Happy Holidays! Good News: Your Stolen Identity and Siphoned Funds Come Giftwrapped!

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

Silent night, holy night. All is calm… all is gone.

As your family members smile and laugh around the room, you spew out a misshapen smile to them to hide the pain from a recently received disastrous SMS text message. This text quickly spiraled out of control, draining your holiday funds and your holiday spirit.

Your teenage nephew walks towards you and taps you on your shoulder. He asks, "What's wrong?" Staring deep beyond his blue eyes – almost into a different dimension behind his head – you wonder how you'll avoid honestly answering his innocent and helpful inquiry. Among the mountain of gifts on a nearby table, you hope to hide in the sea of the others' good intentions as you cringe at the idea that he may notice your lack of gifts for him and the rest of the family. Let's pause and reflect on how you arrived here.

Four weeks ago, you received an SMS text message on your phone. It was "Amazon" informing you that your package was being redirected due to a shipping delay. It further informed you that a new arrival date eagerly awaited you conveniently behind a link. Given that fact that you, among millions of other Amazon customers, were awaiting packages during the holiday season, you acted in good faith to resolve this simple shipping mishap. Concerned about losing a holiday package for someone, you quickly and absentmindedly clicked on the link. [Initiate a mic-drop audio for the bad guys.]

Any other time of the year, you would have easily and hastily deleted that text. In addition, you would have blocked the phone number without hesitation. Nonetheless, this time, your guard was down since the request came in while you awaited a package to be delivered to someone during the holiday season. It was not a perfect storm but perfect timing.

Although some of us may be able to guess where this is going, allow me to paint the picture of both remorse and desperation.

Let's go back to that single SMS text. After clicking on it inside the text and landing on the webpage that the "helpful" link brought you to, you are requested to "confirm" your contact information, shipping address, recipient name and your order number. You oblige the requesting form, not even taking note of the URL as you do this. Of course, it's not that easily spotted being that you're doing this on your phone. As you know, URLs are better hidden on mobile phones than on laptops and desktops. Bad actors even depend on this! These days, many of us now navigate the web and conduct online efforts more often on our phones than on a computer.

After your entry of the requested information, now what? Instead of being directed to the updated ETA on the package, you're requested to enter a payment to ensure that your package gets properly redirected into the hands of your intended recipient by the due date. You pause for a moment at this request, wondering why you should pay for additional shipping on a package that was, essentially, misplaced by the shipping company. You shift to your true email from Amazon and confirm the correct shipping address was provided with the order. Nonetheless, you figure since you're in direct contact with the shipping company, this update is legit and, therefore, you should pay the shipping fee to avoid any awkwardness at a holiday party without a gift.

You dig up your credit card and enter away! The deed is done and you are congratulated by the site for your prompt payment. Your package is assured to arrive on time at the correct address. This chapter is now closed… kind of.

Afterwards, you send a message to Amazon for the frustrating runaround with the shipper. Fast forward to the end of your conversation with Amazon, you realize that you were scammed. Being that hindsight is 20/20, you search your documents and confirm that the package actually showed up one day earlier than the original ETA. More painfully, it was delivered one day before you received the SMS text message from the scammers. Had you paused and checked your account on the Amazon app, you would have likely avoided being victimized. However, within your haste to respond to the text message, you only reviewed the outdated email that confirmed your order. Only now is when you locate the Amazon email confirming delivery inside your inbox; there it is… in your READ pile – as in, previously read and no longer marked UNREAD. You likely clicked on it unknowingly and changed the status of the email, allowing it to rest at the bottom of your inbox, being that you sort your emails and prioritize them by UNREAD status. (UNREAD emails sit at the top of your inbox while the READ emails sit towards the bottom.) It happens to be that you never opened the order confirmation email from Amazon because you saw the preview as it came in immediately after your order was concluded. Therefore, that email was primed [excuse the semi-Amazon pun] for you at the top of your inbox, making it easier to grab in a frenzy. So, this was the first email that you saw at the top of your inbox from Amazon. In effect, you incorrectly assumed it offered the latest status on your order, considering the delivery confirmation email was hidden deeper in your READ pile further down your inbox.

Your concern immediately shifts from the lost $49 that you sent to the scammers via your credit card to your overall financial privacy, given that you realize you provided your full credit card information – yes, even that secret sauce three-digit CVV (Card Verification Value) code – to your social engineer attackers.

Not far from your scheduled holiday celebration with your family, you're drowning in efforts to frantically contact your bank to cancel your credit card. You also request to preview the amount of finances spent within the last few days since you provided the bad actors with your credit

card information. Your bank thanks you for calling them, as they were going to call you due to your recent credit card activity. You're in the hole for the card's maximum amount of $10K. Adding salt to the wound, your bank – where your checking account, savings account and credit card all originate – informs you that another $7K was transferred from your checking account to another. The scammers social engineered themselves into your account, convincing one of your bank's member services operators that they were you. Once "your identity" was confirmed, the helpful bank employee aided with the transfer. (Yes, the offenders would need more than credit card information to do this but let's paint the picture that you were spearphished due to the offenders having personal information on you from a data leak that was purchased. Concerningly, your information was not made available on the dark web but the deep web! Yes, this is a thing.)

Back to our situation. The holiday is nearly here and you are $17K in the hole. Making matters worse, you are an annual late bloomer to holiday shopping. Given your loss, you have no money to continue your shopping agenda. You're financially frozen in your tracks from this single and simple SMS text.

This above example is not a one-off situation. This type of scam is not a fictional story; it is not one best reserved for the rich or the well-known or the celebrities to exclusively be on the lookout for. It is happening to many average persons across the globe. This situation is rigorously applied to persons in the US. I've said this before in my articles, cyber attackers, social engineers and other bad actors are no longer fixated on a mighty payout from the big companies and ignoring the average person. They've learned that it pays to involve average persons into their scams as well. They know that it's a numbers game: the more persons they net into their scheme, they better ROI they receive. Additionally, it's easier to engage the average person, as they don't likely have a polished cyber security infrastructure to negate these simple attacks. Regrettably, the fraudsters are correct, which is why it is nothing short of critical for all of us to be diligent when we decide to action an electronic or telephonic request. Stop and think. If the person on the other end of the communication is harassing you or bullying you to "act now," hang up or don't respond. Challenge the requestor by confirming the provided information via the source: Amazon's app or website, a proper Amazon email or your bank's phone number on the back of your credit card. Keep in mind that outside of this whirlwind of details constructed by the "bad guys," the fix can truly be simple: stop and think. It's the context of the situation that we're delivered that creates the confusion or chaos within an otherwise avoidable loss.

In no way am I claiming that this is easy to do. In fact, that's why these scams work exceedingly well. It's an easy statement to hear but a difficult one to follow at the right time – and at the time it matters most. However, this reminder simply calls on us to "go back to basics" and do what we would do if we were faced with a stranger's request that's not tightly wrapped in a sense of deceit and urgency: stop and think. It's only when we blindly adopt the details of a conniving pretext that we immediately search for a quick fix to satisfy our fears – a knee-jerk reaction. I preach to you to please challenge that "fear," define it and confirm it from outside of the immediacy. Some of you readers are former law enforcement. Unless there is a real threat of life before you, there's no need to act so quickly. The bad actors want your money and don't want you to stop and think but you absolutely can!

Let's add some objective depth to scams like the one above. During the holiday season of 2021, T-Mobile and its partner, First Orion, collectively reported that "…Americans will receive over 27 BILLION scam calls over the next few weeks, resulting in a potential 21 million victims. And people are taking notice – more than 50% of people say they get more scam calls during the holiday season." Additionally, First Orion reported "57% of consumers say they receive more scam calls during the holiday season." [How to Tell Scammers to Take a Hike This Holiday Season by T-Mobile Stories, December 02, 2021: https://www.t-mobile.com/news/un-carrier/scam-shield-holiday-fraud-protection]

Given this information, it is tremendously important for us to remind ourselves that it's OK to challenge persons seeking actions from us, especially when it includes relaying our finances or personal information. The more we remind ourselves to stop and think during non-incident times, the greater capability we'll have in flexing that muscle memory to act appropriately when we find ourselves in such a predicament. Unfortunately, I must say "when" we find ourselves in such predicaments, given the astronomical stats on scammer attempts during the holiday season. Regardless, if we can train ourselves to rely on muscle memory and act as I'm proposing, who knows… maybe one day we can all unwrap a gift of lower stats on holiday scammer victims. Knowledge is power. Be powerful out there, folks, and happy holidays to you and your families. **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. A leading cyber expert and social engineer, he has been a trusted security and investigations leader for 20 years in corporate risk, threat management, 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 the FBI, Homeland Security Investigations, ICE, 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. Christopher has been interviewed on numerous media outlets, including Oxygen's True Crime, other industry-leading media and various podcasts. Any questions or comments? Contact him at csalgado@allpointsinv.com. Thank you for reading!