Skilled Adversaries Closing in on Your Client and His Cash?
Try a Privatized Protection Program

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

SITUATION OVERVIEW

("You" references Mr. Jones, your incoming client)

Congratulations, you're solid! You're a mensch! You're revered in your industry and with good reason. You engage in projects within your scope and educate others on how to successfully do the same in your field. Money's in the bank and you're feeling good. It's at this point, things... begin to change – and not for the better.

Unusual calls start to arrive at convenient times. However, the convenience is not yours but that of the numerous callers. Catching you slightly off guard while you're entrenched in business as usual, you find yourself responding to several abnormal requests from "new clients." Optimistic for more business, you find yourself providing a little too much information on these calls. Yet, you dismiss your concerns, as these requests for more information appear to be reasonable – at least, on the surface.

Fast forward to today and you're checking out of the hospital after being run off the road a few evenings ago. After the crash, you suffered a hit to the back of your head from an apparent separate attack. Unknown to you, this attack stems from a far more devious agenda.

During your attempt to check out of the hospital, you review your phone and notice several notifications from your bank. They alert you to a significant amount of funds that were removed from your account. You confirm that the recipient of these online transactions is unfamiliar to you; additionally, these transactions took place while you were still unconscious in the hospital.

Upon arrival at your residence, you call your bank and the local police to file appropriate reports. Unfortunately, the evidence shows that the account was successfully logged into without any evidence of incorrect password usage or brute force hacking. The immediate assumption from your bank is that there was no apparent theft of these funds. Nonetheless, they assure you they'll investigate and get back to you with an update ASAP. This triggers your memory and you recall several other unusual transactions in the recent past. While you previously dismissed them as legitimate – but forgotten – transactions, you now see that they may have been tests to confirm any scrutiny of your financials. These additional suspicious transactions make it into your reports as well.

Given the amount of money that has recently been removed from your account in the last several days ($250K USD), you terminate your account and move the funds to a new one. While you consider changing your passwords to several other seemingly unaffected financial accounts, the horror of the inconvenience that comes with changing accounts prevents you from doing so. After all, they weren't impacted... yet.

Your next call is to your trusted friend and attorney. You update him with your recent hospital visit and large loss of funds. In that conversation, you develop a new assessment from a macro view of these seemingly disconnected events. You now believe that the stolen money, the physical attack and the suspicious phone calls are all connected. In considering who may behind these horrific attacks, you draw a blank.

Your attorney logs the incidents and your reports with law enforcement and your bank. He then strongly recommends that you take care of the situation immediately before your accounts become depleted or, more importantly, before you end up in the hospital again, or worse. He provides you with the name and contact information of a trusted private investigator who specializes in cyber investigations, cyber surveillance and cyber counter-surveillance. You thank your friend, hang up and call the PI.

ENGAGEMENT

("You" references you, the reader)

It's 7:45 PM. Your phone rings. You're in the middle of eating your favorite meal with your favorite people: your family. Your rule of not tending to phone calls during dinner is paused due to your gut telling you to answer the phone. Annoyed, your family gives you the forced approval to do so. It's Mr. Jones calling. After you answer the call, Mr. Jones immediately begins blurting out his concerning situation at nearly 100 miles per hour. He's obviously very upset and he appears to be on the verge of tears. You excuse yourself from your family and walk into your office. Mr. Jones continues to relay his episodes to you. Additional details display that these instances have been occurring for many months. Mr. Jones has had many parties with new clients at his personal residence as well as his office. Many of these parties included alcohol and illicit substances. One day after a party, an adult male named Paul visited Mr. Jones' residence stating that he was a friend of Mr. Jones' new client. Paul claimed that the new client directed him to show up at Mr. Jones' residence to ask for money. Paul told Mr. Jones that the new client said Mr. Jones would give him money for a "situation." This was highly unusual and Mr. Jones confirmed that he did not know Paul, nor did Mr. Jones ever see him before.

In trying to piece together what's been going on in his life recently, Mr. Jones discovered that he lost access to several of his social media accounts. He also discovered that he has lost another $225K USD in smaller increments. Mr. Jones also admitted that while he is good at bringing in revenue, he's not good at managing it – or keeping an eye on it.

Reflecting further on the last few weeks, Mr. Jones updates you that only days later after several suspicious calls came in, his devices started to "act up." During that time, he noticed several unauthorized transfers from his business' financial accounts. Additionally, some of his online accounts suffered from ATOs (account takeovers). Essentially, the passwords to those accounts were changed as well as the password reset email addresses.

Mr. Jones lastly reports to you that, recently, he began to be concerned about a vehicle that appeared to be in multiple locations that he found himself in. This vehicle even showed up to a very discreet meeting with an old and trusted client. As such, he began to think his phone conversations were being monitored.

You ask Mr. Jones if he believes that his safety is in danger. He informs you that he doesn't think so, at the moment, but he wants to ensure that this remains so. Yet, to satisfy your own concern for his safety, you ask him to stay at a hotel, with a family member or a trusted friend for the next little bit. He states that he has no one to turn to locally and he doesn't want to leave the state. You urge him to check into a hotel in a neighboring town and call the police if anything suspicious arises or if he feels like his safety is at risk. You also request him to pay for the hotel in cash, check into the hotel under a different name and be mindful of any vehicles following him. He provides you with the hotel information and the name he will check in with. You also tell him to place his phone on airplane mode and wrap it in aluminum foil immediately after he ends his call with you. He agrees and asks about your experience with these types of situations. You inform Mr. Jones

that you've assisted many persons involved in similar situations. He immediately demands that you assist him. You agree to do so.

After a pause to allow your new client a good night's rest – urged by him – you engage on this volatile matter. He calls you when he wakes and you commence collecting the background on his situation. He recycles the information provided to you last night, allowing you to believe he may not be inventing this horrible situation.

You tell him that you're willing to assist but you also inform Mr. Jones that if you are to help him, he must abide by your requests and recommendations, as they will only come from the interest of keeping him safe. He agrees.

You provide Mr. Jones with a to-do list to tackle immediately. You've performed this type of aid so many times that the response seems habitual for you. The to-do list is exhausting but effective. The action items include for Mr. Jones to:

1. Immediately sever himself from all of his smart devices (computers, phones, tablets, smart watches, etc.)
2. Disengage from all of his active and accessible email accounts, social media accounts and any other current or previous online accounts
3. Avoid informing anyone of his current location or situation
4. Avoid using current credit cards and financial accounts

Just like many of your other clients entangled in similar situations, Mr. Jones scoffs at the length of care he needs to immediately adopt. You can almost time his response like clockwork, based on your experience with others. Nonetheless, you explain that this is necessary until you can properly assess the true risk to his lifestyle and life itself. Your simple but hard-hitting statement reminds Mr. Jones of the reality of his own situation. He pans around the four walls of his sanitized, white hotel room and realizes the grimness of the situation that he originally called you on. He accepts your recommendations.

Thankfully, Mr. Jones is located in your own state. You take down his current location and assure him you'll be over to continue this engagement in person shortly. You tell him to stay in the hotel and not to call anyone but you via the hotel phone, if needed. You remind him again to call the police, should he find himself in any immediate danger.

You arrive at Mr. Jones' hotel room. His appearance mirrors his situation but his physical appearance also possesses evidence of a successful man. You introduce yourself in person and immediately provide Mr. Jones with an active and clean burner phone. You also hand him a clean burner laptop. You've prepped both devices with adequate antivirus software, camera covers and microphone blockers. The latter two prevent others from peering into the camera or listening in via the microphone without your client's knowledge. You also enrolled your contact information into the burner phone. To be safe, your information is coded. You inform Mr. Jones that these are his sole devices for communication until the completion of your assistance. You tell him to not use public Wi-Fi and to only use the internet supplied by the burner phone as a hot spot.

You request an update from Mr. Jones' engagement with law enforcement, explaining that they are the best responders to the danger element within his situation. He states that he has not received any update yet. You and he discuss your admiration for law enforcement but he stresses his need for immediate help.

The next thing you do is collect all of his devices: a cell phone, tablet and laptop. You place each in a Faraday bag, which terminates any signal from entering or exiting the devices. This helps to negate any tracking of the devices. Your intent is to run digital forensics on each of the devices to possibly capture any evidence of tampering or infiltration of the devices. You inform Mr. Jones to not contact anyone without your approval first, as you want to ensure that he doesn't inadvertently unravel the security tapestry that you're weaving for him.

You request Mr. Jones' intentions with how far he wishes to go with your assistance and his envisioned "end game." He informs you that he wishes to relocate temporarily at his beach home. He wants to have his admin handle his business while he assesses this danger and overcomes it. You deliver the bad news that he won't be able to stay at his beach home due to the possibility that the bad actors may be aware of that location. You and he agree on a location for temporary living during this engagement.

You travel with your client to the secure location and ensure he's safe. Before you leave, you task Mr. Jones with contacting his financial institutions to ensure the cancellation of his accounts. You also request that he contact other relevant accounts to change their passwords and add two factor authentication (2FA) via the new clean phone. You quickly set up a new, encrypted email address for him to assist in this task. You explain that this new email address is the only email address that he should use with you, anyone else that he must contact during this time, and 2FA set-up. You stress that he should only reach out to those that you approve of during this time. Additionally, you inform Mr. Jones that

only the necessary accounts need to be engaged at this point.

You depart the secure location and contact your team to assist in several tasks. You request they pause on other cases to focus on this one for the time being. Your team's action items are:

1. Initiating digital forensics on Mr. Jones' three devices
2. Engaging in aggressive cyber investigations on some of Mr. Jones' newer clients that appear to be reasonable suspects, per Mr. Jones' feedback
3. Conducting a macro view on the exposure level of Mr. Jones to expose his online privacy weaknesses and immediately begin taking down concerns (essentially, acting as his cyber stalker to assess his online overexposure that serves as a danger)
4. Engaging some of your client's non-essential accounts for password changes and 2FA

Fast forwarding to the results of your efforts: You discover that three of Mr. Jones' recent clients fit the bill as suspects. Evidence confirms their prior illicit operations against other high-net-worth individuals. Additionally, you and your team have exposed their criminal records, showcasing prison records for fraud, deadly assault, attempted murder, drug possession and distribution as well as other serious crimes. Among the bad actors involved inside this highly organized operation is a male currently sitting in a maximum prison. It appears that this is the group's ringleader and he's calling the shots from behind bars. The number of bad actors involved in this scheme comes to thirty! Your digital forensics efforts confirm anomalous usage of your client's devices and a trojan horse present on his phone. Attribution efforts to both your software and hardware investigations remain ongoing but you've unlocked several promising leads.

Weeks have passed since the initial evening when Mr. Jones entered your life. You and he reconvene to discuss these results (you've kept him up-to-date during the entire investigation). You inform him that you've updated law enforcement and enrolled some additional law enforcement resources for assistance. You let him know that they've made progress in engaging the most concerning actors. Given this update, you and your client feel that he can return to his beach home – not quite his main residence yet – to allow for a return to some normalcy. You also inform him that his internet network has been overhauled and is now clean. You've also provided him with new, clean devices: a new phone and a new laptop. (Separate from the current burner phone and burner laptop.)

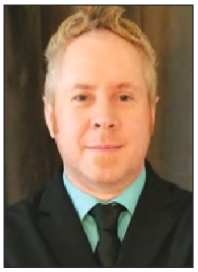
You tell Mr. Jones that his online exposure has been greatly reduced and his new email addresses and phone numbers remain unknown in the cyber world. You educate Mr. Jones on effectively navigating the internet and managing his privacy – both in the cyber world and the physical world. He relays his appreciation for your hard efforts and success. You tell him that the best "thank you" is for him to continue his own security success and avoid contacting you for a repeat service.

An important thought here is that this type of case typically encompasses much more than the above action items and considerations. As a matter of time, I've simply included only a few items that must be considered when you engage in this type of service. The obvious caveat here is extreme diligence must be taken in these cases, as any oversight or improper management of any of the required tasks can result in a terrible result for your client.

Note that this privatized version of a protection program certainly has its limits, being that private investigators are private citizens. Therefore, our capabilities are much more limited in comparison to law enforcement's capabilities. For instance, we cannot create new legal names; create new passports; create new government IDs; offer a travel stipend; offer a salary; pay for training and many more options embedded within the official protection program offered by the US Marshals. Certainly, some of the above financial assistance can be offered by PI's, however, this is not likely the case.

Comparing the private version of the protection program with the official law enforcement program, there's no doubt that the law enforcement program outweighs the private version. However, sometimes people fall short of earning the tremendous protection from the official protection program, yet, they don't reach the threshold for immediate law enforcement assistance. This is when a private protection program can offer great value for such persons. Please note that this article and perspective does not dismiss any portion of law enforcement's great assistance in protecting people. It simply highlights an option for those who fit the mold described above. Again, for those that do, it is dire for the PI to be severely diligent in his/her efforts to avoid an unfortunate outcome. Note that protection efforts should be tailored to the situation and can be peeled back a bit or include additional support from those listed above, per the situation at hand.

While the above example and the need for a private protection program may appear outrageous and unnecessary to some, unfortunately, many victims inside similar scenarios would disagree. Hence, it can be a realistic opportunity for you to service your clients in an incredibly urgent and significant manner. Remember, internet trolls and devious hackers can cross the bridge from the cyber world to the physical world. Once they do, the danger to your client – or yourself – is severely escalated. It only takes one successful aggravated attack to invert someone's world. That is, if they're lucky enough to avoid experiencing the worst outcome of having no world. Consider all the options and stay safe, folks. **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, U.S. Customs and Border Protection 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!