Cyber Investigations?!? We Don't Need No Stinkin' Cyber Investigations!

A Chilling True Story on What Could Have Been Without the Aid of a Revealing Cyber Investigation

BY **CHRISTOPHER SALGADO, CEO OF ALL POINTS INVESTIGATIONS, LLC**

RING RING. "Hello?" You're happy to hear a familiar voice on the other end of the call. It's one of your loyal – and favorite – clients. You and he engage in overplayed chitchat: the weather, what you've both been up to since the last conversation, how business is for both of you, who rocks it better on Call of Duty, etc. Then, your client asks you to engage in a fairly simple case. The details are to reach out to a subject tomorrow who may be engaging in illicit activities that infringe upon your client's rights. (Details beyond this are irrelevant for the purpose of this story.)

You accept the case and inquire as to what information is known on the subject. Your curiosity is rewarded with the response that the intel-gathering element was outsourced to a "friend of the company." The information obtained was enough to go forward with the matter, which is to have you engage the subject directly. Nervously, you ask what information unfurled via the other person's "investigation." You're told that the subject is an adult female and a struggling yoga business owner. She is believed to reside in a mediocre single-family house, located not too far from your office. Her illicit activity is not expected to be significant but, nonetheless, it's concerning enough to warrant subsequent efforts. The specific request by your client is to engage the female subject and inquire as to the depth of her illicit operation. Your client relays to you that no business location for the subject's yoga business was identified and, as such, you are to engage the subject at her residence. Not much more is revealed to you on the subject, her network, properties, or her illicit activities. Something seems amiss here. At a minimum, it may be the faint results from the seemingly short-lived online "investigation." (Yes, the quotes do depict a slight annoyance and mockery of the perceived – I'll do it again – "investigation.")

While the above information provided to you is semi-revealing on the surface, you're still not sold that everything which needs to be known about the subject is currently known. You press one final time for more information on the subject. Your client assures you that all that is known is all that there is to be known on this situation. He adds "You'll have the results of our 'cyber investigation' in your email later today." Begrudgingly, you accept this response and await the email to really begin analyzing the results of the cyber investigation. (Yes, I gave my quotes a

non-alcoholic beverage break that time. Non-alcoholic because I predict I'll need them again later.)

You thank your client for the call and for considering you on this case. You end the call and walk back to your comfy couch to return to your invention of designing a "new and improved" abacus. (I don't know. I'm reaching here for your hobbies.)

A couple of hours pass before you're alerted to a new email. It's the email delivering the case details that you've been awaiting. You open the email and vigorously read those juicy findings of their cyber investigation. Wait… where are the juicy findings? There's some information here but much of it is incomplete before it branches out into two-dimensional conjecture. You tell yourself that there's got to be more. After another unsuccessful search for logical connections from one element to another, you throw in the towel and call your client.

Your call is answered with a response from your client stating that he's surprised to hear from you so soon. You pay him in kind with your very own surprise on the lack of depth within the "cyber investigation." (Hey, I warned you about The Return of the Quotes.) You validate your previous thought that much more information is needed on the subject before you show up at her doorstep. Alas, your client now levels with you. He states that he validates your concern of nearly walking into the situation blindly due to a lack of sufficient information on the female subject. You request to install your very own cyber investigation into the agenda so that you can feel confident of what you're walking into on this case. The client agrees with you and is well aware of your cyber investigative skillset. However, there's a catch… Another person with your client is insistent that the friend of the company's did an excellent job on his investigation and, as such, no additional cyber efforts are needed.

This just doesn't sit right with you. After you end this call with your client, you voluntarily engage in what you perceive as a true cyber investigation. Almost immediately, you unleash valuable information that wasn't known – or, at least, delivered to you – inside the case details. One highly concerning detail is that the subject lives with her boyfriend who is an adult male with an extensive criminal history of incredibly serious charges, including drug trafficking, human smuggling, assault with a deadly weapon (multiple times), aggravated assault upon a law enforcement officer and other serious offenses. He has repeatedly served time in prison for these and other crimes. Loaded with this information, you realize that, although the female subject does not have a criminal history, it could be highly dangerous to engage her at her home, should her boyfriend be present. You also identify that she no longer owns the yoga business – and hasn't for years. She's a fitness coach at a local gym.

Expounding on your very revealing updates, you investigate your client's allegations of the female subject being embedded in the illicit activities. Interestingly, you cannot duplicate the same findings that your client's friend did. You eagerly try to mirror the nexus points leading any illicit activity to the female subject that your client identified. Alas, you fail. You cannot connect the dots here. Another call is due.

You call your client yet again and explain your findings and, just as importantly, your lack of findings. Slightly embarrassed – in the event that you've lost your cyber touch and cannot duplicate some otherwise simple findings – you relay these significant updates to your client. You receive the unsettling tone in his response, but he does agree to retreat to the company friend for more information. He also appears to be relieved that you discovered the boyfriend's criminal background. Your client agrees that it would be too dangerous to engage the female subject at her home, in the event her boyfriend is present. He appreciates the due diligence and places you on ice for the rest of the evening. He explains that he will update you tomorrow morning, but the case must still be worked tomorrow. The sound of the school bell appears to have been rung, which is great because it's late and it's time to catch that bus to The Land of Zs.

Fast forward to your unforgiving morning that greets you with a terribly early call from your client. A thorough conversation informs you that much of the information acquired by the company friend was through confidential sources who state that the female subject is good at hiding her true nature and activities. While this softens the blow a bit on the breathtaking updates that you uncovered, it still feels… weird. Your client requests you to simply engage the female subject today in a conversation about these allegations and nothing more. Your comfort on this case now rests on the fact that you can confirm if she is the true concerning operator or not via a simple conversation. This differs from the original intent on engaging a "confirmed" bad operator. You accept the modified request to query her to understand what's going on here.

After some travel, you land at the female subject's gym. You confirmed her day's work schedule and location among the dozens of gyms in the region. And no, she wasn't working at the closest one to her residence.

You spot her vehicle, sit on it and wait for her departure from the gym. Armed with a very recent photograph of her – not provided by your client but uncovered via your cyber investigation – you approach her in the parking lot when she surfaces from indoors. You identify yourself and the reason for your visit. She listens patiently but then delivers the blow. "This is not me," she says. She explains that she has no tie into the illicit activity in any way. She confirms that she does live with her boyfriend who has "experienced run-ins with the police" – to put it lightly. Nonetheless, she is adamant on not being the proper person behind the illicit activity that your client alleges. A calm conversation concludes and you depart the area.

You call your client and relay the update. He is no longer surprised. He sounds defeated and apologizes to you for the hassle. He even admits that the information obtained at the onset by the company's friend's "investigation" appeared weak, at best. It now even appears to have been flat out wrong in some areas. You offer to run a full cyber investigation on the true culprit and situation starting from scratch. He happily accepts but requests a recess in this case to regroup with the persons involved in the hollow cyber investigation. You thank him and depart the area, initiating your return travel to your office.

Let's review the significant takeaways here, folks. The case that was assigned to you by your client was littered with faulty elements "from the word go," including missing information and incorrect information. Most significantly, the missing information of the boyfriend's dangerous criminal background could have inflamed any engagement of the female subject, should he have been home at the time of your visit. Surely, given the prior charges applied to the boyfriend, by avoiding a confrontation at the female subject's home, you may have even avoided a life-threatening event. Your thorough cyber investigation netted in the subject's current employer; a recent photo of her, which helped in visually identifying her when she departed the gym; her vehicle (no, it wasn't contained in the results of a background database); and the large possibility that the bad actor was not her in the first place due to a lack of connections between the illicit activity and her.

Although your client knows you and respects your effective cyber investigations, there appeared to be an aversion to allow a thorough cyber investigation to be conducted at the onset of the case. Now your client is kicking himself at the wasted efforts due to his company not wanting to second-guess the initial efforts of a friend. If you ask me, second guessing a friend's results surely takes a step back from a dead private investigator because a conversation was blindly initiated inside a dangerous situation. Especially when this information was available but not properly identified.

"Cyber investigations?!?," you scoff. Do you really think that a cyber investigation cannot benefit you in any way? Although the above may be an extreme case, it may not be a woven effect for the sake of an article in an industry-leading magazine. A life may have been saved and considering that it all resulted from a proper cyber investigation, it's highly imperative that we all ensure the installation of our absolute due diligence on every case, especially given those results can possibly negate a dangerous outcome. Cyber investigations?!? We don't need no stinkin' cyber investigations! – I think you do, and I think you'll be thankful at their results. The life you save may be your own. **PI**

Christopher Salgado is a former investigator at Facebook and is CEO of All Points Investigations, LLC, a global cyber and physical investigative firm serving Fortune-listed corporations, including a Fortune 20 corporation, law firms and other entities through various investigations. He is an expert social engineer and has been a trusted security and investigations leader for 20 years in corporate risk, brand protection, threat management, supply chain, surveillance, SIU investigations and more. He is also a member of the London Speaker Bureau. Christopher has presented on cyber and physical investigations to various companies, law firms and law enforcement, including the FBI, Homeland Security Investigations, ICE, Customs and Border Patrol and the DEA as well as members of Interpol, Europol and the European Commission. Christopher was a keynote speaker at CrimeCon 2022 where he spoke on romance scams. He is Founder of AGGOSO™ Training, a comprehensive OSINT training program for investigators, corporations, law firms, journalists and those desiring to upskill their OSINT/cyber investigative skillset. Any questions or comments? Contact him at csalgado@allpointsinv.com. Thank you for reading!