

The Supply Chain and Modus Operandi of Online Romance Fraudsters

Dr. David Maimon
SentiLink
Georgia State University

Background

My name is David Maimon, and I am the Head of Fraud Insight at [SentiLink](#), as well as a Professor in the [Department of Criminal Justice and Criminology at Georgia State University](#). My research focuses on cybercrime, and throughout my career, I have studied a wide range of cybercrimes and online offenders, including hackers and the progression of hacking events (Maimon et al., 2014), online grooming and groomers (e.g., Kamar et al., 2023), darknet market vendors and their responses to deterrence efforts (e.g., Howell et al., 2024), and online fraud (e.g., Maimon et al., 2023).

The central question I strive to answer throughout my academic career is: What works and what doesn't in the context of online crime prevention and mitigation efforts? To answer this question, I collect data directly from key junctions formed by the four major inhabitants of the cybercrime ecosystem: offenders, targets, guardians, and enablers (Maimon and Louderback, 2019). These junctions allow my team and me to deploy data collection efforts in real-world settings. For example, to explore ways to deflect online groomers (offenders) away from children (targets), we developed a chat-bot that simulates a 13-year-old girl. The bot engages in conversations with groomers and presents different situational circumstances, helping us understand what factors might prompt the offender to disengage from the conversation. Similarly, to investigate how hacking events can be disrupted, my team and I deployed honeypots—target computers designed to attract hackers in order to study their behaviors—and studied how hackers (offenders) responded to deterrent messages within the compromised system (targets) (Maimon et al., 2014).

My work in the context of online fraud follows a similar approach, but it involves our team's infiltration into online fraud markets hosted on the Clearnet, darknet environments, and messaging applications such as Telegram and WhatsApp. The commodities available in these markets range from stolen identities and fake documents to stolen checks, credit cards, compromised bank accounts, and skimmers. Often, these markets also feature tutorials that teach others how to engage in fraud. Additionally, these environments foster conversations among market users discussing a wide range of fraudulent activities and tactics. At both the university and the company, my teams focus on extracting data from this ecosystem, analyzing it, and generating actionable insights. For example, one of the most intriguing phenomena we uncovered is the presence of "rippers"—fraudsters who scam other fraudsters. Other key insights include identifying emerging fraud trends, such as the surge in unemployment benefits fraud in 2020 and the rise in check theft and check

fraud in 2022 (see <https://theconversation.com/how-cybercriminals-turn-paper-checks-stolen-from-mailboxes-into-bitcoin-173796>).

Since my academic research is both relevant to the criminological discipline and rigorous, it has been published in numerous peer-reviewed academic journals. My work has also been featured in popular media outlets such as AARP in the USA and *Panorama* in the UK, to name a few. This background, along with my team's efforts to document and analyze fraud groups worldwide—their modus operandi and supply chains—provides the foundation for my testimony.

The supply chain behind online romance fraud

Romance fraud refers to instances in which individuals create fake identities and fabricate romantic relationships to deceive and financially exploit others. Online romance fraud (or online romance scams) occurs when a criminal assumes a false online identity to gain a victim's affection and trust. The scammer then exploits the illusion of a romantic or close relationship to manipulate the victim emotionally and financially, often leading to significant financial losses (FBI, n.d.).

Online romance fraud is a highly organized criminal enterprise that operates with a structured division of labor. Fraudsters specialize in different roles to ensure the efficiency and profitability of their scams. The complexity of these networks makes them difficult to detect and disrupt. Based on Lemieux's (2003) framework, several roles exist within large-scale online romance fraud networks including **an organizer, an extender, an executor and money movers**.

The **organizer** oversees the entire romance scam operation, defining its scope, strategies, and target demographics. They determine how victims will be approached, which platforms will be used (e.g., dating websites, social media, or messaging apps), and what narratives will be crafted to deceive victims.

The **extender** is responsible for growing the operation by recruiting additional scammers and establishing partnerships with other fraud networks. This role ensures a steady supply of individuals who can pose as romantic interests and engage victims in fraudulent relationships. Extenders may use online forums, encrypted chat groups, or even real-world connections to find and train new recruits.

The **executor** is the scammer who directly interacts with the victim. They create fake online identities, often using stolen photos, and initiate romantic conversations with unsuspecting targets. These scammers invest time in building trust and emotional connections, sometimes engaging victims for weeks or months before requesting money.

Finally, **money movers** step in to facilitate financial transfers while minimizing detection by authorities. These individuals move funds between bank accounts, cryptocurrency

wallets, or prepaid cards to obscure the financial trail. By distributing transactions across multiple accounts, scammers make it harder for law enforcement to trace and freeze fraudulent funds.

Consistent with Lemieux's (2023) framework, my research on online romance fraudster online forums and illicit markets suggests the existence of an illicit supply chain behind online romance fraud. This online supply chain involves a network of **suppliers, producers, distributors, and consumers** who facilitate and sustain online fraud, as well as the victims who ultimately suffer from these fraudulent activities.

Suppliers are responsible for setting up social media profiles used to lure victims into conversation. They steal other people's profile pictures to create fake identities or hack social media accounts, taking control and using them as their own to connect with victims. Recently, we have observed an increasing use of Generative AI technology in this process, enabling scammers to create realistic fake images and fabricate social media accounts with entirely synthetic identities. In addition to creating fake profiles, these individuals supply their teams and the broader fraud ecosystem with essential tools such as VPNs, image editing software, voice-changing applications, and face-swapping technology, further enhancing their ability to deceive and manipulate victims.

VPNs are used to obscure fraudsters real location, making it difficult for law enforcement or cybersecurity teams to track them. By masking their IP addresses, scammers can, appear to be in a different country, aligning with the fake identity they are using, bypass security filters on dating platforms that flag suspicious logins, and evade geolocation tracking by authorities or victims attempting to verify their identity. Image editing tools such as Adobe Photoshop help fraudsters create convincing fake profiles by altering stolen images and modifying photos to match fabricated backstories (for example adding military uniforms, luxury cars, or corporate settings to reinforce their fake persona. Voice changers are especially useful in scams that require phone or video calls. Fraudsters use them to mask gender, age, or accent inconsistencies, mimic professional and familiar sounding voices, and avoid recognition by victims. Finally, face-swapping and deepfake tools allow scammers to generate realistic but fake visual identities, making their deception even more convincing. These tools are used to create synthetic identities and generate entirely new faces that do not exist in reality, fabricate "proof of life" videos in cases where victims demand visual confirmation of the scammer's identity, and produce fake video calls where their face appears to match their stolen profile picture.

Producers play a critical role in online romance and investment fraud networks by ensuring that fraudulent schemes appear sophisticated and credible, increasing the likelihood of deceiving victims. One of their primary responsibilities is the creation of fake digital content. Producers design fraudulent websites that mimic legitimate businesses, financial institutions, or government agencies, making scams appear professional and trustworthy. They also offer edit images services to align with the fabricated backstories used in scams.

Beyond digital deception, some producers assist in reinforcing scams with physical elements to deepen victims' trust. For example, they may arrange for the shipment of physical gifts such as flowers, jewelry, or personalized items to victims, making the scam feel more authentic. Additionally, they provide scammers with fake documents, including passports, military IDs, and financial statements, which serve as "proof" of their fabricated identities. Finally, another crucial function of producers is developing training materials and prepared scripts that help standardize deception techniques within fraud networks. They create pre-written love letters, investment pitches, and conversation templates that scammers use to manipulate victims emotionally and financially. These materials often include psychological manipulation guides, teaching fraudsters how to build rapport, gain trust, and ultimately convince victims to send money. Additionally, producers provide language adaptation resources to ensure that scammers tailor their messages based on the victim's background, culture, and personal vulnerabilities.

Distributors are responsible for creating and managing online forums and marketplaces where the aforementioned fraud-related commodities are offered for sale. These platforms play a crucial role not only in facilitating transactions but also in providing educational resources, recruiting new scammers, and establishing reputations within the fraud community. By maintaining these digital spaces, distributors enable fraud networks to grow, evolve, and sustain their operations.

Importantly, beyond offering technical tools and services that support the progression of online romance fraud and investment scams, distributors also engage in selling access to existing victims. Specifically, in some cases, a fraudster may invest significant time and effort in building rapport with a target but fail to convince them to send money or invest. Rather than abandoning the victim, the scammer may sell the victim's contact information and background details to another fraudster, who then picks up the deception where the original scammer left off. This process ensures that the fraud network maximizes potential profits from each target, even when initial attempts are unsuccessful.

Finally, the **consumers** of these illicit commodities are the individuals who directly interact with victims, building trust and emotional connections in an attempt to defraud them. These scammers, often referred to as "executors" or "enforcers", play the most visible role in the fraud ecosystem, engaging in long-term manipulation strategies designed to extract money, personal information, or financial assets from their targets. These individuals are the frontline operators of online fraud networks, executing the scams that generate profits for the entire ecosystem. Their success depends on the infrastructure created by other players in the supply chain, making their role both dependent on and essential to the longevity of these fraud networks. But how do these frontline operators carry out their scams? What is their modus operandi?

The Modus Operandi of Online Romance Fraudsters

Past research suggests that online romance scams progress in five stages (Whitty 2015). The first step in a romance scam is **baiting**, where fraudsters create fake online profiles to lure potential victims. Once contact is established, the fraudster engages in the second stage, **grooming**. In this stage the fraudster works to build trust and intimacy with the victim. This phase can last for weeks or even months as the scammer strategically mirrors the victim's emotions, interests, and vulnerabilities to create a seemingly genuine bond. The fraudster often showers the victim with compliments, professes love quickly, and claims to share similar life goals. The goal is to make the victim emotionally invested to the point where they are willing to offer financial assistance or comply with other fraudulent requests.

After successfully grooming the victim, the fraudster executes the third stage, **the sting**. In this stage the fraudster attempts to extract money. This typically involves an urgent and emotionally charged crisis story designed to pressure the victim into providing financial assistance. Common scenarios include a sudden medical emergency, legal troubles, travel restrictions, or the unexpected death of a family member. Victims, believing they are helping a loved one, often send money via wire transfers, cryptocurrency, or gift cards, making it difficult to recover the funds once the scam is uncovered.

In some cases, the scam extends beyond financial motives to **sexual exploitation** and humiliation. Specifically, some fraudsters manipulate victims into performing sexual acts on camera, claiming it is a sign of trust or intimacy. These recordings are then used for sextortion, where the fraudster threatens to distribute the footage unless the victim pays a ransom. In the last stage, **the revelation**, the victim realizes they have been deceived, either through personal discovery, intervention by friends and family, or contact from authorities. This phase can be devastating, as victims not only face financial losses but also emotional betrayal and psychological distress.

My investigation into the modus operandi of online romance fraud using conversations, video and pictures they share on their online fraud markets provides deeper insight into the specific crime script of this fraudulent activity.

After creating or taking over a social media profile, fraudsters cast a wide net, sending friend requests to as many potential targets as possible. Once a friend request is accepted, they initiate communication using flattery and compliments about the target's appearance to quickly establish a connection. To avoid detection by social media platform administrators, fraudsters swiftly encourage the target to move the conversation to messaging applications such as WhatsApp, Google Hangouts, or Telegram. These platforms offer greater privacy and less oversight, making it easier for scammers to manipulate their victims without risk of being reported. On these messaging platforms, fraudsters build strong emotional bonds with their targets by texting frequently, sharing curated images and videos, and crafting a narrative that fosters trust and intimacy. As the

relationship deepens, they eventually transition to live video calls, making the scam feel even more real and convincing.

To engage in live video calls, fraudsters employ two key methods. The first involves the use of Generative AI (Gen AI) software that facilitates face-swapping and deepfake manipulation. Some of the most commonly used tools in this process include [Xpression Camera](#) and [DeepFaceLive](#). During these calls, fraudsters activate their computer camera to capture their own face. However, by leveraging deepfake software, they can alter their appearance in real time, disguising their true identity and assuming a fabricated persona. This sophisticated deception allows them to reinforce their false identity, making it even more difficult for victims to detect the scam. Talk about the first call and the fact folks are somehow surprised to see that the person they were talking to is real. The first video call is

The second method involves the use of two smartphones to manipulate the scammer's appearance during live video calls. The first phone is used by the fraudster to apply face-swapping filters or software, allowing them to disguise their real face. Specifically, the scammer activates the phone's camera, focuses it on their own face, and then uses built-in or third-party face-swapping technology to replace their face with a pre-selected image stored on the device. The second phone is used to communicate with the victim. It captures and streams the altered image from the first phone, creating the illusion of a real person on the video call. This technique allows scammers to effectively impersonate someone else in real-time, reinforcing their deception and making it even harder for victims to recognize the scam.

Since fraudsters frequently share lessons and tips with others in their group chats and forums, we can observe notable differences between their initial conversations with victims and the more advanced interactions that occur after building rapport. Analyzing these exchanges provides valuable insights into their evolving manipulation techniques. One particularly striking observation is how, during the first video call, victims often appear surprised that the person behind the conversation seems real. This reaction reinforces their emotional attachment to the fraudster, increasing their vulnerability and, in many cases, leading them to develop deep romantic feelings for the scammer. As the relationship progresses, we have observed that victims share increasingly intimate and sensitive details about their lives. This highlights the effectiveness of fraudsters in building strong emotional bonds using the deceptive tools and psychological tactics at their disposal. Their ability to manipulate emotions over time demonstrates just how powerful and convincing their fraudulent strategies can be.

The request for money in online romance and investment fraud scams is a carefully timed and strategic move designed to maximize the victim's emotional investment before financial exploitation begins. Fraudsters rarely ask for money in the early stages of communication. Instead, they focus on building trust, deepening emotional connections, and establishing a sense of commitment with the victim. The first request for money typically appears after weeks or months of communication, once the victim is fully

engaged in the fabricated relationship. Fraudsters ensure that the victim is emotionally dependent on them before introducing a financial need.

They start with a minor request, such as help covering a small bill, phone credit, or a short-term loan to test the victim's willingness to send money. Once trust is established, the scammer fabricates an urgent financial crisis, such as a medical emergency, legal trouble, travel expenses, or a family tragedy. In investment frauds, scammers convince victims to invest in fake opportunities, such as cryptocurrency trading, stock investments, or real estate deals. These often start with small amounts but quickly escalate as the victim sees fabricated returns designed to encourage further deposits. If a victim complies, the scammer continues to exploit them, requesting more money by escalating the crisis or offering a more lucrative investment opportunity. Some fraudsters introduce fake third parties, such as lawyers, doctors, or bank officials, to legitimize their claims and pressure the victim further.

Fraudsters use a variety of methods to move money while minimizing traceability. Some of the most common money transfer techniques include, bank wire transfers, cryptocurrency payments, gift cards and prepaid cards, and Peer-to-Peer Payment Apps.

A concerning trend is the expansion of these fraud groups into other forms of crime, leveraging the intimate relationships they establish with their victims. Fraudsters are increasingly using their manipulation skills not only for financial scams but also for blackmail and extortion. For example, in some cases, fraudsters exploit intimate videos and images sent by victims, later using them as leverage for sextortion demands. Victims are threatened with public exposure unless they comply with financial or further exploitative requests. Similarly, when targeting married individuals on dating platforms, fraudsters take advantage of their victims' fear of exposure. Once they have established that a victim is engaged in an extramarital affair, they threaten to reveal the secret to their spouse or family unless a ransom is paid.

Importantly, the integration of deepfake technology with international fraudsters' success in extortion scams has led them to explore new ways to exploit compromised social media accounts in the U.S. to steal money from victims—not necessarily those targeted through romance or investment fraud. One alarming tactic involves staging fake kidnappings using deepfake technology. Fraudsters manipulate videos to create realistic depictions of a loved one's face, then send the fabricated footage to family members along with a ransom demand. The hyper-realistic nature of deepfakes increases the credibility of the threat, making it more likely that victims will comply out of fear for their loved one's safety.

This disturbing evolution of fraud underscores the growing risks associated with AI-driven deception and highlights the urgent need for enhanced fraud detection systems, public awareness, and stricter regulations on the misuse of deepfake technology.

Conclusions and Recommendations

Online romance fraud and investment scams represent a rapidly evolving cybercrime threat to American citizens, driven by international organized fraud networks that leverage sophisticated technology and psychological manipulation. My testimony highlighted the structured division of labor within fraud networks, the use of advanced digital deception tools, and the various stages of manipulation employed by fraudsters. Addressing these crimes requires a multi-layered policy response that combines law enforcement action, technological interventions, academic research and public awareness initiatives. Below are key policy recommendations:

1. Strengthening Cybercrime Legislation and Law Enforcement Capabilities- Governments should update and expand cybercrime laws to explicitly address online romance and investment fraud, ensuring legal frameworks are equipped to prosecute offenders effectively. An effort should be made to increase cross-border cooperation between law enforcement agencies, financial institutions, and technology companies to track and dismantle international fraud networks. Finally, in addition to specialized task forces dedicated to investigating and disrupting large-scale fraud operations, efforts should be done to enhance law enforcement training in digital forensics, AI-based fraud detection, and financial transaction monitoring to improve fraud investigations.

2. Regulation and Oversight of Digital Platforms – Since social media platforms play important role in the facilitating opportunities for online romance fraud, efforts should be do to mandate stronger identity verification protocols for social media and dating platforms. Furthermore, messaging platforms (e.g., Telegram, WhatsApp) should be encouraged to crack down on scammer networks by implementing stricter content moderation policies.

3. Public Awareness and Victim Support Programs- Governments should invest in nationwide awareness campaigns to educate the public on recognizing red flags in online relationships and investment offers. Fraud awareness education should be integrated into financial literacy programs, especially for vulnerable populations such as older adults and young investors. Finally, we should consider establishing dedicated victim support services, including hotlines, counseling, and legal assistance, to help those affected from online romance fraud and investment scams to recover emotionally and financially.

4. Prioritizing Evidence-Based Research on Disruption Strategies- Governments should invest in rigorous, evidence-based research to assess the effectiveness of existing and emerging disruption strategies against online romance fraud and investment scams. While various interventions—such as scam detection algorithms, platform moderation, and law enforcement crackdowns—have been implemented, their long-term impact remains unclear. Policymakers should fund research initiatives that evaluate which disruption techniques successfully deter fraudsters, reduce victimization rates, and prevent fraud networks from adapting and evolving. Additionally, there is a critical need to operationalize

financial, psychological, and societal losses linked to online romance fraud and investment scams. Establishing standardized tracking mechanisms across law enforcement, financial institutions, and victim support organizations will provide a more accurate picture of the scale of the issue, enabling governments to develop targeted, measurable policies that address the full impact of these crimes.

References:

Dickinson, T., Wang, F., & Maimon, D. (2023). What money can do: examining the effects of rewards on online romance fraudsters' deceptive strategies. *Deviant Behavior*, 44(9), 1386-1400.

Howell, C. J., Maimon, D., Perkins, R. C., Burruss, G. W., Ouellet, M., & Wu, Y. (2024). Risk avoidance behavior on darknet marketplaces. *Crime & Delinquency*, 70(2), 519-538.

Kamar, E., Howell, C. J., Maimon, D., & Berenblum, T. (2023). The moderating role of thoughtfully reflective decision-making on the relationship between information security messages and smishing victimization: An experiment. *Justice Quarterly*, 40(6), 837-858.

Lemieux, V. (2003). Criminal Networks.
<https://publications.gc.ca/collections/Collection/JS62-107-2003E.pdf>

Maimon, D., & Louderback, E. R. (2019). Cyber-dependent crimes: An interdisciplinary review. *Annual Review of Criminology*, 2(1), 191-216.

Maimon, D., Howell, C. J., Moloney, M., & Park, Y. S. (2023). An examination of email fraudsters' modus operandi. *Crime & Delinquency*, 69(11), 2329-2358.

Maimon, D., Santos, M., & Park, Y. (2019). Online deception and situations conducive to the progression of non-payment fraud. *Journal of Crime and Justice*, 42(5), 516-535.

Shah, D., Harrison, T. G., Freas, C. B., Maimon, D., & Harrison, R. W. (2020, December). Illicit activity detection in large-scale dark and opaque web social networks. In *2020 IEEE international conference on big data (Big Data)* (pp. 4341-4350). IEEE.

Whitty, M. T. (2015). Anatomy of the online dating romance scam. *Security Journal*, 28(4), 443-455.