ChatGPT

Analysis of a Long-Term Romance Scam (Slowmance) Involving a Fake Doctor

Chronological Timeline of the Scam

1. **Initial Contact on Dating App:** The scammer first approached the victim, Dana Skully, on the SayHi dating app. Using a profile with photos of a distinguished-looking doctor, he struck up a friendly conversation. Early on, he moved the discussion off the app and onto text messaging using a **burner phone number** (an untraceable prepaid/contact number), a tactic to avoid the oversight of the app and maintain control of communication [1]. This transition to SMS also made it harder to identify him, since a burner number cannot be easily linked to a real identity – an immediate red flag in hindsight.

2. **Courtship and Trust-Building:** Over **an extended period (a slow-burn "slowmance")**, the scammer cultivated an emotional bond with Dana. He frequently **love-bombed** her with affectionate messages and pet names. For example, he would send morning texts like *"Good morning, my beautiful woman… knowing you're mine is the best feeling in the world"* and constantly remind her how *"precious"* she was to him. He complimented even small things to build intimacy – when Dana mentioned her car, he gushed, *"Omg, you have a very beautiful car… I love your car, sweetheart."* Such excessive flattery and rapid escalation of endearments are typical in romance scams [2] [3]. During this phase, the scammer also professed his devotion (even saying "I love you" relatively soon) and discussed future plans together, strengthening Dana's belief in the relationship. All of this was **designed to gain her trust and affection** so she would be more likely to help him later [4].

3. **Establishing a False Identity:** The scammer claimed to be a doctor working abroad, a **persona reinforced by the stolen photos** he used. He gave his name as *"William Garrett"* (not the real name of the man in the photos) and portrayed himself as a successful, caring medical professional. This fake identity was highly strategic – scammers often impersonate **doctors or military officers deployed overseas** to appear both respectable and conveniently unavailable for in-person meetings [5]. In this case, the images sent to Dana were of a well-known physician, lending credibility to his story. He never video-called live, offering excuses for why he couldn't meet or chat face-to-face (common ploys include claiming poor internet or strict work conditions). By keeping interactions to text (and later attempting pre-recorded video), he controlled what Dana saw. Throughout the romance, *he carefully avoided revealing anything (like a live video chat or verifiable personal details) that could expose the fact that he was not the man in the photos.*

4. **Introduction of an Urgent Crisis:** After a long period of grooming, the scammer introduced a dramatic personal crisis to pivot the conversation toward finances. He claimed that while working in a **volatile region (Iran)**, he received an urgent directive: *"Honey, all senior doctors… have been asked to withdraw their personal belongings from all private security companies here in Iran because… ISIS and bandits are planning an attack."* In other words, he fabricated a scenario in which his wealth or important assets were suddenly unsafe due to looming conflict. This elaborate story created a sense

of **immediacy and danger**, pressuring Dana to sympathize and act quickly. (Scam scripts often use overseas crises like war, political unrest, or medical emergencies to justify why a wealthy professional suddenly needs help [6].) The **"personal belongings"** he referenced were later clarified to be a **portfolio of money and documents** he had stored for safety – now he *had* to get these valuables out of the country immediately. This set the stage for involving Dana in a financial solution.

5. **The Diplomatic Package Scheme:** To resolve the crisis, the scammer told Dana he would send his *"portfolio"* to her for safekeeping. He explained that he'd arrange a **diplomatic courier** (a private "diplomat") to deliver a **sealed box of cash and important documents** to her address. This is a classic twist on romance scams: the scammer pretends to **entrust the victim with a valuable package** – often described as a trunk full of money, gold, or personal assets – as a sign of love and commitment [7]. In reality, such diplomatic deliveries are a fiction: *"there is no Diplomatic Delivery Company or Courier Service"* that delivers personal packages of cash to private individuals [8]. But Dana, still believing in "William," was led to think a secure shipment was on its way. At this point, a **third party** entered the story: the scammer provided contact with the supposed *courier/diplomat*. Dana received communication indicating *"an important confidential package to deliver from William Garrett"* was en route to her. This made the situation feel more legitimate to her – an official-sounding courier was now involved. In reality, it was either the scammer himself or an associate impersonating a courier, a common tactic to add layers of believability (fake **emails or messages from "customs" or courier officials are frequently used in such scams** [9]). This stage of the scam was the **culmination of the setup**: Dana was led to expect a box containing a large sum of money and documents, ostensibly proving William's sincerity and providing her a sense of security that funds were available.

6. **Requests for Money and "Help":** Once the package narrative was in play, the scammer introduced **financial requests**. He told Dana that there were fees associated with the shipment – for example, **courier fees or customs charges** – that needed to be paid urgently to get the package delivered. He did not ask Dana outright to *give* him money for personal use; instead, he framed it as a temporary loan to cover official costs. In their texts, he pressed her: *"I would need to pay it back to them right away… I need your word on this!"* and urged her to help arrange the payment. Dana was understandably hesitant about sending money. She indicated she might **borrow funds from a family member** to assist, but only on the condition that the scammer **prove his identity and honesty**. Specifically, Dana said a family member was willing to help if "William" would **make a quick video of himself promising to repay** – a reasonable verification step on her part. This was a pivotal moment: the scammer now faced a serious challenge to his false identity. Initially, he tried to **deflect and plead for trust** instead of complying. He wrote, *"Honey, you've to trust me… we are definitely going to pay her (the family member) back, we are in this together, my sweetheart."* He attempted to reassure Dana with affectionate language and **promises of repayment**, rather than providing the requested video. This kind of response – turning the request for proof into an emotional appeal – is a known strategy when scammers cannot verify their identity. Still, Dana's family insisted on a verification video **before any money was sent**. At this stage, the scammer increased the pressure: he stressed the urgency (implying the delivery or his situation might fall apart without prompt payment) and repeatedly asked if she could get the money ready. Dana, however, stood firm that **no funds would be handed over until he proved himself genuine**.

7. **Fake Video and Exposure of the Scam:** Cornered by Dana's ultimatum, the scammer made an unexpected move – he actually sent a **video**. The video ostensibly showed "William" (the man in the

stolen photos) speaking, likely delivering a promise to repay or a loving message, to satisfy Dana's condition. In reality, the scammer had leveraged technology to create a **deepfake-style AI video** using the doctor's images. This is a newly emerging scam tactic: scammers can use **AI tools to generate a video from photos**, making it appear the person is talking on camera [10]. The goal was to deceive Dana into believing she finally had visual proof of her beloved "William." The video did buy the scammer a bit of time – but it ultimately **backfired**. Upon viewing it, Dana noticed tell-tale signs of manipulation. The footage was not very convincing; it likely had unnatural facial movements or audio, tipping her off that it was not a genuine live recording. Dana realized that "William" was not who he claimed to be. In a final text, she confronted him with a sharp remark: *"I'm still truly impressed by your talent for creating AI videos from photos – it's remarkable work."* Her sarcastic message made it clear she knew the video was a fabrication. She even taunted him by asking for *"a few more videos"* – essentially challenging the scammer to keep up the charade. At **this moment (Sept 29, morning)**, the long-running scam fully unraveled. The scammer, sensing he was exposed, became desperate. He sent anxious messages like *"Sweetheart, let me know when you wake up"* and later, *"Do you block me?"* twice in a row when Dana went quiet. His panic confirmed his guilt. Dana did not send any money in the end, and by openly acknowledging the AI trick, she effectively ended the scam. The promised **box of money was either never actually sent or became irrelevant**, since Dana would no longer cooperate. In similar scam cases, such a "package" typically *never truly existed or is held hostage for fees*. Here, Dana's refusal to pay and demand for proof forced the scammer to either flee or attempt increasingly implausible lies. The romance scam that began with flirtation on a dating app had now come to a close, with the scammer's identity shattered by Dana's due diligence.

Scam Type and Classification

This case is a textbook example of an **online romance scam**, specifically a **long-term romance scam** often dubbed a "slowmance." In a romance scam, a criminal creates a **fake online identity to win a victim's affection and trust**, then exploits the illusion of a romantic relationship to manipulate or steal from the victim [4]. In contrast to quick "love-at-first-sight" cons, a long-term romance scam involves **patient, gradual grooming** over weeks or months before any criminal payoff is attempted [11]. The scammer invested considerable time into building a convincing relationship with Dana, which is characteristic of a slowmance approach. By the time he introduced any money angle, Dana already felt a strong emotional bond – making her more vulnerable to requests that might otherwise raise suspicion.

Typologically, this scam can be classified as a hybrid of a romance scam and an advance-fee fraud scheme involving a fake diplomatic courier. The narrative about shipping a box of cash via a diplomat is a known variant in romance fraud circles [7]. Often referred to as a *"diplomatic package scam"* or *"consignment scam,"* this method entails the scammer claiming to send the victim a valuable parcel (money, gold, etc.), only to then demand the victim pay various fees (shipping, customs, taxes, anti-terrorism certificates, etc.) to secure its release [12] [13]. In Dana's case, the scammer never got to fully execute the fee extraction because she caught on, but he was **attempting the classic ploy**: first he professed his love (romance scam), then he concocted an urgent reason to need financial help (advance-fee scenario), and he used the **diplomatic courier story** as the vehicle for the fraud.

Notably, the scammer's behavior also put Dana at risk of becoming an unwitting **money mule**. Had she complied, she might have been roped into illegally moving money. In fact, asking someone to accept a package of cash from overseas is a huge red flag – transferring large sums of undeclared cash into the U.S. (or any country) is typically illegal without proper documentation, and victims who agree to receive and forward such packages can be culpable of money laundering [14]. Authorities warn that **romance scammers sometimes groom victims to move money under the guise of love**, essentially making them accomplices without their full awareness [11]. In summary, this scam falls under **Romance Fraud (Impostor Persona)** with a subtype of **“Rescue Package” scam,** executed in a long-term, highly orchestrated manner.

Identity Misuse Tactics by the Scammer

Figure: The scammer stole the photos of a real-life physician (a public figure) to craft a credible fake identity. He never used the doctor’s actual name, going instead by an alias "William Garrett," to avoid easy detection. Above is one of the profile images he sent, presenting himself as a mature, successful medical professional.

From the very start, the scammer’s strategy relied on **identity deception.** He appropriated the **images of a well-known doctor** to lend authenticity and attractiveness to his profile. By using a public figure’s photos, he benefited from the real person’s prestige (the man in the images appears professional, wearing a suit and seen in what looks like an office), while the fake name ensured a casual search wouldn’t directly reveal the true person’s identity or any scam warnings tied to those photos. This separation of *image* and *name* is deliberate: scammers know that if a victim Googles a real name, they might find the actual person (who isn’t on the dating app) or reports of scams. In this case, calling himself “William Garrett” gave the scammer cover, since the stolen images’ real owner has a different name. It’s common in romance scams for fraudsters to impersonate **professionals like doctors, soldiers, or engineers working abroad**, because these occupations inspire trust and also provide a built-in excuse for limited direct contact [5].

The scammer carefully **avoided live interaction** that could expose the impersonation. Throughout the relationship, he refused video calls and never met in person, always citing reasons (travel distance, busy schedule in a remote location, poor connectivity, etc.). This aligns with known scam patterns: *if an online love interest is always “too busy” or unable to video chat, especially while claiming to be in an overseas or sensitive job, it’s a warning sign* [15] [16]. Dana grew suspicious eventually, which is why she demanded a verification video. Cornered, the scammer attempted an **AI-generated deepfake video**. This is a notable misuse of technology – he likely used still images of the doctor’s face and some software to create a short clip of “him” speaking. While romance scammers traditionally avoided video altogether, many now turn to tools that can simulate a person’s appearance on camera [10]. In this case, the video was convincing enough at first glance that it could have fooled someone not on guard. However, Dana recognized it as artificial (perhaps the voice didn’t match, or the facial movements were uncanny). By **trying to use the real victim’s likeness in a video**, the scammer escalated his identity theft to a new level. This tactic demonstrates how far scammers will go – even faking live evidence – to maintain their lies.

It’s important to note that the real doctor whose images were used had no involvement; he was an innocent third party. The scammer likely found those photos online (since the doctor is well-known, his images might be publicly available through professional profiles or social media). Impersonation of public figures in scams is alarmingly common, as noted by scam monitoring agencies: scammers “pretend to be public figures or claim they are in remote locations” to explain away why they can’t meet, all while exploiting the trust people place in those identities [16]. Here, the doctor’s reputation was the bait, and the alias plus refusal of direct contact was the hook that kept the scammer’s real identity hidden.

Communication Strategies Used by the Scammer

The scammer in this case employed a range of manipulative communication tactics to further the con. Key strategies included:

- **Love-Bombing and Emotional Seduction:** He overwhelmed Dana with affection and attention. From early on, he sent frequent messages filled with endearments (*"honey," "sweetheart," "baby,"* etc.) and compliments. He even made statements of deep love and attachment relatively soon. This **"fast-forwarding"** of the relationship – behaving as if they were soulmates after a short time – was meant to quickly create an emotional dependence [2]. By showering her with praise (e.g., telling her *"Waking up and knowing you're mine is the best feeling in the world"* every morning) and concern (*"I've been thinking about you all day, hoping you're doing well"*), he fostered intimacy. This relentless positivity and romantic enthusiasm is a calculated tactic: the victim feels adored and reciprocates trust, often overlooking inconsistencies as a result.

- **Establishing Trust and Team Identity:** The scammer often framed things as *"we"* and *"us,"* reinforcing that he and Dana were a unit facing problems together. For instance, when discussing the financial dilemma, he said *"we are in this together, my sweetheart"* to make her feel their fates were linked. He also explicitly asked for trust, saying things like *"you've to trust me"* when she hesitated. By building a narrative of **partnership** and even a future together, he leveraged Dana's feelings to secure cooperation. This is classic in romance scams: the fraudster creates an illusion that helping him is for their mutual benefit (e.g., "our future" or "so we can be together"), not just a one-sided favor [17].

- **Grooming with Personal and Sexual Content:** The communication wasn't only financial or romantic – the scammer also attempted to engage Dana in a sexual context to deepen the bond and potentially gain leverage. At one point, he told her *"Got some new underwear today... let me see yours, baby,"* pressuring her to share intimate photos. Dana rebuffed him (*"Um sorry definitely not that kind of girl"*), but this request was telling. Such **inappropriate or overly forward sexual requests** serve multiple purposes: they test a victim's boundaries, create a false sense of a normal intimate relationship, and can even provide material for blackmail if the victim complies (scammers have been known to later threaten to expose sensitive photos). The fact that he tried this suggests he was probing how much control he had and whether she was pliable to his wishes. It's also a tactic to ensure the victim is *"all in"* on the relationship, thereby less likely to pull away when financial demands come.

- **Urgency and Pressure Messages:** As soon as the scammer initiated the money part of the scam, his tone shifted to high urgency. He repeatedly emphasized how critical the timing was – that the fees or courier costs had to be paid *immediately* or the opportunity would be lost. He wrote messages in rapid succession when she was slow to respond, such as *"Baby I just heard from her again"* and *"Any chance of you being able to do this? She said she could get me the money today."* This pressure is a deliberate strategy to **panic the victim and short-circuit rational decision-making** [18]. By instilling a fear that delay could mean disaster (in this case, perhaps losing his belongings to an attack or the courier leaving), he tried to rush Dana into paying without further deliberation. The urgency was further reinforced by invoking third parties – e.g., *"she said she could get me the money today"* referring to the family loan – making it seem like even others were on a tight schedule.

- **Appeals to Emotion and Sympathy:** The scammer carefully crafted his story to pull at heartstrings. He portrayed himself as a successful but vulnerable man in a dangerous situation. By mentioning being in Iran, the threat of ISIS, and needing to save his life's work, he aimed to evoke **Dana's sympathy and protective instinct**. He often called her his *"beautiful woman"* and expressed how much he *needed* her support, which would make Dana feel special and responsible for his well-being. When she hesitated to send money, he didn't respond with anger but with hurt and desperation – saying things like *"I really understand but…"* and reassuring her of his love. This is emotional manipulation 101: he used her compassion and affection for him as leverage, hoping she'd feel guilty or worried for him, enough to override her caution.

- **Isolation from Outside Advice:** While Dana did involve her family (which ultimately helped expose the scam), the scammer's behavior shows hints of typical **isolation tactics**. He moved the chat off the public app into a private channel early on, as mentioned, which already isolates the victim from the platform's safety features or others' oversight [1]. He also likely preferred that she keep their plans secret. (Although in this scenario he didn't explicitly forbid her from talking to family, he certainly didn't encourage it. The moment she mentioned a family member's conditions, he tried to sidestep it with *"you have to trust me"* – subtly implying that the trust between them should be enough, and external verification shouldn't be needed.) Scammers often **discourage victims from consulting friends or family** about the relationship or the financial requests, knowing a third party might see the red flags clearly [19]. Dana's case is somewhat unique in that she did seek outside counsel (her family), which created an obstacle for the scammer. His insistence on trust and secrecy would likely have increased had she not caught him with the AI video – typically, once a victim agrees to keep things "just between us," the scammer can escalate the fraud without interference.

- **Use of Third-Person Personas (Authority Figures):** As part of the ruse, the scammer introduced the idea of a diplomat/courier and possibly even sent messages posing as that courier or a customs official. While we have limited direct text from the "courier," the scammer did convey messages like *"they will assign a delivery diplomat who will make the delivery"* and gave Dana instructions as if from the courier service. This is a communication strategy where the scammer **plays multiple roles** – their own lover persona and fake officials – to validate their story. By writing in a more formal tone or using separate contact info for the "diplomat," the scammer can pressure the victim from two angles. For example, Dana might get an email from a fake **"Diplomatic Courier Service"** with official-looking language asking for a fee, while "William" simultaneously begs her to just pay it to help him. This one-two punch can overwhelm victims. (Although Dana's scam didn't fully reach the point of fabricated emails, the groundwork was laid for it. Such communications often contain **inconsistencies and errors** that are telltale signs – for instance, unusual phrases like "important confidential package" and requests for payments via odd methods, which real courier companies or customs agencies wouldn't use [20].)

In summary, the scammer's communications were a **carefully orchestrated mix of affection, manipulation, urgency, and deception.** By analyzing his words and requests, one can see nearly every hallmark of romance fraud: fast-tracked intimacy, reluctance for verifiable contact, a dramatic emergency, solicitations of money, and attempts to isolate the victim from skepticism. Dana experienced each of these in turn, and ultimately it was the inconsistencies in his communication – from the far-fetched story to the fake video – that gave him away.

Financial and Logistical Red Flags

Several **red flags** in this case could have indicated the fraudulent nature of the scheme. In retrospect, these warning signs stand out:

- **Requests to Handle Large Sums of Cash Illegally:** The scammer's endgame involved asking Dana to **receive a shipment of cash** – a box allegedly containing his money. This is highly suspicious and improper. Legitimate people do not ship cash across borders in secret, and as Dana herself recognized (being a compliance-savvy person), bringing large undeclared amounts of money into the country is illegal without proper paperwork [14]. Any scenario where someone you've never met wants you to hold or transfer a significant amount of money for them is almost certainly a scam. In fact, authorities warn that agreeing to such requests can make you a **"money mule,"** entangling you in money laundering or other crimes [21]. Dana was prudent to initially refuse this arrangement; her instincts were correct that something was off.

- **"Diplomatic Courier" Story:** The scammer's logistical explanation was that a **diplomat would deliver the package of cash** directly to Dana's door. This is a glaring red flag. **Diplomatic pouches** are used by governments for official documents and are not a personal courier service for individuals' belongings [8]. Scammers invoke "diplomatic courier" or "UN diplomat" to make it sound legitimate and urgent (as if normal shipping can't be used in a conflict zone). In truth, as anti-scam experts note, *"a claim that a diplomat will come to your home to deliver a box is made up and a scam"* [22]. The presence of this element in William's story is a clear indicator of a known fraud tactic.

- **Upfront Money for a "Free" Gift:** Another red flag was the **advance fee** aspect. The scammer promised Dana a valuable gift (his portfolio/fortune), but then introduced fees that **she** had to pay to receive it (shipping costs, etc.). In legitimate situations, a gift giver doesn't ask the recipient to pay handling fees – they would cover any costs themselves. Asking for money **in advance of receiving something** is characteristic of many scams (hence the term *"advance-fee fraud"*). Dana was wise to insist on proof before paying; generally, the moment someone you only know online asks you for **any** money, especially with urgency, the scam alarm should sound [23]. Here, the scammer's insistence that she *loan* a large sum for courier fees – with the promise of immediate reimbursement – was a huge warning sign.

- **Untraceable Contact Information:** The scammer used a **burner phone number** to communicate, which is a logistical red flag. The number was likely not under a contract or real name, making it difficult to trace. Often scammers will use internet-based numbers or foreign numbers; if a victim tries to look up who owns the line, they hit a dead end. While an average person might not initially realize the number is untraceable, there were clues. For instance, if Dana ever called the number, it might have strange call quality or ring inconsistently (signs of a VOIP or forwarding service). Additionally, he likely avoided giving any physical address or verifiable personal contact aside from that phone. Trustworthy individuals you form relationships with will share basic personal details, whereas this scammer remained vague about his exact location and provided no alternate means of contact (no workplace number, no video chat ID, etc.).

- **Excuses to Avoid Live Interaction:** Tied to the above, his constant **refusal to meet in person or video chat** was a red flag that something was wrong. While long-distance relationships can justify not meeting physically right away, a genuine person will usually agree to video call at least, or eventually make concrete plans to meet. In this case, every time the prospect of a real-time interaction arose, the scammer had an excuse. He only attempted a video in a controlled, pre-recorded fashion (which turned out to be fake). This reluctance to show his face or have a spontaneous conversation should have been taken as a warning. Often scammers claim broken cameras, strict overseas contracts, or say they're in a war zone and can't video call – all of which match the pattern here (doctor in a conflict area). Any **consistent avoidance of live communication**, especially after months, is a sign of an impostor [24] .

- **Inconsistencies and Far-Fetched Stories:** The content of the scammer's story contained inconsistencies that are red flags on close inspection. For example, he mentioned *"UN Delegates' secret service agent"* warning about ISIS attacks – a convoluted detail that doesn't square perfectly with his role as a doctor. He also used odd phrases like *"all senior Doctors officials"*, which sound unnatural (mixing "doctors" and "officials"). Small language quirks or factual inconsistencies like this can indicate the person is lying or not who they claim. Additionally, the whole premise that a wealthy doctor needs his new online girlfriend's personal help to save his fortune is highly implausible. A real individual in that position would have institutional support or friends/family to turn to, not someone he's never met. The **elaborateness of the emergency (terrorists, covert shipments, etc.)** was itself a red flag – scammers often construct overly dramatic scenarios to overwhelm the victim's skepticism. Dana did question some of these points (she involved her family, asked for proof), which is good practice.

- **Rapid Escalation to Money Matters:** While the romance was long in duration, once the subject turned to money, it escalated quickly. Within a short span, the scammer went from sweet talk to asking for a large financial favor. He pressured Dana to borrow money and essentially put her finances on the line for him. In legitimate relationships, financial entanglements (especially large loans or handling huge sums of cash) do not come into play so early, if ever. The fact that significant money became a central topic is a red flag. As the Federal Trade Commission bluntly advises: *"As soon as an online love interest asks for money, for any reason, the scam bell rings."* [23] This case was no exception.

- **Involvement of a Third Party Demanding Privacy:** The scammer attempted to involve an alleged diplomat and might have later introduced fake officials (had the scam continued). These actors often demand discretion. For instance, a fake courier might tell the victim not to tell customs or authorities about the cash, or a phony security company might ask for personal info under the guise of verification. In Dana's scenario, while it hadn't progressed to that stage, the groundwork for secrecy was laid (she was dealing directly with "William" and the "courier" in a closed loop). **Any instruction to keep a transaction secret or to lie about its purpose is a severe red flag.** Scammers know if a bank or a friend hears "I'm sending money to receive a box of cash from a diplomat," they will intervene, so they try to keep the victim isolated in the scheme.

In conclusion, this slowmance scam exhibited numerous warning signs that, if recognized, could have revealed the deceit earlier. Hindsight is 20/20 – Dana's trust and emotional investment clouded some of these red flags for a time, which is what scammers count on. Thankfully, key red flags like the demand for a verification video and the suspicious nature of the cash shipment ultimately led Dana to discover the truth before she suffered financial loss. Each element – from the burner phone to the diplomatic courier tale – is a puzzle piece that forms a clear picture of fraud once you know what to look for. By examining these clues in aggregate, one can better understand how to spot and prevent such scams in the future.

Sources:

- Federal Trade Commission – *Consumer Alerts: Romance Scams and Package Fraud* [14] [23]
- Federal Bureau of Investigation – *Romance Scams Definition and Red Flags* [4] [15]
- National Anti-Scam Centre (Australia) – *Characteristics of Long-term Romance Scams* [11] [16] [10]
- LoveScammer.com (Scam education) – *Diplomatic Courier Scam Modus Operandi* [7] [8] [13]

---

[1] [3] [10] [11] [16] [19] New fusion cell focuses on emotional and financial harm of romance scams | National Anti-Scam Centre
https://www.nasc.gov.au/news/new-fusion-cell-focuses-on-emotional-and-financial-harm-of-romance-scams

[2] [4] [15] [24] Romance Scams — FBI
https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/romance-scams

[5] [6] [7] [8] [9] [12] [13] [17] [18] [20] [22] Beware of Diplomatic Courier Service Scams in Online Romance
https://lovescammer.com/lovescam-blog/beware-of-diplomatic-courier-service-scams/

[14] [21] [23] Is that person you met online really a military servicemember...or a scammer? | Consumer Advice
https://consumer.ftc.gov/consumer-alerts/2024/06/person-you-met-online-really-military-servicememberor-scammer