"I Love You. Now Loan Me $100K or I'll Die" — The World of Romance Scams

BY **CHRISTOPHER SALGADO, CO-FOUNDER OF ALL POINTS INVESTIGATIONS, LLC**

The FBI has just called you directly on your unpublished cell phone number. They confirm much of your personal information, including your full name, address, date of birth, and family status. They inform you that your actions – online and offline – have been monitored for several days. After dropping this knowledge on you, they demand that you send them $3K USD immediately or they will prosecute you for various crimes, including money laundering, human trafficking and theft. The self-disclosed agent on the phone is not friendly, and insists that if you do not complete the transaction immediately, a team of federal agents will swarm your house and arrest you, seize your property and send your kids to the state child welfare agency. Another demand made to you is that you initiate this money transfer via multiple gift cards. He warns you to keep him on the phone while you do this so that he can hear this occurring. In fact, if you hang up, he will deploy the agents immediately!

Given the extreme urgency of the demands from the "agent" and the fact that he knows your personal information, you probably should do what he says or risk getting arrested… Or should you?

Shortly before the above experience, you were engaged with a rapid-moving love interest who professed his (or her) love for you after only "knowing" you for six months. How did you meet this incredibly endearing person? The usual avenues: Facebook, Instagram, online dating sites A through Z, etc. So, what does this recent quintessential loving relationship of yours have to do with the above angry experience with a supposed law enforcement member? Simply put, it's called a romance scam. Romance and scam… Two words that – prior to modern times – could have resided in two separate dictionaries as complete antitheses to one another. Thanks to the guise of the internet, people are claiming to be those whom they are not. While identity shams are not new to us, the current number of victims of romance scams, the rising trend of romance scams and the cost of some of these individual scams are incredibly alarming.

According to the Federal Trade Commission (FTC), reported online romance scams reached $304M USD of losses in 2020[1]. (Some reports claim even larger numbers.) The FTC calculates this number to be an increase of approximately 50% from 2019. While the FTC reports an average of $2.5K USD per incident, I know of one specific romance scam that cost its victim hundreds of thousands of dollars. Romance scams have kicked it up by such a high notch recently that last Valentine's Day, the FBI initiated a public service announcement educating the public to what a romance scam is and how to avoid falling victim to one. Unfortunately, as with all other online scams, romance scams have experienced a significant uptick thanks to the more secluded environment that Covid has built for us. A friend of mine wisely commented on this new opportunity for romance scams by saying "…the isolation of COVID enhanced the opportunity of the addiction." Very well put.

The FBI defines a romance scam as "…when a criminal adopts a fake online identity to gain a victim's affection and trust. The scammer then uses the illusion of a romantic or close relationship to manipulate and/or steal from the victim."[2] Some of the popular scams reported include the scammer claiming to: (1) work on an oil rig, (2) be an active military member, (3) work for an international organization or (4) be a doctor.

At the onset, these scammers appear very empathetic towards widows, divorcees, and any other persons dealing with any stress that life deals our way, including the death of our furry loved ones. Once these scammers gain your trust – as far as a short-lived online relationship can receive trust – they begin to move in for the "financial kill." They begin asking for money to sustain their internet usage so that they can continue the novel loving relationship with their victims. Reportedly, they can also ask for money to (1) keep bill collectors away due to hard times at work, (2) pay for work-related mechanical equipment, (3) pay their employees' salaries due to accounting issues, (4) pay for passport renewals or (5) pay for travel arrangements to reign in this long-distance and finally marry their victims! The list goes on and on… and, unfortunately, on.

These scammers will likely request the money to be sent via gift cards or wire transfers. In fact, this occurs so often that, depending on the amount attempting to be purchased or wired, some banks and retailers ask you why you need to conduct such transactions. If the storyline doesn't jive with the inquisitor, they may refuse to allow the transaction to go through. Hooray! A victory in that setting. Nonetheless, given the intense emotion possessed by the victim, he or she will probably just turn to another source, including covertly sending cash to their digital sweetheart in the mail!

At this point, I can almost hear some of my readers thinking, "Yeah but that's not going to happen to me or anyone I know." Many people with the luxury of holding an outside perspective on a romance scam believe that these scams only work on the unintelligent or the easily swayed. While these scams may very well be more effective on persons experiencing raw emotions, such as widows, divorcees, etc., these scams have also been successful on very intelligent and more mentally stable persons. Unfortunately, due to romance scams being so lucrative to their perpetrators, large underground ecosystems have been created in order to enhance these great losses. This even includes the adoption of money mules across the US and, perhaps, across the globe. Money mules have been identified as knowing or unknowing persons who play a role in this money relay system. They receive payments from victims of romance scams and forward the money to the scammer at another address -- sort of a freight forwarder business but dealing in money. Just another layer of obfuscation inside this great system of deceit. As such, the intricacies and lies, frankly, inside these operations have become much more effective than the ten-year-old email from the supposed Nigerian prince that almost all of us have received at one time. I'm referencing the email where the self-declared prince requested you to just cover taxes and fees for a payment transfer of a large sum of money. The reward for your altruistic action is to keep the remaining amount. While this outdated scam is laughable these days, I believe that every one of us is capable of being socially engineered, given the right approach. (Check out my article on social engineering in the May/June issue of PI Magazine.)

My firm was involved in investigating one of these romance scams. Being a former Facebook investigator, a lot of people and companies turn to me for in-depth cyber investigations. This request was no different. As we engaged on the scammer, we discovered that not only was the scammer not who he claimed to be, but the scammer had a plethora of online personas that were likely being used to scam others. We used facial recognition software, incredible surface and deep web dives as well as other methods and tools to confirm this. The scammer was a metaphoric rash across the internet. He claimed to be a US senator, a doctor, a military member and an oil rig worker. I'm sure if we continued searching, we would have found him dressed up as a partridge in a pear tree on a random site. [Insert your favorite ROFLOL emoji here.]

During our investigation, we also unveiled several fake passports of his. When we presented our findings to our client, the client approached the scammer. It was reported that the scammer attempted to "one-up" us by claiming that his twin brother is the culprit in all of this, but not him. I call this "salt in the wound." Thankfully, the client did not buy into this latest façade.

My point with this case study is that these romance scammers will go to great distances to "disprove" any finding that debunks their claimed identity or context. At some point, you have to take a step back and assess the reality of what's in front of you. However, I recognize that such a stance is certainly easier said than done when you're emotionally committed. Nonetheless, these romance scams are real, and they can hurt in more ways than the obvious financial element. They also carry the opportunity to cripple their victims both emotionally and spiritually. Darker effects of romance scams that have been reported include attempted suicides and family murders by jealous partners.

So how do you prevent yourself from falling victim to a romance scam? The FBI, the Federal Trade Commission (FTC) and the Better Business Bureau (BBB) recommend that you be weary of any person asking you to send them money. Specifically, if they ask you to send money via a wire transfer or gift cards – or certainly cash in the mail! I'll take it a step further and say that if anyone almost immediately tries to pressure you into pivoting your communication onto a more secure platform, such as WhatsApp, Telegram, Wire, etc., be very cautious. The motive here is the scammer knows that communication is more difficult to obtain by investigators on such platforms. A great and simple way to identify if a future Mr. or Mrs. is real or not is to conduct a simple reverse image search on Google. There's a good chance that if the online persona is involved in a scam, the photo will have been reported as such. Nonetheless, be mindful that you can be the first victim with the new profile photo.

Another checkpoint to confirm if your pending online romance is a scam or not is to request the person to take a photo of themselves holding a sign with your name and the current date handwritten on it. Given that many of the photos used by these scammers are not real – real as in true photos of them – tailoring such a photo would be pretty difficult to do. This should work even if your scammer has declined your request for a video conversation. FYI, many of these ill-intended folks claim that a bad storm or power outage precludes them from having a video call with you. Or, if one is initiated, it will be interrupted very quickly due to the same. This is in order to not expose the fact that they are not the person in the photos.

I'll lastly say that if you possess any inkling that you may be a victim of a romance scam, it is incredibly important to relay your story to a trusted person to assess the situation with you. A simple query to a trusted confidant without any vested emotion in your story can help shed a light on the situation. Who knows, such a wise choice may even save you from a very dark path once you become aware of the running scam.

If someone you know is suspected of being a victim of a romance scam, please reach out to them sooner than later. Emotional support from a trusted circle can work wonders on these situations. Keep in mind that the scammers don't want their victims telling anyone of their requests, as people not involved with the situation can easily see through these façades. Should you be involved in a romance scam, reach out to friends and/or family for the same support.

Concluding the beginning story with the supposed FBI agent, you may have guessed by now that this call was not made by a legitimate FBI agent. While many money requests in romance scams are initiated by the cyber sweetheart, the aforementioned phone call made by the "FBI" has also been known to occur. Yet, this is simply another method to obtain money from the victim. Additionally, it is likely initiated by the same illicit operation. Hence, how the personal information of the victim is known by the caller. This tactic is deployed to scare the victim into abiding by the money transfer requests. Yet again, it is a scam. I would invite you to Google the phone number that the call comes from. I've also heard of these strongarm threats for money being made by the "FBI" via Gmail accounts. Of course, you can also Google these email addresses, however, an immediate tipoff should be that the supposed FBI agent is conducting "official business" via a Gmail account.

Unfortunately, many of these offenders are not seated in the US, which makes it difficult to engage criminal charges. Nonetheless, there are several resources for you, should you experience a romance scam. You can report these instances to the site that the scammer engaged you on as well as the following sites: FTC = ReportFraud.FTC.gov; FBI Internet Crime Complaint Center (IC3) = Bit.ly/2Ue445W and the BBB Scam Tracker = BBB.org/ScamTracker.

The internet is a great resource for many of us – both personally and professionally. While we continue turning to the online world in order to expand our experiences with others, remember that those online profiles aren't even skin deep. It's up to us to police ourselves accordingly before our emotions persuade us otherwise.**PI**

REFERENCES:

[1] "What You Need To Know About Romance Scams", Federal Trade Commission (https://bit.ly/3eiCCL6, May 20, 2021)

[2] "Romance Scams", FBI (bit.ly/2TfEa1e, Feb 10, 2021)

Christopher Salgado is a former managing investigator with Facebook and is Co-Founder and CEO of All Points Investigations, LLC, a global cyber and physical investigative firm serving corporations, including Fortune 100 companies; law firms and other entities in various types of investigations. He is an expert social engineer and has been a trusted security and investigations leader for 19 years in corporate risk, brand protection, supply chain, surveillance and SIU investigations. 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 members of Interpol, Europol and the European Commission. Christopher Salgado is also the Founder of AGGOSO™ Training, a comprehensive OSINT training program for investigators, corporations, law firms and journalists. Any questions or comments? Contact him at csalgado@allpointsinv.com. Thank you for reading!