond the normal call of the investigative profession, either for professional dedication or humanitarian accomplishments. The first award was presented to **Jerry Adams,** Austin, Texas.

Jerry Adams Recognized for Public Service

On April 23, 2009, **Jerry Adams**, Austin, Texas, was inducted into the Stephen F. Austin High School Hall of Honor for his community activities. Jerry is one of only 60 out of 50,000 graduates to receive this honor. In 1991, he established a non-profit charitable organization to fund scholarships for needy students to help them get into and stay in college. He also participates in numerous community organizations and activities. There is not a more deserving Intellenet member for such an honor.

Acceptable Use Policies

Kevin J. Ripa, EnCE
Computer Evidence Recovery, Inc
Calgary, Alberta, Canada

In today's business world, computers are as ubiquitous as the pencil and paper of yesteryear. Most any type of business cannot function today without the use of computers in one fashion or another. It seems a paradox then that at no other time in history has the commodity of time been stolen and wasted by employees. These computers that were supposed to speed up our tasks and make us so much more efficient are being used as tools with which to waste more time than we could have ever been able to without them.

Imagine finding out that an employee has been wasting as much as 1-2 hours per day using the computer to surf the Internet or chat online with friends. As a supervisor, you let them know that their services are no longer required for obvious reasons. Mere days later, you are served with a Statement of Claim for wrongful dismissal. The claim? Nobody ever told this employee that they couldn't perform such activities. This has been used successfully in the past. This sadly is the unfortunate byproduct of a legal system in a democratic society.

In order to respond to this type of travesty, we meet the challenge with a Corporate Acceptable

Use Policy (AUP). Every company or entity with more than 1 employee (the owner) should have a strong AUP in place, and yet easily less than 40% of businesses have them. Most small businesses would say they aren't big enough to need one, but our example above shows that even 1 or 2 staff members could cause problems such as this.

There should be no question that an AUP is a necessary and integral part of any business's computing environment. Out of the less than 40% of companies that actually have an AUP, only about 10% are properly deployed. Experience, (usually bad), teaches us what works and what doesn't, and we have found in our investigations, that an improperly worded or deployed AUP is every bit as bad as no AUP at all.

A myriad of issues needs to be addressed in any AUP, and we have tried to address the most important ones here. Obviously no two companies are alike, and any AUP will need to be adjusted accordingly.

The single most important consideration for any computer network must be security. Security above all else will dictate the freedom of access that any user will have over their computer. Most small businesses have nothing to govern the access their users have. A user can make changes to the computer, transfer data at will, and use the Internet to go anywhere they want, with no restriction. On the other end of the spectrum, high security installations, such as various branches of government, and R & D for large scale companies have extremely tight restrictions on what employees can do.

An AUP is not just for employees either. It needs to have direction in it regarding contractors that may use your network, either by sitting at your computers, or by connecting their own devices.

Security is a double-edged sword that must be considered. At one end of the scale is convenience, and at the other end is security. The trick is to find the balance at which the two work for a company's applications. As well, it would be unreasonable to apply the same settings and rules to all computers in the network. Obviously the CEO, as well as a development department may need far greater access than a data entry clerk.

Deployment Considerations

Having an AUP is not enough. We have seen cases where a wrongful dismissal case was successfully won because the employee stated that although they had signed an AUP upon being hired 2 years prior, they couldn't possibly remember what it said. You cannot have an employee sign a piece of paper upon hiring, and expect them to remember its contents forever. You must have the AUP deployed in such a way as to ensure the employees always have access to it.

The most efficient way to do this is to have what is called a "click through" notice. In order for employees to log on to computers, they must first click their acknowledgement and agreement with the AUP. There should be a clickable link to the full AUP from this page. This completely eliminates the "I didn't know" argument.

How Much Internet Access and When

There is no question that employees would be perturbed if they were not allowed any access to the Internet. Having said that, if the employee has no need at all to use the Internet for their daily role, then why have it? It is possible in many different ways for an employee to send and receive email with no Internet access.

Arguments that have been brought up in court in the past have been things like how the AUP applies to coffee breaks, lunches, overtime, employees staying late on their own time, etc. While an unpaid lunch hour may very well be the employee's time, the computer and network used to access the Internet still belong to the company. If the employee accidentally infects the network and causes a great deal of damage and downtime, the virus won't care if it was done on paid time or not. Purely from a security perspective, Internet activity needs to be strongly regulated no matter when the computer is in use.

Transferring of Data

Probably one of the most prevalent abuses seen in the corporate world is the theft of proprietary data. Very common also, is the destruction of corporate data by a disgruntled employee. An AUP should outline what access, if any, an employee has to the data storage areas of the network, as well as what the rules are pertaining to removing it from the network. AUPs should address the deletion of files as well.

Connecting Devices

Any AUP needs to address the connection of outside devices to the computer. Are employees allowed to use their USB thumb drives on any computer in the network? How about outside CDs or DVDs? A very common example of corporate espionage today involves loading a number of USB drives with malicious programming that will open a back door into the network. These USB drives are then randomly "dropped" somewhere where employees will find them, such as the coffee shop in the building lobby, or around the elevator on the company floor. Human nature is such that the first thing we want to do is plug it into our computer to see what is on it. Once plugged in, it is too late, and the malicious programming automatically deploys. It is also possible to allow USB devices, but set the computers up so that data transfer is one way. In other words, users can move data FROM the device TO the computer, but not the other way. The vast majority of competitive intelligence is stolen in this manner. Fortunately, we have the investigative and technical ability to not only show what was stolen, but how, and when.

Changing Settings

Your AUP should give direction on what a user is allowed to change or modify on their computer. Most AUPs have a blanket policy that bars users from changing any settings. This is a good policy, but again this is one area that a lot of damage can be done. By accidentally changing a setting (or intentionally), a user can cause thousands upon thousands of dollars of damage to a network. Viruses can be injected into a system through something as innocent as changing a screensaver or the desktop wallpaper. As well, a common monitoring program found in Windows networked computers can easily be shut off by a couple of mouse clicks.

AUP Augmentation

Although an AUP should be an integral part of any network environment, it is not a panacea. It should be backed up with proper network administration. Most every issue I have addressed in this article can be further enforced by proper permissions deployment across the computers in the network. A very brief list of settings that can be controlled include:

- When the Internet can be accessed, if at all
- What websites can be accessed and which ones cannot
- What settings a user can change on their computer
- What programs can be accessed and when
- What devices can be connected to the computer, if any?

Although some of the above may sound draconian, the employer must first ask themselves what they have to lose, if the above is not followed. Without a properly advised and administered AUP the employer might also find themselves on the wrong end of Federal Wiretap Laws. Acceptable Use Policies have not developed simply because somebody had extra time on their hands. Sadly they have been born of necessity.

Kevin J. Ripa is a former member, in various capacities of the Department of National Defence serving in both foreign and domestic postings. He is now providing superior service to various levels of law enforcement and Fortune 500 companies, and has assisted in many sensitive investigations around the world. Mr. Ripa is a respected and sought after individual within the investigative industry for his expertise in Information Technology Investigations, and has been called upon to testify as an expert witness on numerous occasions. He has been involved in numerous complex cyber-forensics investigations. Mr. Ripa can be contacted via email at kevin@computerpi.com.

THE SOLDIER

Michele E.N. Stuart
May 26, 2000

The Soldier laid in his hole very afraid
As he heard the bombs explode up ahead.
He prayed to his God – "Please give me some strength"
As he saw most of his friends were all dead.

His heart and head pounded, bullets exploding around him
Knowing he had fought a good fight.
He looked up ahead to the hills covered in red
Praying "Please don't let this be my last night"

Then somewhere from nowhere – he heard someone yell
"Men it's time to move out"

He found himself running as fast as he could
Thinking this time I'll die – there's no doubt.

Suddenly he felt it – the piercing of hot lead
As he slammed sharply to the ground.
He yelled out "Lord - just let them know I stood up and stood tall
And fought for the freedom of all"

"Don't ever forget, I gave up my life
For our children to grow up in a better land.
Now it's my turn to go home, I will now close my eyes
And pray for the sweet touch of HIS hand."

Suddenly he awoke to the touch of soft hands
Confused and not knowing why.
An Angel there stood - "Your time has not come"
And she was gone in the blink of an eye.

Now he walks with a limp, a cane by his side
As he makes his way through the graves.
As tears fall from his eyes, he raises his head high
For he will never forget these men
That died for this land of the brave.

Saving Taylor

Intellenet Member Jeff Williams thought something was odd about his new friend – a suspicion that would ultimately reunite a mother and her missing daughter.

THEY FOUND TAYLOR! The words that would end three years of tear-filled days were spoken into Julie Coleman's cell phone as she rode home from a church-league softball game in Webster Groves, Missouri. Eight months pregnant, Coleman sat beside her husband, Jeff, while their 2-year old daughter, Lauren, munched French fries in the backseat. Coleman's eyes welled up as she repeated the line she had so longed to hear. "They found Taylor!"

That was in June 2005. Coleman's daughter, Taylor Hill, just a year old at the time, had disappeared in 2002 following a visit with her father, Arlen Dean Hill. During her long absence, the child's room awaited her return, along with presents for each missed birthday and holiday. "Every Easter there was a basket for Taylor and a new outfit," Coleman said.

For Taylor, the road back to her room started with a quick eye of a complete stranger, Intellenet member Jeff Williams, halfway around the world. A 60 year-old Illinois native, Williams had moved to the Philippines 20 years earlier as a U.S. Air Force Special Agent and, after retiring, stayed to start an investigative agency. Ever gregarious, Williams began playing pool regularly with a new friend, Paul Reynolds. The two discovered that they came from nearby towns in southern Illinois, and Reynolds even knew Williams' sister. The long-lost neighbors formed an immediate bond.

But Williams soon grew suspicious of his new friend. Reynolds told Williams that he built golf courses for a living and had a young daughter with a Filipino woman who had abandoned the child. Williams' business partner got a different tale – the girl's mother was a Singaporean. Still others were told she died in a car accident. The veteran investigator's curiosity was piqued.

Williams recalls the moment when Reynolds finally asked him what he did for a living. "He suddenly became less talkative when he learned I was a former federal agent," Williams said.

By October 2004, Reynolds had decided to leave the Philippines. He invited Williams to dinner – and seemed nervous. "He kept looking around like someone was about to arrest him," says Williams. "He made sure to tell me that his daughter's mother had returned to claim her, and he said he was heading to Mexico to work on a golf course."

Williams put it all together in May 2005, while visiting his hometown of DuQuoin, Illinois, near St. Louis. Over coffee with Patty and Lonnie James, his sister and brother-in-law, Williams mentioned that he had met an acquaintance of theirs in Manila: Paul Reynolds. His comment was greeted with blank stares. They had never heard of anyone by that name.

"Was he with a daughter?" Lonnie James wanted to know. When Williams answered yes, Patty James then asked what brought the man to the Philippines. He worked on a golf course Williams replied.

Stunned, Lonnie James realized, "That's the guy from Pinckneyville (Illinois) who stole his daughter!" Arlen Hill, who built golf courses in St. Louis, had disappeared with his daughter, Taylor, three years earlier.

At the Sheriff's office in Perry County, Illinois, Williams looked at an old photograph of Hill with a different hair color. "It took me a nano-second to be 98 percent sure that Paul Reynolds was Arlen Hill." Williams said. So he returned to the Philippines and set his team of investigators loose. Within 72 hours, Williams had both Arlen and Taylor Hill's aliases from immigration records. Williams tracked their travel from the Philippines to Auckland, New Zealand. He immediately passed the crucial information to U.S. federal authorities.

By the end of the week, Hill, 33, was arrested in New Zealand. He then pleaded guilty to charges related to passport and immigration violations and was sentenced to 16 months in prison there, and upon release, flown back to the U.S. by federal authorities where he was sentenced to 6 years imprisonment for kidnapping.

In the meantime, Julie Coleman jumped on the first flight to New Zealand that she could find. Mother and daughter arrived back home on June 27, 2005. That was when Taylor first met her half-sister Lauren and claimed all of her Easter baskets. Five weeks later, Taylor greeted yet another little sister, Grace, and the family was once again whole.

"The family wanted the world to know that they believe with all their heart that the Lord answered their many prayers and that it was nothing short of a miracle that Jeff Williams happened to meet Arlen Hill in the Philippines, thousands of miles from Pinckneyville," Julie Coleman said. "It was no coincidence, it was meant to be."

The tale of the capture reaffirms the notion that it is indeed a small, small world.

Q: Who has the right of way when four cars come to a four-way at the same time?

A: The pickup truck with the gun rack and the bumper sticker that reads: "Guns don't kill, I do"

The day a redneck will clean his house is when Sears comes out with a riding vacuum cleaner.

2009 Intellenet Conference

The 2009 Intellenet Conference was a great success, both from the professional education aspect and the social activities perspective. Many memorable and enjoyable events occurred. Jerry Adams was presented with a hula skirt and forever on will be known as "Hula Muffin." Attendees also had the unique opportunity to visit JPAC - Joint Prisoners of War, Missing in Action Accounting

Command at Hickam Air Force Base where they are currently striving to identify the remains of military personnel from all wars since World War II. The 2010 Conference will be held in New Orleans, Louisiana, on March 24-27.

Thoughts for Business Survival

Bill Blake
Littleton, Colorado

Survival is a basic human instinct. It may be for food, shelter, companionship or any other basic human need. To the more mature generation, it takes on another aspect—that of survival of our income stream. In recent times, we have seen massive employment layoffs, as well as reduction in retirement income, caused by executive theft, mismanagement, or other criminal and unethical behavior. Our governmental entities have done little to regulate or eliminate these problem areas. Only we are responsible for our business survival. The question is how to best accomplish this goal.

"The old order changeth, yielding place to new." This quotation from Alfred Lord Tenneyson's *Idylls of the King,* is a directional key to survival. Over a lifetime, subtle changes are made but seldom at great variance from our primary beliefs and ways of conducting business. The time has arrived when more drastic changes must be made if we are to continue as successful business persons. Continuing to do business in the

same manner as ten years ago may have already reduced us to the dinosaur generation. The time has come to reevaluate our business goals and strategies. The dinosaur still uses the black rotary telephone while the contemporary business person is adept with the iPod and Blackberry. It's surprising how many "professional" investigators do not have e-mail accounts, or not use the Internet.

"Lead, follow, or get out of the way." Thomas Paine had the right idea on how to accomplish success. You can be a leader, one who hangs onto the coattails of a leader or be an impediment to progress, change and success. A leader is one who actively searches for new opportunities and takes maximum advantage of these opportunities and the associated technology. A follower is someone without independent thought who thinks a leader has a great idea and copies, frequently without permission, the activities of the leader. An example of a follower is best exemplified by the number of copycat television series. When a good idea is exposed for the first time, there are numerous individuals copying the original ideas, hoping for success. Those who don't get out of the way of progress and change will be relegated to secondary positions when trying to get new business opportunities.

"He who hesitates is lost—swift and resolute action leads to success; self-doubt is a prelude to disaster." This statement goes back to "Cato" (1713) by English essayist and poet Joseph Addison. Variations of this statement have been quoted by numerous individuals in a multitude of documents over the years. This statement best illustrates the need for constant appraisal of business activities as they relate to the future. Things are constantly changing and failure to act in an expeditious manner leaves the best business opportunities to those who act first. The question is where do you fit into the future of private investigation and security consulting?

Subpoena Information for Major Cellular Companies

Provided by Sandra Stibbard
Camelot Investigations

Subpoenas for T-Mobile records (including what used to be Aerial and VoiceStream) go to:

Custodian of Records
T-Mobile Subpoena Compliance
4 Sylvan Way
Parsippany NJ 07054
(f) 973.292.8697
973.292.8911

Subpoenas for Verizon records go to:

Custodian of Records
Verizon Cellco Partnership, d/b/a Verizon Wireless
Subpoena Compliance
180 Washington Valley Road
Bedminster, NJ 07921
Fax (888) 667-0028
Voice (800) 451-5242

Subpoenas for AT&T records (including what used to be Cingular) go to:

Custodian of Records
AT&T Subpoena Compliance
P.O. Box 24679
West Palm Beach, FL 33416
Fax (888) 938-4715
Voice (800) 635-6840

Subpoenas for Sprint records (including Boost and what used to be Nextel) go to:

Custodian of Records
Sprint Corporate Security
6480 Sprint Parkway
Overland Park, KS 66251
Fax (816) 600-3111
Voice (800) 877-7330

Subpoenas for Cricket records go to:

Custodian of Records
Attention: Subpoena Compliance
Cricket Communications/Leap Wireless
10307 Pacific Center Court
San Diego, California 92121
Fax: (858) 882-9237
or scan and email to:
compliance@cricketcommunications.com
Voice (858) 882-9301

Cybercrime One-Upmanship

Kevin J. Ripa, EnCE
Computer Evidence Recovery, Inc

Calgary, Alberta, Canada

The investigation of cybercrime is not unlike the challenge of investigating wrongdoing that has gone on for centuries. It is largely driven by the bad guys figuring out a way to manipulate or cheat the system, and then the good guys finding a way to respond to it and stop it from happening again.

In the computer world, we are largely dealing with intangibles, making it even harder to chase down the bad guy and bring him/her to justice. Cybercrime investigation is typically an exercise in responding, rather than being proactive.

Since the advent of cybercrime, criminals have found various ways to get away with their nefarious plans. They have continually come up with better and more sophisticated methods in which to hide data or the evidence of their dealings. With more and more complex cybercrimes occurring, the perpetrators have no choice but to keep an electronic record just so they can keep things straight. In the past, they have been using methods like hiding files, putting passwords on files, using stegenography (the science of hiding data in other data), and file encryption to hide it from detection. As a result, cyber sleuths have had to continually respond to these methods by finding ways to detect this activity. Although we are usually engaged in a game of catch up, it is only a matter of time before some brilliant mind comes up with a new and better way to hide things, while another brilliant mind comes up with new and better ways to detect this.

The most recent example of this was a specialized encryption program that would allow the user to essentially create two separate spaces on their hard drive. They could create one section that would contain the operating system and decoy data, so that if they were investigated, nothing bad would be found. They could then use the other space they created to hide all of their illicit data. If the entire hard drive was analyzed by a forensics expert, it would look like unreadable random data that is not unfamiliar to an examiner, and no illegal activity would be found, because of the encryption method used. When the computer is started up, it asks for a password. Each of the two spaces on the hard drive has a different password, and this is how the computer decides which section to go into. When the bad guy was investigated, they would provide a password that would open the "safe" side of the computer, and nothing would be found. Cyber investigators had no way of detecting the other space, let alone knowing what was in it.

That is until now. Forensic Innovations, Inc of Fishers, Indiana has stepped up to the plate and found a way to detect these hidden spaces. Once again, the playing field has been leveled, and it is the bad guys that are having to find a new way to hide.

There is no telling how digital forensics will progress, but history shows us that it will be a "catch up" style of response. But for now, chalk one up for the good guys.

Airtight Employment Investigations

Prevent Claims, LLC
Exton, Pennsylvania

Whether an employment claim gets dismissed by court or ends in hefty damage awards often depends on the quality of the investigation. Thus, you want an airtight investigation to protect your client from liability.

What goes into an airtight investigation? Elements crucial to a solid investigation include whom you choose, how they proceed, what their experience is, when they get underway and complete the investigation and how their findings are presented.

More routine investigations can be conducted ably by Human Resource professionals or in-house counsel. More complex or sensitive investigations are probably better farmed out to outside investigators. Otherwise, the investigation could be perceived as an inside "cover-up," or the investigators could be perceived as biased. The investigator, whether in-house or outside, should be mindful that his or her results will be discoverable. Indeed, the client will want to proffer the investigative results to show that they looked into the matter promptly and thoroughly, and took the appropriate corrective steps if any were warranted.

Your outside investigator might be your usual outside counsel. When and whether to use outside counsel, however, is a tricky call. If you routinely use outside counsel for legal advice and would turn to them in case of an administrative claim or lawsuit, you would do better to use a different

investigator. Otherwise, your outside counsel will become a fact witness about their findings and likely be conflicted out of representing you in a later proceeding. Heaven knows you don't want to give up your pit bull just because he or she dug up a bone in the first instance!

So look beyond your usual outside counsel and find a savvy, experienced investigator to dig up the facts. First, find someone with experience conducting factual investigations – which are different than depositions. Factual investigations focus on open-ended questions such as who, what, when, where, and how. They are not geared towards locking parties into legal corners.

Investigations must be undertaken promptly and completed as quickly as reasonably possible to avoid claims of undue delay. If your investigator has a full plate already, he or she may not be the investigator of choice for that particular inquiry.

Ask your candidate how he or she conducts their investigations as styles are as varied as the investigators who do use them. My preferences are as follows.

I like to use court reporters if the client can afford the expense. This provides me with a verbatim and irreproachable record of what was said. As fast as I can write, my notes could never be as complete. Second, and perhaps more importantly, this provides counsel in any subsequent proceeding with a sworn record. This record has an evidentiary value that exceeds handwritten notes, taped proceedings, or affidavits that the investigator has prepared.

I outline my investigation with special attention to the order of my witnesses. This forces the mind to focus on what facts are essential to the investigation and what credibility disputes must be resolved. There is then a natural order as to how to proceed. One often, but not always, begins with the complainant, but a good investigator will recognize the exceptions to this rule.

I also review all documents and set aside those that I will want to have as exhibits to a witness's testimony. Documents can range from the mundane that I just need help understanding to the "smoking gun" on which a factual finding might turn. I am also careful to segregate a clean copy of all documents from those I will use in interviews. I am equally careful to separate and identify non-identical duplicates as each document can tell a different story about its provenance.

I focus on whether there are outside experts I might need to consult. For example, if emails will be key in ferreting out the truth, I may need a forensic computing expert to help recover 'deleted' email or verify when emails were opened, sent, and received. If a harassment investigation uncovers a parallel abuse of power (often the case), I might consult with a financial fraud expert or someone skilled at following credit card trails.

If I don't have the luxury of having a court reporter, I am scrupulous about dating my notes. If I have multiple witnesses in one day, I will put the time of the interviews as well since the order in which I interview witnesses could later be important for follow up interviews and I may have forgotten the order of my witnesses. Claims may also trigger retaliation charges, and times and dates can be crucial to assessing whether retaliation occurred.

Investigative reports can range from 10 pages to a hundred pages depending on the scope of the inquiry. As a preliminary matter, I list all witnesses interviewed. If there are potential witnesses that have not been interviewed, I name them and state why.

My investigative reports are detailed and refer to all relevant exhibits in the body of the report. They also make conclusions as to the credibility of various witnesses as these conclusions are key to the ultimate investigative findings. Credibility disputes must be resolved if an investigative report is to have weight.

My investigative reports are numbered, for example 1 out of 3 copies, and only that many are printed. I limit the number of copies of reports coming out of my office to provide copies only to those with a need to know my results.

I also print a disclaimer on the front of the report stating that only three copies, for example, are being provided and that I disclaim responsibility for the distribution of any copies beyond those provided. I do this to underscore the confidential nature of the reports and to protect myself from any claims of defamation or undue dissemination.

Finally, I do not provide electronic copies of my reports to clients. Electronic documents are too

easily disseminated either by accident or by design. Instead, my limited number of hard copy reports go out by overnight courier, so it is always clear just how many copies have come out of my office. If clients want electronic copies, they may scan them and distribute them more liberally.

These few tips should help you insure that any employment investigations you undertake are airtight and fully defensible in any subsequent proceedings. More importantly, your investigations should get you where you want to go: to a decision as to what did, or did not, occur.

Ms. May is an attorney and experienced investigator with special expertise in sexual harassment issues and with special strength in investigating, preventing, and resolving claims.